FEDERAL REGISTER

Vol. 78 Friday,
No. 17 January 25, 2013

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 and 164

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

45 CFR Parts 160 and 164

RIN 0945–AA03

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

AGENCY: Office for Civil Rights, Department of Health and Human Services.

ACTION: Final rule.

SUMMARY: The Department of Health and Human Services (HHS or ''the Department'') is issuing this final rule to: Modify the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Enforcement Rules to implement statutory amendments under the Health Information Technology for Economic and Clinical Health Act (''the HITECH Act'' or ''the Act'') to strengthen the privacy and security protection for individuals' health information; modify the rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) under the HITECH Act to address public comment received on the interim final rule; modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA); and make certain other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities.

DATES: *Effective date:* This final rule is effective on March 26, 2013.

Compliance date: Covered entities and business associates must comply with the applicable requirements of this final rule by September 23, 2013.

FOR FURTHER INFORMATION CONTACT: Andra Wicks 202–205–2292.

SUPPLEMENTARY INFORMATION:

I. Executive Summary and Background

A. Executive Summary

i. Purpose of the Regulatory Action

Need for the Regulatory Action

This final rule is needed to strengthen the privacy and security protections established under the Health Insurance Portability and Accountability of 1996 Act (HIPAA) for individual's health information maintained in electronic health records and other formats. This final rule also makes changes to the HIPAA rules that are designed to increase flexibility for and decrease burden on the regulated entities, as well as to harmonize certain requirements with those under the Department's Human Subjects Protections regulations. These changes are consistent with, and arise in part from, the Department's obligations under Executive Order 13563 to conduct a retrospective review of our existing regulations for the purpose of identifying ways to reduce costs and increase flexibilities under the HIPAA Rules. We discuss our specific burden reduction efforts more fully in the Regulatory Impact Analysis.

This final rule is comprised of four final rules, which have been combined to reduce the impact and number of times certain compliance activities need to be undertaken by the regulated entities.

Legal Authority for the Regulatory Action

The final rule implements changes to the HIPAA Rules under a number of authorities. First, the final rule modifies the Privacy, Security, and Enforcement Rules to strengthen privacy and security protections for health information and to improve enforcement as provided for by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The rule also includes final modifications to the Breach Notification Rule, which will replace an interim final rule originally published in 2009 as required by the HITECH Act. Second, the final rule revises the HIPAA Privacy Rule to increase privacy protections for genetic information as required by the Genetic Information Nondiscrimination Act of 2008 (GINA). Finally, the Department uses its general authority under HIPAA to make a number of changes to the Rules that are intended to increase workability and flexibility, decrease burden, and better harmonize the requirements with those under other Departmental regulations.

ii. Summary of Major Provisions

This omnibus final rule is comprised of the following four final rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act, and certain other modifications to improve the Rules, which were issued as a proposed rule on July 14, 2010. These modifications:

- Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements.
- Strengthen the limitations on the use and disclosure of protected health information for marketing and fundraising purposes, and prohibit the sale of protected health information without individual authorization.
- Expand individuals' rights to receive electronic copies of their health information and to restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full.
- Require modifications to, and redistribution of, a covered entity's notice of privacy practices.
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others.
- Adopt the additional HITECH Act enhancements to the Enforcement Rule not previously adopted in the October 30, 2009, interim final rule (referenced immediately below), such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

2. Final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act, originally published as an interim final rule on October 30, 2009.

3. Final rule on Breach Notification for Unsecured Protected Health Information under the HITECH Act, which replaces the breach notification rule's ''harm'' threshold with a more objective standard and supplants an interim final rule published on August 24, 2009.

4. Final rule modifying the HIPAA Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA) to prohibit most health plans from using or disclosing genetic information for underwriting purposes, which was published as a proposed rule on October 7, 2009.

iii. Costs and Benefits

This final rule is anticipated to have an annual effect on the economy of $100 million or more, making it an economically significant rule under Executive Order 12866. Accordingly, we have prepared a Regulatory Impact Analysis that presents the estimated costs and benefits of the proposed rule. The total cost of compliance with the rule's provisions is estimated to be between $114 million and $225.4 million in the first year of implementation and approximately $14.5 million annually thereafter. Costs associated with the rule include: (i) Costs to HIPAA covered entities of revising and distributing new notices of privacy practices to inform individuals of their rights and how their information is protected; (ii) costs to covered entities related to compliance with breach notification requirements; (iii) costs to a portion of business associates to bring their subcontracts into compliance with business associate agreement requirements; and (iv) costs to a portion of business associates to achieve full compliance with the Security Rule. We summarize these costs in Table 1 below and explain the components and distribution of costs in detail in the Regulatory Impact Analysis.

We are not able to quantify the benefits of the rule due to lack of data and the impossibility of monetizing the value of individuals' privacy and dignity, which we believe will be enhanced by the strengthened privacy and security protections, expanded individual rights, and improved enforcement enabled by the rule. We also believe that some entities affected by the rule will realize cost savings as a result of provisions that simplify and streamline certain requirements, and increase flexibility, under the HIPAA Rules. However, we are unable to quantify such cost savings due to a lack of data. We describe such benefits in the Regulatory Impact Analysis.

TABLE 1—ESTIMATED COSTS OF THE FINAL RULE

Cost element	Approximate number of affected entities	Total cost
Notices of Privacy Practices	700,000 covered entities	$55.9 million.
Breach Notification Requirements	19,000 covered entities	14.5 million.[1]
Business Associate Agreements	250,000–500,000 business associates of covered entities	21 million–42 million.
Security Rule Compliance by Business Associates.	200,000–400,000 business associates of covered entities	22.6 million–113 million.
Total		114 million–225.4 million.

B. Statutory and Regulatory Background

i. HIPAA and the Privacy, Security, and Enforcement Rules

The HIPAA Privacy, Security, and Enforcement Rules implement certain of the Administrative Simplification provisions of title II, subtitle F, of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104–191), which added a new part C to title XI of the Social Security Act (sections 1171–1179 of the Social Security Act, 42 U.S.C. 1320d–1320d–8). The HIPAA Administrative Simplification provisions provided for the establishment of national standards for the electronic transmission of certain health information, such as standards for certain health care transactions conducted electronically and code sets and unique identifiers for health care providers and employers. The HIPAA Administrative Simplification provisions also required the establishment of national standards to protect the privacy and security of personal health information and established civil money penalties for violations of the Administrative Simplification provisions. The Administrative Simplification provisions of HIPAA apply to three types of entities, which are known as ''covered entities'': health care providers who conduct covered health care transactions electronically, health plans, and health care clearinghouses.

The HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164, requires covered entities to have safeguards in place to ensure the privacy of protected health information, sets forth the circumstances under which covered entities may use or disclose an individual's protected health information, and gives individuals rights with respect to their protected health information, including rights to examine and obtain a copy of their health records and to request corrections. Covered entities that engage business associates to work on their behalf must have contracts or other arrangements in place with their business associates to ensure that the business associates safeguard protected health information, and use and disclose the information only as permitted or required by the Privacy Rule.

The HIPAA Security Rule, 45 CFR Part 160 and Subparts A and C of Part 164, applies only to protected health information in electronic form and requires covered entities to implement certain administrative, physical, and technical safeguards to protect this electronic information. Like the Privacy Rule, covered entities must have contracts or other arrangements in place with their business associates that provide satisfactory assurances that the business associates will appropriately safeguard the electronic protected health information they create, receive, maintain, or transmit on behalf of the covered entities.

The HIPAA Enforcement Rule, 45 CFR Part 160, Subparts C–E, establishes rules governing the compliance responsibilities of covered entities with respect to the enforcement process, including the rules governing investigations by the Department, rules governing the process and grounds for establishing the amount of a civil money penalty where a violation of a HIPAA Rule has been found, and rules governing the procedures for hearings and appeals where the covered entity challenges a violation determination.

Since the promulgation of the HIPAA Rules, legislation has been enacted requiring modifications to the Rules. In particular, the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted on February 17, 2009, as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Public Law 111–5, modifies certain provisions of the Social Security Act pertaining to the HIPAA Rules, as well as requires certain modifications to the Rules themselves, to strengthen HIPAA privacy, security, and enforcement. The

[1] The costs associated with breach notification will be incurred on an annual basis. All other costs are expected in the first year of implementation.

Act also provides new requirements for notification of breaches of unsecured protected health information by covered entities and business associates. In addition, the Genetic Information Nondiscrimination Act of 2008 (GINA) calls for changes to the HIPAA Privacy Rule to strengthen privacy protections for genetic information. This final rule implements the modifications required by GINA, as well as most of the privacy, security, and enforcement provisions of the HITECH Act. This final rule also includes certain other modifications to the HIPAA Rules to improve their workability and effectiveness.

ii. The Health Information Technology for Economic and Clinical Health Act

The HITECH Act is designed to promote the widespread adoption and interoperability of health information technology. Subtitle D of title XIII, entitled ''Privacy,'' supports this goal by adopting amendments designed to strengthen the privacy and security protections for health information established by HIPAA. These provisions include extending the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities; requiring that Health Information Exchange Organizations and similar organizations, as well as personal health record vendors that provide services to covered entities, shall be treated as business associates; requiring HIPAA covered entities and business associates to provide for notification of breaches of ''unsecured protected health information''; establishing new limitations on the use and disclosure of protected health information for marketing and fundraising purposes; prohibiting the sale of protected health information; and expanding individuals' rights to access their protected health information, and to obtain restrictions on certain disclosures of protected health information to health plans. In addition, subtitle D adopts provisions designed to strengthen and expand HIPAA's enforcement provisions.

We discuss these statutory provisions in more detail below where we describe section-by-section how this final rule implements the provisions. We do not address in this rulemaking the accounting for disclosures requirement in section 13405 of the Act, which is the subject of a separate proposed rule published on May 31, 2011, at 76 FR 31426, or the penalty distribution methodology requirement in section 13410(c) of the Act, which will be the subject of a future rulemaking.

Since enactment of the HITECH Act a number of steps have been taken to implement the strengthened privacy, security, and enforcement provisions through rulemakings and related actions. On August 24, 2009, the Department published interim final regulations to implement the breach notification provisions at section 13402 of the HITECH Act (74 FR 42740), which were effective September 23, 2009. Similarly, the Federal Trade Commission (FTC) published final regulations implementing the breach notification provisions at section 13407 for personal health record vendors and their third party service providers on August 25, 2009 (74 FR 42962), effective September 24, 2009. For purposes of determining to what information the HHS and FTC breach notification regulations apply, the Department also issued, first on April 17, 2009 (published on April 27, 2009, 74 FR 19006), and then later with its interim final rule, the guidance required by the HITECH Act under 13402(h) specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Additionally, to conform the provisions of the Enforcement Rule to the HITECH Act's tiered and increased civil money penalty structure, which became effective on February 18, 2009, the Department published an interim final rule on October 30, 2009 (74 FR 56123), effective November 30, 2009.

The Department published a notice of proposed rulemaking (NPRM) on July 14, 2010, (75 FR 40868) to implement many of the remaining privacy, security, and enforcement provisions of the HITECH Act. The public was invited to comment on the proposed rule for 60 days following publication. The comment period closed on September 13, 2010. The Department received about 300 comments on the NPRM.

The NPRM proposed to extend the applicability of certain of the Privacy and Security Rules' requirements to the business associates of covered entities, making business associates directly liable for violations of these requirements. Additionally, the NPRM proposed to define a subcontractor as a business associate to ensure any protected health information the subcontractor creates or receives on behalf of the business associate is appropriately safeguarded. The NPRM proposed to establish new limitations on the use and disclosure of protected health information for marketing and fundraising purposes and to prohibit the sale of protected health information without an authorization. The NPRM also proposed to expand an individual's right to obtain an electronic copy of an individual's protected health information, and the right to restrict certain disclosures of protected health information to a health plan for payment or health care operations purposes. In addition, the NPRM proposed to further modify the Enforcement Rule to implement more of the HITECH Act's changes to HIPAA enforcement.

In addition to the proposed modifications to implement the HITECH Act, the NPRM also proposed certain other modifications to the HIPAA Rules. The NPRM proposed to permit the use of compound authorizations for conditioned and unconditioned research activities and requested comment regarding permitting authorizations for future research. Additionally, the NPRM proposed to modify the Privacy Rule's application to the individually identifiable health information of decedents and to permit covered entities that obtain the agreement of a parent to provide proof of immunization without written authorization to schools that are required to have such information.

iii. The Genetic Information Nondiscrimination Act

The Genetic Information Nondiscrimination Act of 2008 (''GINA''), Pub. L. 110–233, 122 Stat. 881, prohibits discrimination based on an individual's genetic information in both the health coverage (Title I) and employment (Title II) contexts. In addition to the nondiscrimination provisions, section 105 of Title I of GINA contains new privacy protections for genetic information, which require the Secretary of HHS to revise the Privacy Rule to clarify that genetic information is health information and to prohibit group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.

On October 7, 2009, the Department published a proposed rule to strengthen the privacy protections for genetic information under the HIPAA Privacy Rule by implementing the protections for genetic information required by GINA and making related changes to the Rule. The 60-day public comment period for the proposed rule closed on December 7, 2009. The Department received about 25 comments on the proposed rule.

II. Overview of the Final Rule

In this final rule the Department finalizes the modifications to the HIPAA Privacy, Security, and Enforcement Rules to implement many of the

privacy, security, and enforcement provisions of the HITECH Act and make other changes to the Rules; modifies the Breach Notification Rule; finalizes the modifications to the HIPAA Privacy Rule to strengthen privacy protections for genetic information; and responds to the public comments received on the proposed and interim final rules. Section III below describes the effective and compliance dates of the final rule. Section IV describes the changes to the HIPAA Privacy, Security, and Enforcement Rules under the HITECH Act and other modifications that were proposed in July 2010, as well as the modifications to the Enforcement Rule under the HITECH Act that were addressed in the interim final rule published in October 2009. Section V describes the changes to the Breach Notification Rule. Section VI discusses the changes to the HIPAA Privacy Rule to strengthen privacy protections for genetic information.

III. Effective and Compliance Dates

With respect to the HITECH Act requirements, section 13423 of the Act provides that the provisions in subtitle D took effect one year after enactment, i.e., on February 18, 2010, except as specified otherwise. However, there are a number of exceptions to this general rule. For example, the tiered and increased civil money penalty provisions of section 13410(d) were effective for violations occurring after the date of enactment, and sections 13402 and 13407 of the Act regarding breach notification required interim final rules within 180 days of enactment, with effective dates 30 days after the publication of such rules. Other provisions of the Act have later effective dates. For example, the provision at section 13410(a)(1) of the Act providing that the Secretary's authority to impose a civil money penalty will only be barred to the extent a criminal penalty has been imposed, rather than in cases in which the offense in question merely constitutes an offense that is criminally punishable, became effective for violations occurring on or after February 18, 2011. The discussion below generally pertains to the statutory provisions that became effective on February 18, 2010, or, in a few cases, on a later date.

Proposed Rule

We proposed that covered entities and business associates would have 180 days beyond the effective date of the final rule to come into compliance with most of the rule's provisions. We believed that a 180-day compliance period would suffice for future modifications to the HIPAA Rules, and we proposed to add a provision at § 160.105 to address the compliance date generally for implementation of new or modified standards in the HIPAA Rules. We proposed that § 160.105 would provide that with respect to new standards or implementation specifications or modifications to standards or implementation specifications in the HIPAA Rules, except as otherwise provided, covered entities and business associates would be required to comply with the applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change. For future modifications to the HIPAA Rules necessitating a longer compliance period, we would specify a longer period in the regulatory text. Finally, we proposed to retain the compliance date provisions at §§ 164.534 and 164.318, which provide the compliance dates of April 14, 2003, and April 20, 2005, for initial implementation of the HIPAA Privacy and Security Rules, respectively, for historical purposes only.

Overview of Public Comments

Most of the comments addressing the proposed compliance periods as outlined above fell into three categories. First, several commenters supported the proposed compliance timelines and agreed that 180 days is sufficient time for covered entities, business associates, and subcontractors of all sizes to come into compliance with the final rule. Second, a few commenters supported the proposed 180-day compliance period, but expressed concern that the Department may wish to extend the 180-day compliance period in the future, if it issues modifications or new provisions that require a longer compliance period. Third, several commenters requested that the Department extend the 180-day compliance period both with regard to the modifications contained in this final rule and with regard to the more general proposed compliance deadline, as they believe 180 days is an insufficient amount of time for covered entities, business associates, and subcontractors to come into compliance with the modified rules, particularly with regard to changes in technology.

Final Rule

The final rule is effective on March 26, 2013. Covered entities and business associates of all sizes will have 180 days beyond the effective date of the final rule to come into compliance with most of the final rule's provisions, including the modifications to the Breach Notification Rule and the changes to the HIPAA Privacy Rule under GINA. We understand that some covered entities, business associates, and subcontractors remain concerned that a 180-day period does not provide sufficient time to come into compliance with the modifications. However, we believe not only that providing a 180-day compliance period best comports with section 1175(b)(2) of the Social Security Act, 42 U.S.C. 1320d–4, and our implementing provision at § 160.104(c)(1), which require the Secretary to provide at least a 180-day period for covered entities to comply with modifications to standards and implementation specifications in the HIPAA Rules, but also that providing a 180-day compliance period best protects the privacy and security of patient information, in accordance with the goals of the HITECH Act.

In addition, to make clear to the industry our expectation that going forward we will provide a 180-day compliance date for future modifications to the HIPAA Rules, we adopt the provision we proposed at § 160.105, which provides that with respect to new or modified standards or implementation specifications in the HIPAA Rules, except as otherwise provided, covered entities and business associates must comply with the applicable new or modified standards or implementation specifications no later than 180 days from the effective date of any such change. In cases where a future modification necessitates a longer compliance period, the Department will expressly provide for one, as it has done in this rulemaking with respect to the time permitted for business associate agreements to be modified.

For the reasons proposed, the final rule also retains the compliance date provisions at §§ 164.534 and 164.318, which provide the compliance dates of April 14, 2003, and April 20, 2005, for initial implementation of the HIPAA Privacy and Security Rules, respectively. We note that § 160.105 regarding the compliance date of new or modified standards or implementation specifications does not apply to modifications to the provisions of the HIPAA Enforcement Rule, because such provisions are not standards or implementation specifications (as the terms are defined at § 160.103). Such provisions are in effect and apply at the time the final rule becomes effective or as otherwise specifically provided. In addition, as explained above, our general rule for a 180-day compliance period for new or modified standards would not apply where we expressly provide a different compliance period in

the regulation for one or more provisions. For purposes of this rule, the 180-day compliance period would not govern the time period required to modify those business associate agreements that qualify for the longer transition period in § 164.532, as we discuss further below.

Finally, the provisions of section 13402(j) of the HITECH Act apply to breaches of unsecured protected health information discovered on or after September 23, 2009, the date of the publication of the interim final rule. Thus, during the 180 day period before compliance with this final rule is required, covered entities and business associates are still required to comply with the breach notification requirements under the HITECH Act and must continue to comply with the requirements of the interim final rule. We believe that this transition period provides covered entities and business associates with adequate time to come into compliance with the revisions in this final rule and at the same time to continue to fulfill their breach notification obligations under the HITECH Act.

IV. Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the HITECH Act; Other Modifications to the HIPAA Rules

The discussion below provides a section-by-section description of the final rule, as well as responds to public comments where substantive comments were received regarding particular provisions.

A. Subparts A and B of Part 160: Statutory Basis and Purpose, Applicability, Definitions, and Preemption of State Law

Subpart A of Part 160 of the HIPAA Rules contains general provisions that apply to all of the HIPAA Rules. Subpart B of Part 160 contains the regulatory provisions implementing HIPAA's preemption provisions. We proposed to amend a number of these provisions. Some of the proposed, and now final, changes are necessitated by the statutory changes made by the HITECH Act and GINA, while others are of a technical or conforming nature.

1. Subpart A—General Provisions, Section 160.101—Statutory Basis and Purpose

This section sets out the statutory basis and purpose of the HIPAA Rules. We proposed and include in this final rule a technical change to include references to the provisions of GINA and the HITECH Act upon which most of the regulatory changes below are based.

2. Subpart A—General Provisions, Section 160.102—Applicability

This section sets out to whom the HIPAA Rules apply. We proposed to add and include in this final rule a new paragraph (b) to make clear, consistent with the HITECH Act, that certain of the standards, requirements, and implementation specifications of the subchapter apply to business associates.

3. Subpart A—General Provisions, Section 160.103—Definitions

Section 160.103 contains definitions of terms that appear throughout the HIPAA Rules. The final rule modifies a number of these definitions to implement the HITECH Act and make other needed changes.

a. Definition of ''Business Associate''

The HIPAA Privacy and Security Rules permit a covered entity to disclose protected health information to a business associate, and allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, provided the covered entity obtains satisfactory assurances in the form of a contract or other arrangement that the business associate will appropriately safeguard the information. The HIPAA Rules define ''business associate'' generally to mean a person who performs functions or activities on behalf of, or certain services for, a covered entity that involve the use or disclosure of protected health information. We proposed a number of modifications to the definition of ''business associate'' to implement the HITECH Act, to conform the term to the statutory provisions of the Patient Safety and Quality Improvement Act of 2005 (PSQIA), 42 U.S.C. 299b–21, et seq., and to make other changes to the definition.

i. Inclusion of Patient Safety Organizations

Proposed Rule

We proposed to add patient safety activities to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship. PSQIA, at 42 U.S.C. 299b–22(i)(1), provides that Patient Safety Organizations (PSOs) must be treated as business associates when applying the Privacy Rule. PSQIA provides for the establishment of PSOs to receive reports of patient safety events or concerns from providers and provide analyses of events to reporting providers. A reporting provider may be a HIPAA covered entity and, thus, information reported to a PSO may include protected health information that the PSO may analyze on behalf of the covered provider. The analysis of such information is a patient safety activity for purposes of PSQIA and the Patient Safety Rule, 42 CFR 3.10, et seq. While the HIPAA Rules as written would treat a PSO as a business associate when the PSO was performing quality analyses and other activities on behalf of a covered health care provider, we proposed this change to the definition of ''business associate'' to more clearly align the HIPAA and Patient Safety Rules.

Overview of Public Comment

Commenters on this topic supported the express inclusion of patient safety activities within the definition of ''business associate.''

Final Rule

The final rule adopts the proposed modification.

ii. Inclusion of Health Information Organizations (HIO), E-Prescribing Gateways, and Other Persons That Facilitate Data Transmission; as Well as Vendors of Personal Health Records

Proposed Rule

Section 13408 of the HITECH Act provides that an organization, such as a Health Information Exchange Organization, E-prescribing Gateway, or Regional Health Information Organization, that provides data transmission of protected health information to a covered entity (or its business associate) and that requires access on a routine basis to such protected health information must be treated as a business associate for purposes of the Act and the HIPAA Privacy and Security Rules. Section 13408 also provides that a vendor that contracts with a covered entity to allow the covered entity to offer a personal health record to patients as part of the covered entity's electronic health record shall be treated as a business associate. Section 13408 requires that such organizations and vendors enter into a written business associate contract or other arrangement with the covered entity in accordance with the HIPAA Rules.

In accordance with the Act, we proposed to modify the definition of ''business associate'' to explicitly designate these persons as business associates. Specifically, we proposed to include in the definition: (1) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect

to protected health information to a covered entity and that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity.

We proposed to refer to ''Health Information Organization'' in the NPRM rather than ''Health Information Exchange Organization'' as used in the Act because it is our understanding that ''Health Information Organization'' is the more widely recognized and accepted term to describe an organization that oversees and governs the exchange of health-related information among organizations.[2] The Act also specifically refers to Regional Health Information Organizations; however, we did not believe the inclusion of the term in the definition of ''business associate'' was necessary as a Regional Health Information Organization is simply a Health Information Organization that governs health information exchange among organizations within a defined geographic area.[3] Further, the specific terms of ''Health Information Organization'' and ''E-prescribing Gateway'' were included as merely illustrative of the types of organizations that would fall within this paragraph of the definition of ''business associate.'' We requested comment on the use of these terms within the definition and whether additional clarifications or additions were necessary.

Section 13408 also provides that the data transmission organizations that the Act requires to be treated as business associates are those that require access to protected health information on a routine basis. Conversely, data transmission organizations that do not require access to protected health information on a routine basis would not be treated as business associates. This is consistent with our prior interpretation of the definition of ''business associate,'' through which we have stated that entities that act as mere conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis are not business associates. See *http://www.hhs.gov/ocr/privacy/hipaa/faq/providers/business/245.html*. In contrast, entities that manage the exchange of protected health information through a network, including providing record locator services and performing various oversight and governance functions for electronic health information exchange, have more than ''random'' access to protected health information and thus, would fall within the definition of ''business associate.''

Overview of Public Comments

Commenters generally supported the inclusion of Health Information Organizations, personal health record vendors, and similar entities in the definition of ''business associate.'' However, commenters sought various clarifications as discussed below.

Commenters generally supported use of the term Health Information Organization in lieu of more restrictive terms, such as Regional Health Information Organization. Some commenters suggested that the term Health Information Organization be defined, so as to avoid confusion as the industry develops, and suggested various alternatives for doing so. Several commenters recommended that the Office for Civil Rights (OCR) maintain a Web site link that lists current terms for entities that OCR considers to be Health Information Organizations.

Other commenters requested clarification on what it means to have ''access on a routine basis'' to protected health information for purposes of the definition and determining whether certain entities are excluded as mere conduits. For example, commenters asked whether the definition of business associate would include broadband suppliers or internet service providers, vendors that only have the potential to come into contact with protected health information, or entities contracted on a contingency basis that may at some point in the future have access to protected health information. Several document storage companies argued that entities like theirs should be characterized as conduits, as they do not view the protected health information they store.

Several commenters sought clarification regarding when personal health record vendors would be considered business associates. For example, commenters asked whether personal health record vendors would be business associates when the vendor provided the personal health record in collaboration with the covered entity, when the personal health record is linked to a covered entity's electronic health record, or when the personal health record is offered independently to the individual, among other scenarios. One commenter suggested that a vendor offering a personal health record to a patient on behalf of a covered entity only acts as a conduit because there is no access by the vendor to protected health information; another commenter suggested that personal health record vendors be business associates only when they have routine access to protected health information.

Final Rule

The final rule adopts the language that expressly designates as business associates: (1) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity.

We decline to provide a definition for Health Information Organization. We recognize that the industry continues to develop and thus the type of entities that may be considered Health Information Organizations continues to evolve. For this reason, we do not think it prudent to include in the regulation a specific definition at this time. We anticipate continuing to issue guidance in the future on our web site on the types of entities that do and do not fall within the definition of business associate, which can be updated as the industry evolves.

Regarding what it means to have ''access on a routine basis'' to protected health information with respect to determining which types of data transmission services are business associates versus mere conduits, such a determination will be fact specific based on the nature of the services provided and the extent to which the entity needs access to protected health information to perform the service for the covered entity. The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. As we have stated in prior guidance, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law. For example, a telecommunications company may have occasional, random access to protected health information when it reviews whether the data transmitted over its network is arriving

[2] Department of Health and Human Services Office of the National Coordinator for Health Information Technology, The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology: Defining Key Health Information Terms, Pg. 24 (2008).

[3] *Id.* at 25.

at its intended destination. Such occasional, random access to protected health information would not qualify the company as a business associate. In contrast, an entity that requires access to protected health information in order to perform a service for a covered entity, such as a Health Information Organization that manages the exchange of protected health information through a network on behalf of covered entities through the use of record locator services for its participants (and other services), is not considered a conduit and, thus, is not excluded from the definition of business associate. We intend to issue further guidance in this area as electronic health information exchange continues to evolve.

We note that the conduit exception is limited to transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission. In contrast, an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information. We recognize that in both situations, the entity providing the service to the covered entity has the opportunity to access the protected health information. However, the difference between the two situations is the transient versus persistent nature of that opportunity. For example, a data storage company that has access to protected health information (whether digital or hard copy) qualifies as a business associate, even if the entity does not view the information or only does so on a random or infrequent basis. Thus, document storage companies maintaining protected health information on behalf of covered entities are considered business associates, regardless of whether they actually view the information they hold. To help clarify this point, we have modified the definition of ''business associate'' to generally provide that a business associate includes a person who ''creates, receives, *maintains,* or transmits'' (emphasis added) protected health information on behalf of a covered entity.

Several commenters sought clarification on when a personal health record vendor would be providing a personal health record ''on behalf of'' a covered entity and thus, would be a business associate for purposes of the HIPAA Rules. As with data transmission services, determining whether a personal health record vendor is a business associate is a fact specific determination. A personal health record vendor is not a business associate of a covered entity solely by virtue of entering into an interoperability relationship with a covered entity. For example, when a personal health record vendor and a covered entity establish the electronic means for a covered entity's electronic health record to send protected health information to the personal health record vendor pursuant to the individual's written authorization, it does not mean that the personal health record vendor is offering the personal health record on behalf of the covered entity, even if there is an agreement between the personal health record vendor and the covered entity governing the exchange of data (such as an agreement specifying the technical specifications for exchanging of data or specifying that such data shall be kept confidential). In contrast, when a covered entity hires a vendor to provide and manage a personal health record service the covered entity wishes to offer its patients or enrollees, and provides the vendor with access to protected health information in order to do so, the personal health record vendor is a business associate.

A personal health record vendor may offer personal health records directly to individuals and may also offer personal health records on behalf of covered entities. In such cases, the personal health record vendor is only subject to HIPAA as a business associate with respect to personal health records that are offered to individuals on behalf of covered entities.

We also clarify that, contrary to one commenter's suggestion, a personal health record vendor that offers a personal health record to a patient on behalf of a covered entity does not act merely as a conduit. Rather, the personal health record vendor is maintaining protected health information on behalf of the covered entity (for the benefit of the individual). Further, a personal health record vendor that operates a personal health record on behalf of a covered entity is a business associate if it has access to protected health information, regardless of whether the personal health record vendor actually exercises this access. We believe the revisions to the definition of ''business associate'' discussed above clarify these points. As with other aspects of the definition of ''business associate,'' we intend to provide future guidance on when a personal health record vendor is a business associate for purposes of the HIPAA Rules.

Response to Other Public Comments

Comment: One commenter recommended that the term ''person'' used in describing who provides transmission services to a covered entity be clarified to apply also to entities and organizations.

Response: The term ''person'' as defined at § 160.103 includes entities as well as natural persons.

Comment: One commenter asked whether subcontractors that support business associates with personal health record related functions are subject to the breach notification requirements under the HIPAA Breach Notification Rule or that of the FTC.

Response: As discussed below, a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate, including with respect to personal health record functions, is a HIPAA business associate and thus, is subject to the HIPAA Breach Notification Rule and not that of the FTC. The analysis of whether a subcontractor is acting on behalf of a business associate is the same analysis as discussed above with respect to whether a business associate is acting on behalf of a covered entity.

iii. Inclusion of Subcontractors

Proposed Rule

We proposed in the definition of ''business associate'' to provide that subcontractors of a covered entity, i.e., those persons that perform functions for or provide services to a business associate other than in the capacity as a member of the business associate's workforce, are also business associates to the extent that they require access to protected health information. We also proposed to define ''subcontractor'' in § 160.103 as a person who acts on behalf of a business associate, other than in the capacity of a member of the workforce of such business associate. Even though we used the term ''subcontractor,'' which implies there is a contract in place between the parties, the definition would apply to an agent or other person who acts on behalf of the business associate, even if the business associate has failed to enter into a business associate contract with the person. We requested comment on the use of the term ''subcontractor'' and its proposed definition.

The intent of the proposed extension of the Rules to subcontractors was to avoid having privacy and security protections for protected health information lapse merely because a function is performed by an entity that is a subcontractor rather than an entity

with a direct relationship with a covered entity. Allowing such a lapse in privacy and security protections could allow business associates to avoid liability imposed upon them by sections 13401 and 13404 of the Act. Further, applying HIPAA privacy and security requirements directly to subcontractors also ensures that the privacy and security protections of the HIPAA Rules extend beyond covered entities to those entities that create or receive protected health information in order for the covered entity to perform its health care functions. Therefore, we proposed that downstream entities that work at the direction of or on behalf of a business associate and handle protected health information would also be required to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary business associate, and likewise would incur liability for acts of noncompliance. This proposed modification would not require the covered entity to have a contract with the subcontractor; rather, the obligation would remain on each business associate to obtain satisfactory assurances in the form of a written contract or other arrangement that a subcontractor will appropriately safeguard protected health information. For example, if a business associate, such as a third party administrator, hires a company to handle document and media shredding to securely dispose of paper and electronic protected health information, then the shredding company would be directly required to comply with the applicable requirements of the HIPAA Security Rule (e.g., with respect to proper disposal of electronic media) and the Privacy Rule (e.g., with respect to limiting its uses and disclosures of the protected health information in accordance with its contract with the business associate).

Overview of Public Comments

While some commenters generally supported extending the business associate provisions of the Rules to subcontractors, many opposed such an extension arguing, among other things, that doing so was not the intent of Congress and beyond the statutory authority of the Department, that confusion may ensue with covered entities seeking to establish direct business associate contracts with subcontractors or prohibiting business associates from establishing subcontractor relationships altogether, and/or that creating direct liability for subcontractors will discourage such entities from operating and participating in the health care industry. Some commenters asked how far down the ''chain'' of subcontractors do the HIPAA Rules apply—i.e., do the Rules apply only to the first tier subcontractor or to all subcontractors down the chain.

In response to our request for comment on this issue, several commenters were concerned that use of the term subcontractor was confusing and instead suggested a different term be used, such as business associate contractor or downstream business associate, to avoid confusion between primary business associates of a covered entity and subcontractors. Other commenters suggested changes to the definition of subcontractor itself to better clarify the scope of the definition.

Several commenters requested specific guidance on who is and is not a subcontractor under the definitions of ''business associate'' and ''subcontractor.'' For example, one commenter asked whether an entity that shreds documents for a business associate for the business associate's activities and not for the covered entity, would qualify as a subcontractor. Another commenter asked whether disclosures by a business associate of protected health information for its own management and administration or legal needs creates a subcontractor relationship. Other commenters recommended that subcontractors without routine access to protected health information, or who do not access protected health information at all for their duties, not be considered business associates.

Final Rule

The final rule adopts the proposal to apply the business associate provisions of the HIPAA Rules to subcontractors and thus, provides in the definition of ''business associate'' that a business associate includes a ''subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.'' In response to comments, we clarify the definition of ''subcontractor'' in § 160.103 to provide that subcontractor means: ''a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.'' Thus, a subcontractor is a person to whom a business associate has delegated a function, activity, or service the business associate has agreed to perform for a covered entity or business associate. A subcontractor is then a business associate where that function, activity, or service involves the creation, receipt, maintenance, or transmission of protected health information. We also decline to replace the term ''subcontractor'' with another, as we were not persuaded by any of the alternatives suggested by commenters (e.g., ''business associate contractor,'' ''downstream business associate,'' or ''downstream entity'').

We disagree with the commenters that suggested that applying the business associate provisions of the HIPAA Rules to subcontractors is beyond the Department's statutory authority. In the HITECH Act, Congress created direct liability under the HIPAA Privacy and Security Rules for persons that are not covered entities but that create or receive protected health information in order for a covered entity to perform its health care functions, to ensure individuals' personal health information remains sufficiently protected in the hands of these entities. As stated in the NPRM, applying the business associate provisions only to those entities that have a direct relationship with a covered entity does not achieve that intended purpose. Rather, it allows privacy and security protections for protected health information to lapse once a subcontractor is enlisted to assist in performing a function, activity, or service for the covered entity, while at the same time potentially allowing certain primary business associates to avoid liability altogether for the protection of the information the covered entity has entrusted to the business associate. Further, section 13422 of the HITECH Act provides that each reference in the Privacy subtitle of the Act to a provision of the HIPAA Rules refers to such provision as in effect on the date of enactment of the Act *or to the most recent update of such provision* (emphasis added). Thus, the Act does not bar the Department from modifying definitions of terms in the HIPAA Rules to which the Act refers. Rather, the statute expressly contemplates that modifications to the terms may be necessary to carry out the provisions of the Act or for other purposes.

Further, we do not agree that covered entities will be confused and seek to establish direct business associate contracts with subcontractors or will prohibit business associates from engaging subcontractors to perform functions or services that require access to protected health information. The final rule makes clear that a covered entity is not required to enter into a contract or other arrangement with a business associate that is a subcontractor. See §§ 164.308(b)(1) and 164.502(e)(1)(i). In addition, as commenters did not present direct evidence to the contrary, we do not believe that covered entities will begin

prohibiting business associates from engaging subcontractors as a result of the final rule, in cases where they were not doing so before. Rather, we believe that making subcontractors directly liable for violations of the applicable provisions of the HIPAA Rules will help to alleviate concern on the part of covered entities that protected health information is not adequately protected when provided to subcontractors.

The Department also believes that the privacy and security protections for an individual's personal health information and associated liability for noncompliance with the Rules should not lapse beyond any particular business associate that is a subcontractor. Thus, under the final rule, covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far ''down the chain'' the information flows. This ensures that individuals' health information remains protected by all parties that create, receive, maintain, or transmit the information in order for a covered entity to perform its health care functions. For example, a covered entity may contract with a business associate (contractor), the contractor may delegate to a subcontractor (subcontractor 1) one or more functions, services, or activities the business associate has agreed to perform for the covered entity that require access to protected health information, and the subcontractor may in turn delegate to another subcontractor (subcontractor 2) one or more functions, services, or activities it has agreed to perform for the contractor that require access to protected health information, and so on. Both the contractor and all of the subcontractors are business associates under the final rule to the extent they create, receive, maintain, or transmit protected health information.

With respect to requests for specific guidance on who is and is not a subcontractor, we believe the above changes to the definition provide further clarity. We also provide the following in response to specific comments. Disclosures by a business associate pursuant to § 164.504(e)(4) and its business associate contract for *its own* management and administration or legal responsibilities do not create a business associate relationship with the recipient of the protected health information because such disclosures are made outside of the entity's role as a business associate. However, for such disclosures that are not required by law, the Rule requires that the business associate obtain reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and the person notifies the business associate of any instances of which it is aware that the confidentiality of the information has been breached. See § 164.504(e)(4)(ii)(B).

In contrast, disclosures of protected health information by the business associate to a person who will assist the business associate in performing a function, activity, or service for a covered entity or another business associate may create a business associate relationship depending on the circumstances. For example, an entity hired by a business associate to appropriately dispose of documents that contain protected health information is also a business associate and subject to the applicable provisions of the HIPAA Rules. If the documents to be shredded do not contain protected health information, then the entity is not a business associate. We also clarify that the same interpretations that apply to determining whether a first tier contractor is a business associate also apply to determining whether a subcontractor is a business associate. Thus, our interpretation of who is and is not excluded from the definition of business associate as a conduit also applies in the context of subcontractors as well. We refer readers to the above discussion regarding transmission services and conduits.

iv. Exceptions to Business Associate

Proposed Rule

Sections 164.308(b)(2) and 164.502(e)(1)(ii) of the HIPAA Rules currently describe certain circumstances, such as when a covered entity discloses protected health information to a health care provider concerning the treatment of an individual, in which a covered entity is not required to enter into a business associate contract or other arrangement with the recipient of the protected health information. We proposed to move these provisions to the definition of ''business associate'' itself as exceptions to make clear that the Department does not consider the recipients of the protected health information in these circumstances to be business associates. The movement of these exceptions also was intended to help clarify that a person or an entity is a business associate if the person or entity meets the definition of ''business associate,'' even if a covered entity, or business associate with respect to a subcontractor, fails to enter into the required business associate contract with the person or entity.

Final Rule

The Department did not receive substantive public comment on this proposal. The final rule includes the exceptions within the definition of ''business associate.''

v. Technical Changes to the Definition

Proposed Rule

For clarity and consistency, we also proposed to change the term ''individually identifiable health information'' in the current definition of ''business associate'' to ''protected health information,'' since a business associate has no obligation under the HIPAA Rules with respect to individually identifiable health information that is not protected health information.

Final Rule

The Department did not receive substantive public comment on this proposal. The final rule adopts the proposed modification to the definition. Additionally, as indicated above, we have revised the definition of business associate to clarify that a business associate includes an entity that ''creates, receives, maintains, or transmits'' protected health information on behalf of a covered entity. This change is intended to make the definition more consistent with language at § 164.308(b) of the Security Rule and § 164.502(e) of the Privacy Rule, as well as to clarify that entities that maintain or store protected health information on behalf of a covered entity are business associates, even if they do not actually view the protected health information.

vi. Response to Other Public Comments

Comment: One commenter suggested that some covered entities do not treat third party persons that handle protected health information onsite as a business associate.

Response: A covered entity may treat a contractor who has his or her duty station onsite at a covered entity and who has more than incidental access to protected health information as either a member of the covered entity's workforce or as a business associate for purposes of the HIPAA Rules.

Comment: A few commenters asked for confirmation that researchers are not considered business associates. In addition, the Secretary's Advisory

Committee on Human Research Protections, in its November 23, 2010, letter to the Secretary providing comments on the NPRM, asked the Department to confirm that outsourced research review, approval, and continuing oversight functions (such as through using an external or independent Institutional Review Board) similarly do not give rise to a business associate relationship.

Response: A person or entity is a business associate only in cases where the person or entity is conducting a function or activity regulated by the HIPAA Rules on behalf of a covered entity, such as payment or health care operations, or providing one of the services listed in the definition of ''business associate,'' and in the performance of such duties the person or entity has access to protected health information. Thus, an external researcher is not a business associate of a covered entity by virtue of its research activities, even if the covered entity has hired the researcher to perform the research. See *http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/239.html*. Similarly, an external or independent Institutional Review Board is not a business associate of a covered entity by virtue of its performing research review, approval, and continuing oversight functions.

However, a researcher may be a business associate if the researcher performs a function, activity, or service for a covered entity that does fall within the definition of business associate, such as the health care operations function of creating a de-identified or limited data set for the covered entity. See paragraph (6)(v) of the definition of ''health care operations.'' Where the researcher is also the intended recipient of the de-identified data or limited data set, the researcher must return or destroy the identifiers at the time the business associate relationship to create the data set terminates and the researcher now wishes to use the de-identified data or limited data set (subject to a data use agreement) for a research purpose.

Comment: A few commenters asked for clarification as to whether the business associate provisions applied to banking and financial institutions. Commenters sought clarification as to whether the exemption at § 1179 of the HIPAA statute for financial institutions was applicable to subcontractors.

Response: This final rule is not intended to affect the status of financial institutions with respect to whether they are business associates. The HIPAA Rules, including the business associate provisions, do not apply to banking and financial institutions with respect to the payment processing activities identified in § 1179 of the HIPAA statute, for example, the activity of cashing a check or conducting a funds transfer. Section 1179 of HIPAA exempts certain activities of financial institutions from the HIPAA Rules, to the extent that these activities constitute authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments for health care or health plan premiums. However, a banking or financial institution may be a business associate where the institution performs functions above and beyond the payment processing activities identified above on behalf of a covered entity, such as performing accounts receivable functions on behalf of a health care provider.

We clarify that our inclusion of subcontractors in the definition of business associate does not impact the exclusion of financial institutions from the definition of ''business associates'' when they are only conducting payment processing activities that fall under § 1179 of the HIPAA statute. Accordingly, a business associate need not enter into a business associate agreement with a financial institution that is solely conducting payment activities that are excluded under § 1179.

Comment: One commenter sought clarification of the status of a risk management group or malpractice insurance company that receives protected health information when contracted with a covered entity to mitigate the covered entity's risk and then contracts with legal groups to represent the covered entity during malpractice claims.

Response: A business associate agreement is not required where a covered entity purchases a health plan product or other insurance, such as medical liability insurance, from an insurer. However, a business associate relationship could arise if the insurer is performing a function on behalf of, or providing services to, the covered entity that does not directly relate to the provision of insurance benefits, such as performing risk management or assessment activities or legal services for the covered entity, that involve access to protected health information.

b. Definition of ''Electronic Media''

Proposed Rule

The term ''electronic media'' was originally defined in the Transactions and Code Sets Rule issued on August 17, 2000 (65 FR 50312) and was included in the definitions at § 162.103. That definition was subsequently revised and moved to § 160.103. The purpose of that revision was to clarify that the physical movement of electronic media from place to place is not limited to magnetic tape, disk, or compact disk, so as to allow for future technological innovation. We further clarified that transmission of information not in electronic form before the transmission (e.g., paper or voice) is not covered by this definition. See 68 FR 8339, Feb. 20, 2003.

In the NPRM, we proposed to revise the definition of ''electronic media'' in the following ways. First, we proposed to revise paragraph (1) of the definition to replace the term ''electronic storage media'' with ''electronic storage material'' to conform the definition of ''electronic media'' to its current usage, as set forth in the National Institute for Standards and Technology (NIST) ''Guidelines for Media Sanitization'' (*Definition of Medium,* NIST SP 800–88, Glossary B, p. 27 (2006)). The NIST definition, which was updated subsequent to the issuance of the Privacy and Security Rules, was developed in recognition of the likelihood that the evolution of the development of new technology would make use of the term ''electronic storage media'' obsolete in that there may be ''storage material'' other than ''media'' that house electronic data. Second, we proposed to add to paragraph (2) of the definition of ''electronic media'' a reference to intranets, to clarify that intranets come within the definition. Third, we proposed to change the word ''because'' to ''if'' in the final sentence of paragraph (2) of the definition of ''electronic media.'' The definition assumed that no transmissions made by voice via telephone existed in electronic form before transmission; the evolution of technology has made this assumption obsolete since some voice technology is digitally produced from an information system and transmitted by phone.

Overview of Public Comments

The Department received comments in support of the revised definition and the flexibility created to account for later technological developments. Certain other commenters raised concerns that changes to the definition could have unintended impacts when applied to the administrative transaction and code set requirements. One commenter specifically supported the change in language from ''because'' to ''if,'' noting the distinction was important to provide protection for digital audio recordings containing protected health information. One commenter suggested including the

word ''immediately'' in the final sentence of paragraph (2) to indicate that fax transmissions are excluded from the definition of electronic media if the information being exchanged did not exist in electronic form *immediately* before the transmission. Several commenters sought clarification as to whether data that is retained in office machines, such as facsimiles and photocopiers, is subject to the Privacy and Security Rules.

Final Rule

The final rule adopts the definition as proposed with two additional modifications. First, in paragraph (2) we remove the parenthetical language referring to ''wide open'' with respect to the Internet and ''using Internet technology to link a business with information accessible only to collaborating parties'' with respect to extranets and intranets. The parenthetical language initially helped clarify what was intended by key words within the definition. As these key words have become more generally understood and guidance has become available through the NIST regarding specific key terms, such as intranet, extranet, and internet, (see, for example, NIST IR 7298 Revision 1, Glossary of Key Information Security Terms, February 2011, available at *http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf*), we believe the parenthetical language is no longer helpful. Second, we do accept the recommendation that we alter the language in paragraph (2) to include the word ''immediately,'' to exclude transmissions when the information exchanged did not exist in electronic form immediately before transmission. This modification clarifies that a facsimile machine accepting a hardcopy document for transmission is not a covered transmission even though the document may have originated from printing from an electronic file.

We do not believe these changes will have unforeseen impacts on the application of the term in the transactions and code sets requirements at Part 162.

In response to commenters' concerns that photocopiers, facsimiles, and other office machines may retain electronic data, potentially storing protected health information when used by covered entities or business associates, we clarify that protected health information stored, whether intentionally or not, in photocopier, facsimile, and other devices is subject to the Privacy and Security Rules. Although such devices are not generally relied upon for storage and access to stored information, covered entities and business associates should be aware of the capabilities of these devices to store protected health information and must ensure any protected health information stored on such devices is appropriately protected and secured from inappropriate access, such as by monitoring or restricting physical access to a photocopier or a fax machine that is used for copying or sending protected health information. Further, before removal of the device from the covered entity or business associate, such as at the end of the lease term for a photocopier machine, proper safeguards should be followed to remove the electronic protected health information from the media.

c. Definition of ''Protected Health Information''

Proposed Rule

For consistency with the proposed modifications to the period of protection for decedent information at § 164.502(f) (discussed below), the Department proposed to modify the definition of ''protected health information'' at § 160.103 to provide that the Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

Overview of Public Comment

The public comments received on this proposal are discussed and responded to below in the section describing the modifications to § 164.502(f).

Final Rule

For the reasons stated in the section regarding § 164.502(f), the final rule adopts the proposed modification to the definition of ''protected health information.''

d. Definition of ''State''

Proposed Rule

The HITECH Act at section 13400 includes a definition of ''State'' to mean ''each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.'' This definition varies from paragraph (2) of the HIPAA definition of ''State'' at § 160.103, which does not include reference to American Samoa and the Northern Mariana Islands. Thus, for consistency with the definition applied to the HIPAA Rules by the HITECH Act, we proposed to add reference to American Samoa and the Commonwealth of the Northern Mariana Islands in paragraph (2) of the definition of ''State'' at § 160.103.

Final Rule

The Department did not receive substantive public comment on this proposal and the final rule adopts the proposed modifications to the definition of ''State.''

e. Other Changes to the Definitions in Section 160.103

In addition to the changes discussed above, the final rule makes the following changes as proposed in the NPRM to various definitions in § 160.103:

(1) Relocates the definitions of ''administrative simplification provision,'' ''ALJ,'' ''civil money penalty,'' ''respondent,'' and ''violation or violate'' from § 160.302 to § 160.103 for ease of reference;

(2) Adds a reference to sections 13400–13424 of the HITECH Act to the definition of ''administrative simplification provision'';

(3) Removes a comma from the definition of ''disclosure'' inadvertently inserted into the definition in a prior rulemaking;

(4) Replaces the term ''individually identifiable health information'' with ''protected health information'' in the definition of ''standard'' to better reflect the scope of the Privacy and Security Rules;

(5) Adds a reference to ''business associate'' following the reference to ''covered entity'' in the definitions of ''respondent'' and ''compliance date,'' in recognition of the potential liability imposed on business associates for violations of certain provisions of the Privacy and Security Rules by sections 13401 and 13404 of the Act; and

(6) Revises the definition of ''workforce member'' in § 160.103 to make clear that the term includes the employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a business associate, is under the direct control of the business associate, because some provisions of the Act and the Privacy and Security Rules place obligations on the business associate with respect to workforce members.

4. Subpart B—Preemption of State Law

a. Section 160.201—Statutory Basis

Proposed Rule

We proposed to modify § 160.201 regarding the statutory basis for the preemption of State law provisions to add a reference to section 264(c) of HIPAA, which contains the statutory basis for the exception to preemption at § 160.203(b) for State laws that are more stringent than the HIPAA Privacy Rule. We also proposed to add a reference to

section 13421(a) of the HITECH Act, which applies HIPAA's preemption rules to the HITECH Act's privacy and security provisions. Finally, we proposed to re-title the provision to read ''Statutory basis'' instead of ''Applicability.''

Overview of Public Comments

Several commenters expressed concerns about the lack of uniform Federal and State privacy laws and the resultant confusion and expense associated with determining which laws apply to a given circumstance, particularly as more and more health care entities operate across multiple state lines. Commenters recommended that the Department make efforts to engage States and other partners to examine divergent Federal and State requirements and to attempt to coordinate various disclosure rules to drive Federal-State consensus.

Final Rule

The final rule adopts the proposed modifications. In response to the comments concerned with the lack of uniform Federal and State privacy laws, we note that the preemption provisions of the HIPAA Rules are based on section 1178 of the Social Security Act and section 264(c)(2) of HIPAA. Through these statutory provisions, Congress made clear that the HIPAA privacy requirements are to supersede only contrary provisions of State law, and not even in all such cases, such as where the provision of State law provides more stringent privacy protections than the HIPAA Privacy Rule. Accordingly, the HIPAA Privacy Rule provides a Federal floor of privacy protections, with States free to impose more stringent privacy protections should they deem appropriate.

b. Section 160.202—Definitions

i. Definition of ''Contrary''

Proposed Rule

The term ''contrary'' is defined in § 160.202 to make clear when the preemption provisions of HIPAA apply to State law. For the reasons set forth on page 40875 of the July 2010 NPRM, we proposed to amend the definition of ''contrary'' by inserting references to business associates in paragraph (1) of the definition. We also expanded the reference to the HITECH statutory provisions in paragraph (2) of the definition to encompass all of the sections of subtitle D of the HITECH Act, rather than merely to section 13402, which was added by the breach notifications interim final rule. These changes would give effect to section 13421(a).

Final Rule

The Department did not receive substantive public comment on this proposal. The final rule adopts the proposed modifications.

ii. Definition of ''More Stringent''

Proposed Rule

The term ''more stringent'' is part of the statutory preemption language under HIPAA. HIPAA preempts State law that is contrary to a HIPAA privacy standard unless, among other exceptions, the State law is more stringent than the contrary HIPAA privacy standard. We proposed to amend the definition to add a reference to business associates.

Final Rule

The Department did not receive substantive public comment on this proposal. The final rule adopts the proposed modification.

B. Subparts C and D of Part 160: Amendments to the Enforcement Rule

Section 13410 of the HITECH Act made several amendments to the Social Security Act to strengthen the HIPAA Enforcement Rule, which applies to the Secretary's enforcement of all of the HIPAA Administrative Simplification Rules, as well as the Breach Notification Rule.

On October 30, 2009, the Department issued an interim final rule (IFR) revising the Enforcement Rule to incorporate the provisions of section 13410(d) of the HITECH Act that took effect immediately to apply to violations of the HIPAA Rules occurring after the enactment date of February 18, 2009. See 74 FR 56123. In general, section 13410(d) of the HITECH Act revised section 1176(a) of the Social Security Act to establish four categories of violations that reflect increasing levels of culpability and four corresponding tiers of penalty amounts that significantly increased the minimum penalty amount for each violation, with a maximum penalty amount of $1.5 million annually for all violations of an identical provision. Section 13410(d) also amended section 1176(b) of the Social Security Act by removing the previous affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (these violations are now punishable under the lowest tier of penalties), and by providing a prohibition on the imposition of penalties for any violation that is timely corrected, as long as the violation was not due to willful neglect. The IFR updated the HIPAA Enforcement Rule to reflect these statutory amendments. The IFR did not make amendments with respect to those enforcement provisions of section 13410 of the HITECH Act that were not effective immediately upon enactment.

In its July 2010 NPRM, the Department proposed a number of additional modifications to the Enforcement Rule to reflect other provisions of section 13410 of the HITECH Act, some of which became effective on February 18, 2010, or were to become effective at a later date: (1) Requiring that the Secretary formally investigate complaints indicating violations due to willful neglect, and impose civil money penalties upon finding violations due to willful neglect; (2) making business associates of covered entities directly liable for civil money penalties for violations of certain provisions of the HIPAA Rules; (3) requiring the Secretary to determine civil money penalty amounts based upon the nature and extent of the harm resulting from a violation; and (4) providing that the Secretary's authority to impose a civil money penalty will be barred only to the extent a criminal penalty has been imposed with respect to an act under Section 1177, rather than in cases in which the act constitutes an offense that is criminally punishable under Section 1177.

The following discussion describes the enforcement provisions of the IFR and the NPRM, responds to public comment received by the Department on both rules, and describes the final modifications to the Enforcement Rule adopted by this final rule. In addition to the modifications discussed below, this final rule also adopts the NPRM proposal to add the term ''business associate'' to the following provisions of the Enforcement Rule: §§ 160.300; 160.304; 160.306(a) and (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402; 160.404(b); 160.406; 160.408(c) and (d); and 160.410(a) and (c). This is done to implement sections 13401 and 13404 of the Act, which impose direct civil money penalty liability on business associates for their violations of certain provisions of the HIPAA Rules.

1. Subpart C of Part 160—Compliance and Investigations

a. Sections 160.304, 160.306, 160.308, and 160.312—Noncompliance Due to Willful Neglect

Proposed Rule

Section 13410(a) of the HITECH Act adds a new subsection (c) to section 1176 of the Social Security Act, which requires the Department to formally investigate a complaint if a preliminary investigation of the facts of the complaint indicates a possible violation due to willful neglect (section 1176(c)(2)) and to impose a civil money penalty for a violation due to willful neglect (section 1176(c)(1)). The Department proposed a number of modifications to Subpart C of the Enforcement Rule to implement these provisions.

First, § 160.306(c) of the Enforcement Rule currently provides the Secretary with discretion to investigate HIPAA complaints through the use of the word ''may.'' As a practical matter, however, the Department currently conducts a preliminary review of every complaint received and proceeds with the investigation in every eligible case where its preliminary review of the facts indicates a possible violation of the HIPAA Rules. Nonetheless, to implement section 1176(c)(2), the Department proposed to add a new paragraph (1) to § 160.306(c) (and to make conforming changes to the remainder of § 160.306(c)) to make clear that the Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect. Under proposed § 160.306(c)(2), the Secretary would have continued discretion with respect to investigating any other complaints.

Second, the Department proposed to modify § 160.308 by adding a new paragraph (a) to provide that the Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provision when a preliminary review of the facts indicates a possible violation due to willful neglect. Like § 160.306(c) with respect to complaints, the current § 160.308(c) provides the Secretary with discretion to conduct compliance reviews. While section 13410(a) of the HITECH Act specifically mentions complaints and not compliance reviews with respect to willful neglect, the Department proposed to treat compliance reviews in the same manner because it believed doing so would strengthen enforcement with respect to potential violations of willful neglect and would ensure that investigations, whether or not initiated by a complaint, would be handled in a consistent manner. Under proposed § 160.308(b), the Secretary would continue to have discretion to conduct compliance reviews in circumstances not indicating willful neglect.

Third, given the HITECH Act's requirement that the Secretary impose a penalty for any violation due to willful neglect, the Department proposed changes to § 160.312, which currently requires the Secretary to attempt to resolve investigations or compliance reviews indicating noncompliance by informal means. The NPRM proposed to provide instead in § 160.312(a) that the Secretary ''may'' rather than ''will'' attempt to resolve investigations or compliance reviews indicating noncompliance by informal means. This change would permit the Department to proceed with a willful neglect violation determination as appropriate, while also permitting the Department to seek resolution of complaints and compliance reviews that did not indicate willful neglect violations by informal means (e.g., where the covered entity or business associate did not know and by exercising reasonable diligence would not have known of a violation, or where the violation is due to reasonable cause).

Finally, the Department proposed a conforming change to § 160.304(a), which currently requires the Secretary to seek, to the extent practicable, the cooperation of covered entities in obtaining compliance with the HIPAA Rules. The NPRM proposed to clarify that the Secretary would continue to do so ''consistent with the provisions of this subpart'' in recognition of the new HITECH Act requirement to impose a civil money penalty for a violation due to willful neglect. While the Secretary often will still seek to correct indications of noncompliance through voluntary corrective action, there may be circumstances (such as circumstances indicating willful neglect), where the Secretary may proceed directly to formal enforcement.

Overview of Public Comments

One commenter supported maintaining the current language at §§ 160.306 and 160.308 of the Enforcement Rule, providing the Secretary with discretion to conduct complaint investigations and compliance reviews, regardless of indications of willful neglect. One commenter suggested that OCR look to whether facts indicate a ''probable,'' rather than ''possible,'' violation due to willful neglect to limit the likelihood of unnecessary formal investigations or compliance reviews. While one commenter supported the proposal to require a compliance review in circumstances indicating a possible violation due to willful neglect, others argued that requiring compliance reviews in such circumstances is not required by the statute, will detract from resources to investigate complaints, and will be duplicative if a formal complaint investigation is also underway.

Several commenters expressed concern over the proposal at § 160.312(a) to give the Secretary discretion, rather than to require the Secretary, to attempt to resolve investigations or compliance reviews indicating noncompliance by informal means, even in cases of noncompliance that did not involve willful neglect (e.g., cases involving reasonable cause or lack of knowledge of a violation). Commenters indicated support for the Department's seeking compliance through voluntary corrective action as opposed to formal enforcement proceedings and argued that the Department should retain the requirement for the Secretary to attempt informal resolution in all circumstances except those involving willful neglect. One commenter recommended that the Secretary be able to assess penalties regardless of whether corrective action was obtained.

Final Rule

The final rule adopts the modifications to §§ 160.304, 160.306, 160.308, and 160.312, as proposed in the NPRM. The Department believes these changes to the enforcement provisions to be appropriate given the HITECH Act's requirements at section 13410(a) with respect to circumstances indicating or involving noncompliance due to willful neglect. We do not provide in the Rule that the Secretary will investigate when a preliminary review of the facts indicates a ''probable'' rather than ''possible'' violation due to willful neglect as the statute requires an investigation even in cases indicating a ''possible'' violation due to willful neglect. In response to commenters concerned about requiring the Secretary to conduct compliance reviews in circumstances in which facts indicate a possible violation due to willful neglect, we continue to believe that, while not expressly required by the statute, doing so appropriately strengthens enforcement with respect to violations due to willful neglect and ensures consistency in the handling of complaints and compliance reviews in

which violations due to willful neglect are indicated. We emphasize that the Department retains discretion to decide whether to conduct a compliance review (or complaint investigation) where a preliminary review of the facts indicates a degree of culpability less than willful neglect. Further, with respect to commenter concerns about duplication between complaint investigations and compliance reviews, we clarify that the Department generally conducts compliance reviews to investigate allegations of violations of the HIPAA Rules brought to the Department's attention through a mechanism other than a complaint. For example, the Department may use a compliance review to investigate allegations of violations of the Rules brought to our attention through a media report, or from a State or another Federal agency. If the Department initiates an investigation of a complaint because its preliminary review of the facts indicates a possible violation due to willful neglect, the Department is not also required to initiate a compliance review under § 160.308 because doing so would initiate a duplicative investigation.

With respect to § 160.312, where the Rule previously mandated that the Secretary attempt to resolve indicated violations of the HIPAA Rules by informal means, the final rule now provides the Secretary with the discretion to do so, to reflect Section 13410 of the HITECH Act with regard to violations due to willful neglect. Nothing in Section 13410 of the HITECH Act limits the Secretary's ability to resolve such cases by informal means. However, through its introduction of higher penalties and its mandate for formal investigations with regard to possible violations due to willful neglect, Section 13410 strengthens enforcement and accordingly we have revised § 160.312 so that the Secretary may move directly to a civil money penalty without exhausting informal resolution efforts at her discretion, particularly in cases involving willful neglect violations.

Response to Other Public Comments

Comment: A number of commenters requested further clarification on the scope and depth of what constitutes a ''preliminary review of the facts'' for purposes of determining whether facts indicate a possible violation due to willful neglect and thus, warrant a formal complaint investigation or compliance review. Certain commenters suggested that a preliminary review of the facts should go beyond merely a review of the allegations asserted in a complaint.

Response: As noted above, currently the Department conducts a preliminary review of every complaint received and proceeds with the investigation in every eligible case where its preliminary review of the facts indicates a possible violation of the HIPAA Rules. The Department anticipates that some complaints, on their face, or reports or referrals that form the basis of a potential compliance review, will contain sufficient information to indicate a possible violation due to willful neglect, and some may not. In any event, the Department may on a case-by-case basis expand the preliminary review and conduct additional inquiries for purposes of identifying a possible violation due to willful neglect. Notwithstanding the scope of a preliminary review, OCR will determine if an indicated violation was due to willful neglect based on the evidence from its investigation of the allegations, even if a violation due to willful neglect was not indicated at the preliminary review stage.

b. Section 160.310—Protected Health Information Obtained by the Secretary

Proposed Rule

Section 160.310 requires that covered entities make information available to and cooperate with the Secretary during complaint investigations and compliance reviews. Section 160.310(c)(3) provides that any protected health information obtained by the Secretary in connection with an investigation or compliance review will not be disclosed by the Secretary, except as necessary for determining and enforcing compliance with the HIPAA Rules or as otherwise required by law. In the proposed rule, we proposed to modify this paragraph to also allow the Secretary to disclose protected health information if permitted under the Privacy Act at 5 U.S.C. 552a(b)(7). Section 5 U.S.C. 552a(b)(7) permits the disclosure of a record on an individual contained within a government system of records protected under the Privacy Act to another agency or instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law and if the agency has made a written request to the agency that maintains the record. The proposed change would permit the Secretary to coordinate with other law enforcement agencies, such as the State Attorneys General pursuing civil actions to enforce the HIPAA Rules on behalf of State residents pursuant to section 13410(e) of the Act, or the FTC pursuing remedies under other consumer protection authorities.

Overview of Public Comments

One commenter requested clarification and transparency on how or if Federal regulators such as OCR and the FTC will collaborate, when such information sharing will be initiated or occur as a routine process, or whether Federal and State agencies will work together to enforce suspected violations.

Final Rule

To facilitate cooperation between the Department and other law enforcement agencies, the final rule adopts the modifications to § 160.310(c)(3) as proposed in the NPRM. In response to the comment regarding transparency in how the Department is or will cooperate with other agencies in enforcement, we note that the Department's web site at *http://www.hhs.gov/ocr/enforcement/* contains information about how the Department coordinates with the Department of Justice to refer cases involving possible criminal HIPAA violations and how the Department has worked with the FTC to coordinate enforcement actions for violations that implicate both HIPAA and the FTC Act. Further, the Department will be working closely with State Attorneys General to coordinate enforcement in appropriate cases, as provided under section 13410(e) of the HITECH Act. The Department will continue to update its web site as necessary and appropriate to maintain transparency with the public and the regulated community about these coordinated activities and its other enforcement actions and activities.

2. Subpart D—Imposition of Civil Money Penalties

a. Section 160.401—Definitions

Section 160.401 defines ''reasonable cause,'' ''reasonable diligence,'' and ''willful neglect.'' Given that section 13410(d) of the HITECH Act uses these terms to describe the increasing levels of culpability for which increasing minimum levels of penalties may be imposed, the Department moved these definitions in the IFR from their prior placement at § 160.410, which pertains only to affirmative defenses, to § 160.401, so that they would apply to the entirety of Subpart D of Part 160 and the provisions regarding the imposition of civil money penalties. The IFR did not modify the definitions themselves as the HITECH Act did not amend the definitions.

Even though the HITECH Act did not amend the definitions of these terms,

the Department in its NPRM proposed certain modifications to the definition of ''reasonable cause'' to clarify the mens rea (state of mind) required for this category of violations, and to avoid the situation where certain violations would not fall within one of the established penalty tiers. This modification is discussed below. The Department did not propose modifications to the definitions of ''reasonable diligence'' and ''willful neglect.''

In the NPRM, the Department also included examples and guidance as to how the Department planned to apply the definitions of ''reasonable cause,'' ''reasonable diligence,'' and ''willful neglect'' to distinguish among the tiers of culpability. 75 FR 40877–40879. As commenters generally found this guidance helpful, the Department intends to publish the guidance on its web site.

Modifications to the Definition of ''Reasonable Cause''

Proposed Rule

Reasonable cause is currently defined at § 160.401 to mean: ''circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.'' This definition is consistent with the Supreme Court's ruling in *United States* v. *Boyle,* 469 U.S. 241, 245 (1985), which focused on whether circumstances were beyond the regulated person's control, thereby making compliance unreasonable. See 70 FR 20224, 20238. Prior to the HITECH Act, section 1176 of the Social Security Act provided an affirmative defense to the imposition of a civil money penalty if the covered entity established that its violation was due to reasonable cause and not willful neglect and was corrected within a 30-day period (or such additional period determined by the Secretary to be appropriate).

As described above, section 13410(d) of the HITECH Act revised section 1176 of the Social Security Act to establish four tiers of increasing penalty amounts to correspond to the levels of culpability associated with the violation. The first category of violation (and lowest penalty tier) covers situations where the covered entity or business associate did not know, and by exercising reasonable diligence would not have known, of a violation. The second category of violation (and next highest penalty tier) applies to violations due to reasonable cause and not to willful neglect. The third and fourth categories apply to circumstances where the violation was due to willful neglect that is corrected within a certain time period (second highest penalty tier) and willful neglect that is not corrected (highest penalty tier). The mens rea, or state of mind, associated with the tiers is clear with respect to the first, third, and fourth categories, in that there is no mens rea with respect to the lowest category of violation, while the existence of mens rea is presumed with respect to the third and fourth categories of violation.

However, the current definition of ''reasonable cause'' does not address mens rea with respect to the second category of violations. Therefore, the Department proposed to amend the definition of ''reasonable cause'' at § 160.401 to clarify the mens rea associated with the reasonable cause category of violations and to clarify the full scope of violations that will come within the category. Specifically, the Department proposed to modify the definition of ''reasonable cause'' to mean ''an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.'' Thus, the proposed definition would now include violations due both to circumstances that would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated, as well as to other circumstances in which a covered entity or business associate has knowledge of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category of violations.

Overview of Public Comments

Commenters addressing the definition of ''reasonable cause'' expressed general support for the proposed clarifications to the scope of this category of violations.

Final Rule

The final rule adopts the proposed modifications to the definition.

b. Section 160.402—Basis for a Civil Money Penalty

Proposed Rule

Section 160.402(a) states generally that the Secretary will impose a civil money penalty upon a covered entity if the Secretary determines that the covered entity violated an administrative simplification provision. Section 164.402, in paragraphs (b) and (c), provides the basis for a civil money penalty against a covered entity where more than one covered entity is responsible for a violation, where an affiliated covered entity is responsible for a violation, and where an agent of a covered entity is responsible for a violation.

The proposed rule proposed to remove the exception at § 160.402(c) for covered entity liability for the acts of its agent in cases where the agent is a business associate, the relevant contract requirements have been met, the covered entity did not know of a pattern or practice of the business associate in violation of the contract, and the covered entity did not fail to act as required by the Privacy or Security Rule with respect to such violations. The proposed rule also proposed to add a parallel provision in a new paragraph (2) at § 160.402(c) that would provide for civil money penalty liability against a business associate for the acts of its agent. The existing language of § 160.402(c) regarding the liability of covered entities for the acts of their agents would be re-designated as paragraph (1).

These proposed changes would make covered entities and business associates liable under § 160.402(c) for the acts of their business associate agents, in accordance with the Federal common law of agency, regardless of whether the covered entity has a compliant business associate agreement in place. Section 160.402(c) closely tracks the language in section 1128A(l) of the Social Security Act, which is made applicable to HIPAA by section 1176(a)(2) of such Act, which states that ''a principal is liable for penalties * * * under this section for the actions of the principal's agents acting within the scope of the agency.'' One reason for removing the exception to the general provision at § 160.402(c), as we explained in the NPRM, is to ensure, where a covered entity or business associate has delegated out an obligation under the HIPAA Rules, that a covered entity or business associate would remain liable for penalties for the failure of its business associate agent to perform the obligation on the covered entity or business associate's behalf.

Overview of Public Comments

Several commenters requested that the Department clarify and provide additional guidance regarding how the Federal common law of agency applies to business associate relationships. These commenters expressed an overall concern that applying the Federal common law of agency to business

associate relationships would add unnecessary confusion to and place an undue burden on business associate relationships. Several commenters argued that the proposed change would require covered entities and business associates to determine whether their business associates or business associate subcontractors are agents, resulting in costly and burdensome challenges when drafting business associate contracts and monitoring ongoing relationships. One commenter argued that the Federal common law of agency should not be applied to covered entity and business associate relationships because it does not generally control when the parties have entered into a contractual agreement that specifies their respective rights and obligations. Instead, the commenter argued, the contractual provisions control, and are interpreted and enforced in accordance with State law specified by the contract.

Final Rule

This final rule adopts the proposed modifications to § 160.402(c). We do not believe that this change will place an undue burden on covered entities and business associates. As we explained in the NPRM, a covered entity's liability for acts of its agents is customary under common law. See 75 FR 40880. Further, section 1128A(l) of the Social Security Act, applicable to HIPAA covered entities and now business associates by section 1176(a)(2) of the Act, states that a principal is liable for civil money penalties for the actions of the principal's agent acting within the scope of agency. Before the changes to § 160.402(c) were finalized in this rule, if a covered entity failed to comply with the business associate provisions in the HIPAA Rules, a covered entity potentially would have been liable for the actions of its business associate agent. Thus, we believe that the notion that a principal is liable for the acts of its agent should not be an unfamiliar concept to covered entities and business associates. However, we appreciate and understand the commenters' concerns and take this opportunity to provide additional guidance.

While section 1128A(l) is silent as to how to define ''principal,'' ''agent,'' and ''scope of agency,'' § 160.402(c) references the Federal common law of agency. As we explained in the Enforcement Rule preamble, 71 FR 8390, 8403–04, adopting the Federal common law to determine the definitions and application of these terms achieves nationwide uniformity in the implementation of the HIPAA Rules. We believe that relying on the Federal common law is particularly important because of HIPAA's express objective of furthering the efficiency and effectiveness of the health care system as a whole. Further, adopting the Federal common law here is consistent with the precept that Federal statutes are meant to have uniform nationwide application. Therefore, we disagree with the comment that argued that Federal common law should not be applied with respect to relationships between covered entities and business associates.

An analysis of whether a business associate is an agent will be fact specific, taking into account the terms of a business associate agreement as well as the totality of the circumstances involved in the ongoing relationship between the parties. The essential factor in determining whether an agency relationship exists between a covered entity and its business associate (or business associate and its subcontractor) is the right or authority of a covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity. The right or authority to control the business associate's conduct also is the essential factor in determining whether an agency relationship exists between a business associate and its business associate subcontractor. Accordingly, this guidance applies in the same manner to both covered entities (with regard to their business associates) and business associates (with regard to their subcontractors).

The authority of a covered entity to give interim instructions or directions is the type of control that distinguishes covered entities in agency relationships from those in non-agency relationships. A business associate generally would not be an agent if it enters into a business associate agreement with a covered entity that sets terms and conditions that create contractual obligations between the two parties. Specifically, if the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent. In contrast, a business associate generally would be an agent if it enters into a business associate agreement with a covered entity that granted the covered entity the authority to direct the performance of the service provided by its business associate after the relationship was established. For example, if the terms of a business associate agreement between a covered entity and its business associate stated that ''a business associate must make available protected health information in accordance with § 164.524 based on the instructions to be provided by or under the direction of a covered entity,'' then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship. An agency relationship also could exist between a covered entity and its business associate if a covered entity contracts out or delegates a particular obligation under the HIPAA Rules to its business associate. As discussed above, whether or not an agency relationship exists in this circumstance again would depend on the right or authority to control the business associate's conduct in the performance of the delegated service based on the right of a covered entity to give interim instructions.

While these principles are well established under the Federal common law of agency, we again note that any analysis regarding scope of agency depends on the facts of each circumstance. Several factors are important to consider in any analysis to determine the scope of agency: (1) The time, place, and purpose of a business associate agent's conduct; (2) whether a business associate agent engaged in a course of conduct subject to a covered entity's control; (3) whether a business associate agent's conduct is commonly done by a business associate to accomplish the service performed on behalf of a covered entity; and (4) whether or not the covered entity reasonably expected that a business associate agent would engage in the conduct in question.

The terms, statements, or labels given to parties (e.g., independent contractor) do not control whether an agency relationship exists. Rather, the manner and method in which a covered entity actually controls the service provided decides the analysis. As mentioned above, an analysis of whether a business associate is an agent will be fact specific and consider the totality of the circumstances involved in the ongoing relationship between the parties. We note here several circumstances that are important. The type of service and skill level required to perform the service are relevant factors in determining whether a business associate is an agent. For example, a business associate that is hired to perform de-identification of protected health information for a small provider would likely not be an agent because the small provider likely would not have the expertise to provide interim instructions regarding this activity to the business associate. Also, an agency relationship would not likely exist when a covered entity is legally or

otherwise prevented from performing the service or activity performed by its business associate. For example, the accreditation functions performed by a business associate cannot be performed by a covered entity seeking accreditation because a covered entity cannot perform an accreditation survey or award accreditation. We also note that a business associate can be an agent of a covered entity: (1) Despite the fact that a covered entity does not retain the right or authority to control every aspect of its business associate's activities; (2) even if a covered entity does not exercise the right of control but evidence exists that it holds the authority to exercise that right; and (3) even if a covered entity and its business associate are separated by physical distance (e.g., if a covered entity and business associate are located in different countries).

Response to Other Public Comments

Comment: One commenter asked whether the Department intends to eliminate the exceptions afforded by the Federal common law of agency. This commenter also argued that if a business associate were an agent of a covered entity, and a HIPAA compliant business associate agreement was in place, any deviation from the terms in the agreement would be by definition outside the scope of agency.

Response: As we discussed above, § 160.402(c) provides that covered entities and business associates are liable for the acts of their business associate agents, in accordance with the Federal common law of agency. Section 160.402(c) is derived from section 1128A(l) of the Social Security Act which states that ''a principal is liable for penalties * * * under this section for the actions of the principal's agents acting within the scope of the agency.'' Accordingly, § 160.402(c) incorporates the Federal common law of agency, which includes the understanding that for a principal to be liable for the actions of an agent, the agent must be acting within the scope of agency. Thus, the exceptions to the Federal common law of agency (as the commenter identified them) are incorporated in the final rule at § 160.402(c).

We do not agree with the commenter that any deviation from the terms in a business associate contract would be by definition outside the scope of agency. A business associate agent's conduct generally is within the scope of agency when its conduct occurs during the performance of the assigned work or incident to such work, regardless of whether the work was done carelessly, a mistake was made in the performance, or the business associate disregarded a covered entity's specific instruction. For example, a business associate agent would likely be acting within the scope of agency if it impermissibly disclosed more than the minimum necessary information to a health plan for purposes of payment, even if the disclosure is contrary to clear instructions of the covered entity. In contrast, a business associate agent's conduct generally is outside the scope of agency when its conduct is solely for its own benefit (or that of a third party), or pursues a course of conduct not intended to serve any purpose of the covered entity.

Comment: One commenter stated that the proposed change would impose strict liability on covered entities for the actions of third parties not under their control. Another commenter stated that an agent would always fall within the scope of a workforce member, which by definition is not a business associate.

Response: We disagree with both comments and believe that the comments may reflect a misunderstanding of the proposed change. First, as explained above, § 160.402(c) closely tracks the language in section 1128A(l) of the Social Security Act, which is made applicable to HIPAA by section 1176(a)(2) of such Act. It does not make a covered entity or business associate liable for the acts of third parties that are not under its control because such third parties are not its agents. With regard to the second comment, an agent could always fall within the definition of a workforce member because of the direct control requirement in that definition, but the definition of business associate excludes a workforce member. This definitional exclusion allows the covered entity to determine whether, for example, to provide training to the agent under the Privacy Rule. A covered entity would be required to provide training to a workforce member but not to a business associate agent. However, the covered entity is required to enter into a business associate agreement with a business associate agent that it does not treat as a workforce member. The proposed change to § 160.402(c) simply makes the covered entity or business associate liable for the acts of its agents acting within the scope of agency, whether the agents are workforce members or business associates. See the definitions of ''business associate'' and ''workforce member'' at § 160.103.

c. Section 160.404—Amount of a Civil Monetary Penalty

Interim Final Rule

The IFR amended § 160.404 to revise the range of potential civil money penalty amounts a covered entity (or business associate) will be subject to for violations occurring on or after February 18, 2009, as a result of section 13410(d) of the HITECH Act.

Prior to the HITECH Act, section 1176(a) of the Social Security Act authorized the Secretary to impose a civil money penalty of not more than $100 for each violation, with the total amount imposed on a covered entity for all violations of an identical requirement or prohibition during a calendar year not to exceed $25,000. As described above, section 13410(d) of the HITECH Act modified section 1176(a) to establish tiers of increasing penalty amounts for violations based on increasing levels of culpability associated with each tier.

Accordingly, the IFR adopted at § 160.404(b) the new penalty scheme provided for at section 13410(d) of the HITECH Act for violations occurring on or after February 18, 2009. The IFR retained the pre-HITECH maximum penalty amounts of not more than $100 per violation and $25,000 for identical violations during a calendar year, for violations occurring before February 18, 2009.

In adopting the HITECH Act's penalty scheme, the Department recognized that section 13410(d) contained apparently inconsistent language (i.e., its reference to two penalty tiers ''for each violation,'' each of which provided a penalty amount ''for all such violations'' of an identical requirement or prohibition in a calendar year). To resolve this inconsistency, with the exception of violations due to willful neglect that are not timely corrected, the IFR adopted a range of penalty amounts between the minimum given in one tier and the maximum given in the second tier for each violation and adopted the amount of $1.5 million as the limit for all violations of an identical provision of the HIPAA rules in a calendar year. For violations due to willful neglect that are not timely corrected, the IFR adopted the penalty amount of $50,000 as the minimum for each violation and $1.5 million for all such violations of an identical requirement or prohibition in a calendar year.

Specifically, the IFR revised § 160.404 to provide, for violations occurring on or after February 18, 2009, the new HITECH penalty scheme, as follows: (1) For violations in which it is established that the covered entity did not know

and, by exercising reasonable diligence, would not have known that the covered entity violated a provision, an amount not less than $100 or more than $50,000 for each violation; (2) for a violation in which it is established that the violation was due to reasonable cause and not to willful neglect, an amount not less than $1000 or more than $50,000 for each violation; (3) for a violation in which it is established that the violation was due to willful neglect and was timely corrected, an amount not less than $10,000 or more than $50,000 for each violation; and (4) for a violation in which it is established that the violation was due to willful neglect and was not timely corrected, an amount not less than $50,000 for each violation; except that a penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1,500,000 in a calendar year. See Table 2 below.

TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect-Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect-Not Corrected	50,000	1,500,000

In applying these amounts, the Department will not impose the maximum penalty amount in all cases but rather will determine the penalty amounts as required by the statute at section 1176(a)(1) and the regulations at § 160.408 (i.e., based on the nature and extent of the violation, the nature and extent of the resulting harm, and the other factors set forth at § 160.408).

Further, for counting violations, the Department continues to utilize the methodology discussed in prior preambles of the Enforcement Rule. See 70 FR 20224, 20233–55 (April 18, 2005) and 71 FR 8390, 8404–07 (February 16, 2006). For violations that began prior to February 18, 2009, and continue after that date, the Department will treat violations occurring before February 18, 2009, as subject to the penalties in effect prior to February 18, 2009, and violations occurring on or after February 18, 2009, as subject to the penalties in effect on or after February 18, 2009.

Overview of Public Comments

Most comments on the civil money penalty amounts expressed concern with the new penalty structure set forth in the IFR. A few of these commenters expressed a generalized concern about the potential impact the available penalty amounts might have on covered entities, particularly smaller entities. One commenter argued that the Secretary should not fine entities for violations of which a covered entity had no knowledge or those due to reasonable cause, and that civil money penalties should only be imposed as a last resort. A few commenters expressed concern with the Secretary's wide range of discretion in determining a civil money penalty amount and suggested that the regulations or guidance should further define how the Secretary would determine such an amount.

Some commenters specifically expressed concern about the maximum penalty amounts set forth for each violation (i.e., $50,000) and for all violations of an identical provision in a calendar year ($1,500,000). Commenters argued that the IFR's penalty scheme is inconsistent with the HITECH Act's establishment of different tiers based on culpability because the outside limits were the same for all culpability categories and this ignored the outside limits set forth by the HITECH Act within the lower penalty tiers, rendering those limits meaningless. A few commenters expressed particular concern with what they believed to be the unfair ability of the Secretary to impose the maximum penalty amounts to violations falling within the two lowest categories of culpability (i.e., did not know violations and violations due to reasonable cause and not willful neglect).

Final Rule

This final rule retains the revised penalty structure in § 160.404(b) as implemented by the IFR. We continue to believe the penalty amounts are appropriate and reflect the most logical reading of the HITECH Act, which provides the Secretary with discretion to impose penalties for each category of culpability up to the maximum amount described in the highest penalty tier.

With respect to those comments expressing concern about the discretion available to the Secretary under the adopted scheme we emphasize again that the Department will not impose the maximum penalty amount in all cases but will rather determine the amount of a penalty on a case-by-case basis, depending on the nature and extent of the violation and the nature and extent of the resulting harm, as required by the HITECH Act, as well as the other factors set forth at § 160.408. In response to those commenters particularly concerned about the impact of penalties on smaller entities, we note that the other factors include both the financial condition and size of the covered entity or business associate. These factors are discussed more fully below.

In addition, with respect to comments expressing specific concern about fairness regarding those violations of which an entity did not know or by exercising reasonable diligence would not have known or for which there was a reasonable cause and not willful neglect, we note that in both cases an entity may establish that an affirmative defense applies under § 160.410, where the entity corrects the violation within 30 days from the date the entity had knowledge of the violation or with the exercise of reasonable diligence would have had knowledge of the violation, or during a period determined appropriate by the Secretary based upon the nature and extent of the entity's failure to comply. These affirmative defenses are described more fully below.

In addition, Section 13410(d) of the HITECH Act and Section 1176(a) of the Social Security Act, give the Secretary further ability to waive a civil money penalty, in whole or in part, under certain circumstances. Thus, to the extent an entity fails to correct such violations within the mandated timeframe, the Secretary may also utilize her waiver authority provided for at § 160.412, to waive the penalty amount in whole or in part, to the extent that payment of the penalty would be excessive relative to the violation.

Further, pursuant to 42 U.S.C. 1320a–7a(f), the Secretary always has the discretion to settle any issue or case or to compromise the amount of a civil money penalty assessed for a violation of the HIPAA Rules.

Finally, in the event an entity believes that a civil money penalty has been imposed unfairly, the entity could exercise its right under § 160.504 to appeal the imposition of a civil money penalty in a hearing before an administrative law judge.

Response to Other Public Comments

Comment: We received a few comments in response to the IFR and NPRM requesting clarification as to how the Secretary will count violations for purposes of calculating civil money penalties. One commenter requested clarification as to how the numbers of ''occurrences'' are determined, suggesting that penalties could be very significant, and vary significantly, depending on the counting methodology utilized. The Department also received one comment asking whether a violation is defined as one event. This commenter queried, for example, whether the loss of unsecured electronic media would be considered as a single violation, even if the media contained several hundred records. The commenter also asked for confirmation that $1,500,000 is the aggregate limit of all fines for all violations in a given calendar year which would apply across an entire enterprise, regardless of violations occurring in different business units.

Response: How violations are counted for purposes of calculating a civil money penalty vary depending on the circumstances surrounding the noncompliance. Generally speaking, where multiple individuals are affected by an impermissible use or disclosure, such as in the case of a breach of unsecured protected health information, it is anticipated that the number of identical violations of the Privacy Rule standard regarding permissible uses and disclosures would be counted by the number of individuals affected. Further, with respect to continuing violations, such as lack of appropriate safeguards for a period of time, it is anticipated that the number of identical violations of the safeguard standard would be counted on a per day basis (i.e., the number of days the entity did not have appropriate safeguards in place to protect the protected health information). Note also that in many breach cases, there will be both an impermissible use or disclosure, as well as a safeguards violation, for each of which the Department may calculate a separate civil money penalty. We refer readers to prior Enforcement Rule preambles for additional discussion on the counting methodology. See 70 FR 20224, 20233–55 (April 18, 2005) and 71 FR 8390, 8404–07 (February 16, 2006).

With respect to whether the aggregate CMP limit of $1.5 million would apply to all violations in a given calendar year, across an entire enterprise, regardless of violations occurring in different business units of the enterprise, we note that the Enforcement Rule's penalty scheme, and thus the limit for identical violations in a calendar year applies to the legal entity that is a covered entity or business associate. However, as we indicated above, a covered entity or business associate may be liable for multiple violations of multiple requirements, and a violation of each requirement may be counted separately. As such, one covered entity or business associate may be subject to multiple violations of up to a $1.5 million cap for each violation, which would result in a total penalty above $1.5 million.

d. Section 160.408—Factors Considered in Determining the Amount of a Civil Money Penalty

Proposed Rule

Section 160.408 implements section 1176(a)(2) of the Social Security Act, which requires the Secretary, when imposing a civil money penalty, to apply the provisions of section 1128A of the Social Security Act ''in the same manner as such provisions apply to the imposition of a civil money penalty under section 1128A.'' In determining a penalty amount, section 1128A requires the Secretary to take into account the nature of the claims and the circumstances under which they were presented; the degree of culpability, history of prior offenses and financial condition of the person presenting the claims; and such other matters as justice may require.

Section 160.408 adopted these factors and provided a more specific list of circumstances within each. Because the Enforcement Rule applies to a number of rules, which apply to an enormous number of entities and circumstances, the Secretary has the discretion to decide whether and how to consider the factors (i.e., as either aggravating or mitigating) in determining the amount of a civil money penalty.

As previously indicated, section 13410(d) of the HITECH Act modified section 1176(a)(1) of the Social Security Act to require that the Department base determinations of appropriate penalty amounts on the nature and extent of the violation and the nature and extent of the harm resulting from such violation. However, the HITECH Act did not modify section 1176(a)(2),which continues to require application of the factors in section 1128A.

The proposed rule proposed to revise the structure and list of factors at § 160.408 to make explicit the new HITECH Act requirement that the Secretary consider the nature and extent of the violation and the nature and extent of the harm resulting from the violation, in addition to those factors enumerated in section 1128A. We proposed to exclude, however, the factor at § 160.408(c) regarding the degree of culpability of the covered entity, which originated in section 1128A, because culpability is now reflected in the penalty tiers.

Specifically, the Department proposed to revise § 160.408(a) to identify ''the nature and extent of the violation,'' ''the nature and extent of the harm resulting from the violation,'' and the ''history of prior compliance with the administrative simplification provision, including violations by the covered entity or business associate,'' the ''financial condition of the covered entity or business associate,'' and ''such other matters as justice may require,'' as the five general factors the Secretary will consider in determining a civil money penalty. Under each of these categories, we proposed to reorganize and list the specific factors that may be considered.

In addition, in the first, second, and third factors, we proposed to add certain circumstances which may be considered in determining a penalty amount. Under the first factor, we proposed to add ''the number of individuals affected'' as relevant to the extent of a violation. Under the second factor, we proposed to add ''reputational harm'' to the specific circumstances which may be considered, to make clear that reputational harm is as cognizable a form of harm as physical or financial harm. Finally, in the third factor, the Department proposed to modify the phrase ''prior violations'' to ''indications of noncompliance,'' because use of the term ''violation'' is generally reserved for instances where the Department has made a formal finding of a violation through a notice of proposed determination. However, a covered entity's general history of HIPAA compliance is relevant in determining the amount of a civil money penalty within the penalty range.

The Department did not propose to modify the Secretary's discretion in how to apply the factors—i.e., as either mitigating or aggravating.

Overview of Public Comments

We received one comment requesting that the Department limit the number of mitigating factors it will consider when determining penalty amounts and apply

civil money penalties in every case of noncompliance, including where resolution and compliance have been achieved by informal means. The commenter also argued that a covered entity's or business associate's financial condition or financial difficulties should not be considered as mitigating factors in determining the amount of civil money penalties. The commenter recommended that penalties should apply to all violators except those who despite due diligence could not discover the violation, who reported the violation immediately, and who fully corrected the problem within 30 days of discovery.

We received two comments in support of considering reputational harm in the computation of civil money penalties. One commenter emphasized that reputational harm addresses harm to individuals' dignity interest and recommended the inclusion of ''other'' harm as well. However, another covered entity expressed concern that damages for reputational harm are difficult to quantify and, therefore, claims might lead to protracted litigation and expensive settlements, ultimately increasing the costs of health care. Finally, we received one comment requesting examples of situations involving a cognizable claim of reputational harm.

We also received several comments requesting that the Department continue to consider the degree of culpability when determining the amount of a civil money penalty. One commenter specifically recommended that the Department consider whether unauthorized access has occurred when determining civil money penalty amounts. We also received one comment suggesting that the Department revise proposed § 160.408(c) to recognize as a mitigating factor whether the current violation is inconsistent with an entity's prior history of compliance.

With respect to the evaluation of a covered entity's or business associate's history of prior compliance, we received a number of comments expressing concern that replacing ''violations'' with ''indications of noncompliance'' would create ambiguity, and would not adequately inform covered entities and business associates of the factors that the Department will consider when determining civil money penalty amounts. The commenters expressed concern that expanding the evaluation of prior compliance beyond documented, formal findings of noncompliance would permit the Department to rely on information of dubious credibility. Commenters requested that, to prevent uncertainty, the Department either retain the term ''violations'' or provide a clear definition, including examples, of ''indications of noncompliance.''

Finally, we received several comments requesting additional examples and guidance on how the Department will apply the factors in assessing penalty amounts.

Final Rule

The final rule adopts the proposed modifications. We do not eliminate the factors concerning an entity's financial condition, as such factors are based on the requirement in section 1128A(d) of the Social Security Act. We emphasize that the goal of enforcement is to ensure that violations do not recur without impeding access to care. Further, we note that an entity's financial condition can affect a civil money penalty in either direction, that is, while an entity in poor financial condition may face a lesser penalty if its financial condition affected its ability to comply, an entity with greater financial resources could be subject to higher penalties for violations, in part because it had the resources to maintain compliance.

When considering the nature of the violation, the Department intends to consider factors such as the time period during which the violation(s) occurred and the number of individuals affected. Such considerations reflect the nature of the violation, specifically with respect to potential violations that affect a large number of individuals, for example, where disclosure of protected health information in multiple explanation of benefits statements (EOBs) that were mailed to the wrong individuals resulted from one inadequate safeguard but affected a large number of beneficiaries. However, we do recognize that these specific circumstances might also be considered under § 160.406, with respect to counting violations. See 71 FR 8390, 8409.

Whether reputational harm is implicated in a HIPAA violation will be a fact-specific inquiry. We emphasize, however, that we do not consider reputational harm to arise solely from the unlawful disclosure of protected health information relating to medical diagnoses that may be considered especially sensitive, such as sexually transmitted infections or mental health disorders. Rather, the facts of the situation will determine whether reputational harm has occurred, such as whether the unlawful disclosure resulted in adverse effects on employment, standing in the community, or personal relationships. With respect to requests to consider ''other'' harm or whether unauthorized access has occurred, we reiterate that, in determining the nature and extent of the harm involved, we may consider all relevant factors, not just those expressly included in the text of the regulation.

Regarding the shift in terminology from ''history of violations'' to ''prior indications of noncompliance,'' we note that use of the terms ''violation'' or ''violate'' generally indicates that the Department has made a formal finding of a violation through a notice of proposed determination. Because the Department has a number of enforcement tools, such as informal resolution through a corrective action plan, the number of ''violations'' incurred by a covered entity or business associate does not constitute an accurate picture of a covered entity's or business associate's general history of compliance with all HIPAA Rules, which is relevant in determining the amount of a civil money penalty within the penalty range. See 71 FR 8390, 8408. As such, the Department modified the provision to reflect the Department's policy of considering the covered entity's or business associate's general history of compliance with the HIPAA Rules when determining a civil money penalty.

With regard to the phrase ''indications of noncompliance,'' we first clarify that a mere complaint does not constitute an indication of noncompliance. Instead, prior indications of noncompliance may refer to the number of times the Department has investigated an entity in the past and discovered indications of noncompliance that the Department resolved by informal means, such as satisfactory corrective action voluntarily taken by the covered entity. Finally, we agree that an entity's history of compliance—not only a history of noncompliance—is important, and will consider such a factor.

e. Section 160.410—Affirmative Defenses

Interim Final Rule and Proposed Rule

As noted above, the IFR made changes to the affirmatives defenses found in the Enforcement Rule at § 160.410 to implement the modifications to section 1176(b) of the Social Security Act made by section 13410(d) of the HITECH Act. Specifically, the IFR removed the previous affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation (since such violations are now punishable under the lowest tier of penalties), and by providing a prohibition on the

imposition of penalties for any violation that is corrected within a 30-day time period, as long as the violation was not due to willful neglect.

The proposed rule included additional modifications to § 160.410 to conform to the changes made to section 1176(b) by the HITECH Act. Specifically, we proposed to implement the revision of section 1176(b)(1) of the Social Security Act by providing in § 160.410(a)(1) and (2) that the affirmative defense of criminally ''punishable'' is applicable to penalties imposed prior to February 18, 2011, and on or after February 18, 2011, the Secretary's authority to impose a civil money penalty will only be barred to the extent a covered entity or business associate can demonstrate that a criminal penalty has been imposed. Additionally, the Department also proposed modifications to the affirmative defenses in § 160.410 for violations occurring prior to February 18, 2009, to ensure the prior definition of ''reasonable cause'' continued to apply in such circumstances and avoiding any potential issues regarding a retroactive application of the revised term.

Final Rule

The final rule adopts the proposed modifications to § 160.410. The Department did not receive any comments in response to the NPRM's proposed revisions to this section.

f. Section 160.412—Waiver

Prior to February 18, 2009, § 160.412 stated that ''[f]or violations described in § 160.410(b)(3)(i) that are not corrected within the period described in § 160.410(b)(3)(ii), the Secretary may waive the civil money penalty, in whole or in part, to the extent that payment of the penalty would be excessive relative to the violation.'' This language implicitly recognized a covered entity's ability to claim an affirmative defense to the imposition of a civil money penalty, under what was then § 160.410(b)(2), by establishing that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred. While section 13410(d) of the HITECH Act revised section 1176(b) of the Social Security Act to eliminate the affirmative defense for such violations, absent corrective action during a 30-day period, it did not revise the Secretary's waiver authority. As a result, the Enforcement IFR amended § 160.412 to reflect the revisions made to § 160.410 to provide that ''[r]egardless of whether violations occur before, on, or after February 18, 2009, the Secretary had the authority to provide a waiver for violations due to reasonable cause and not willful neglect that are not timely corrected (pursuant to the correction period in revised § 160.410(a)(3)(ii) or (b)(2)(ii), as applicable).'' See 74 FR 56129.

The proposed rule included conforming changes to § 160.412 to align the provision with the revisions to § 160.410. See 75 FR 40881. The proposed revision would effectively provide the Secretary with the authority to waive a civil money penalty, in whole or in part, for violations described in § 160.410(b)(2) (occurring prior to February 18, 2009, and due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated) or § 160.410(c) (occurring on or after February 18, 2009, and involving an establishment to the satisfaction of the Secretary that the violation is not due to willful neglect) and that are not corrected within the period specified under such paragraphs.

Overview of Public Comments

The Department received a few comments in response to the IFR regarding the Secretary's authority to waive the imposition of a civil money penalty for violations occurring on or after February 18, 2009, each of which urged that the Secretary's waiver authority be extended to apply also to penalties for violations of which a covered entity did not know, or through the exercise of reasonable diligence, would not have known, in addition to reasonable cause violations, because ''did not know'' violations are a less culpable category of violation than reasonable cause violations.

Final Rule

The final rule adopts the modifications to § 160.412 proposed in the NPRM, which addresses the concerns of the above commenters on the IFR.

g. Section 160.418—Penalty Not Exclusive

Proposed Rule

We proposed to revise this section to incorporate a reference to the provision of PSQIA at 42 U.S.C. 299b–22 that provides that penalties are not to be imposed under both PSQIA and the HIPAA Privacy Rule for the same violation.

Final Rule

The Department did not receive substantive public comment on this proposal. The final rule adopts the proposed modification to § 160.418.

h. Section 160.420—Notice of Proposed Determination

Interim Final Rule

The Enforcement IFR also amended § 160.420(a)(4) to add the requirement that, in addition to the proposed penalty amount, the Secretary identify in a notice of proposed determination the applicable violation category in § 160.404 upon which the proposed penalty amount is based. While not statutorily required, the Enforcement IFR included this amendment to provide covered entities and business associates with additional information that would increase their understanding of the violation findings in the notice of proposed determination.

Overview of Public Comment

The Department received three comments supporting this amendment.

Final Rule

The final rule retains the provision as modified in the IFR.

i. Calculation of the 30-Day Cure Period for Willful Neglect Violations

Interim Final Rule

In its discussion of the HITECH Act's revision of affirmative defenses, the Department noted that section 1176(b)(2)(A) of the Social Security Act still operates to exclude violations due to willful neglect from those that, if timely corrected, would be exempt from the Secretary's imposition of a civil money penalty. However, a covered entity's timely action to correct still would be determinative with respect to which of the two tiers of willful neglect penalty amounts would apply. To determine the appropriate penalty tier for such violations, the Department stated it would calculate the 30-day cure period in the same manner as described for determining whether an affirmative defense applied. That is, the Department would look at when a covered entity first had actual or constructive knowledge of a violation due to willful neglect, based on evidence gathered during its investigation, on a case-by-case basis. See 74 FR 56128 (October 30, 2009), 70 FR 20224, 20237–8 (April 18, 2005) and 71 FR 8390, 8410 (February 16, 2006) for prior, more detailed discussions about the Department's determination of when knowledge exists.

Because the Department recognized that the minimum penalty amount under the HITECH Act of a violation due to willful neglect that is corrected during the 30-day cure period is significantly less than that for a violation due to willful neglect that is not timely corrected (equating to a $40,000 minimum penalty amount difference), the IFR specifically requested comment on whether there are alternative approaches to calculating the beginning of the 30-day cure period for this purpose.

Overview of Public Comments

While a few commenters expressed support for utilizing the current scheme in determining which tier should apply to a violation due to willful neglect, other commenters expressed concerns with this approach due to the uncertainty with determining exactly when the cure period begins and that a business associate's knowledge of a violation could be imputed to the covered entity prior to the business associate notifying the covered entity, as well as concerns if the Secretary does not notify an entity of a potential violation in a timely manner. A few commenters suggested that the 30-day cure period begin once the Department notifies the covered entity of a complaint.

Final Rule

The final rule retains the policy that the 30-day cure period for violations due to willful neglect, like those not due to willful neglect, begins on the date that an entity first acquires actual or constructive knowledge of the violation and will be determined based on evidence gathered by the Department during its investigation, on a case-by-case basis.

First, the requirement that an entity have knowledge that a ''violation'' has occurred, and not only of the facts underlying the violation, is a higher standard than that which is often required by other law. Also, as a practical matter, the date an entity has actual or constructive knowledge of a violation will vary depending on the circumstances involved, and may be the result of notice by a workforce member or business associate, a complaint received by a health care consumer, or notification by the Department that a complaint has been filed. However, other sources of information exist that could establish knowledge, including internal indications of a potential noncompliance such as unusual access or audit log activity.

While we understand commenters' concerns relating to the uncertainty inherent to constructive knowledge, we believe that it provides an appropriate incentive that is consistent with the strengthened enforcement of the HIPAA Rules, as provided in the HITECH Act. Reliance on notification by a complainant or the Department would not encourage self-correction or an entity's establishment of a compliance program that proactively prevents, detects and corrects indications of noncompliance. If the cure period were solely based on external notification, it is quite possible that entities would have little or no incentive to make corrections of noncompliance until long after an incident occurred, if ever. In response to concerns that constructive knowledge may be imputed to the principal when an agent fails to notify the responsible entity, we note that an agent must be acting within the scope of agency for a covered entity or a business associate to be liable for the agent's acts or failures to act. An agent that fails to notify a covered entity or business associate may be acting outside its scope of authority as an agent. In such a circumstance, the agent's knowledge is not imputed to the principal under the Federal Common Law of Agency.

Finally, an entity will have the opportunity to submit evidence establishing its knowledge or lack of knowledge, during the Department's investigation. Entities will also have a right to request a hearing to appeal a finding about knowledge in a notice of proposed determination to the extent they believe the finding is not based on a preponderance of the evidence. An administrative law judge would then review the finding and affirm or modify it.

Response to Other Public Comments

Comment: A few commenters suggested that 30 days may not be sufficient for a covered entity to complete corrective action, particularly with respect to large organizations with complex systems, structures and relationships. One commenter suggested there should be a process available to allow an organization to apply for a reasonable extension to complete the cure.

Response: In response to commenters' concern about the length of the 30-day cure period, we note that this time period is defined by statute at section 1176(b) of the Social Security Act, and was not modified by section 13410(d) of the HITECH Act. Thus, we believe there is no authority upon which to base a modification to the length of the cure period.

Comment: One commenter requested that the Department clarify whether the new enforcement provisions will apply to violations of all HIPAA Administrative Simplification provisions or just to the privacy and security requirements.

Response: The enforcement regulations at 45 CFR Part 160, Subparts C, D, and E, relate to compliance with, and the enforcement of, all of the Administrative Simplification regulations adopted under subtitle F of Title II of HIPAA, including the Standards for Electronic Transactions and Code Sets (Transactions and Code Sets Rule(s) (referred to in both a singular and plural sense); Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule); Standard Unique Employer Identifier (EIN Rule); Security Standards (HIPAA Security Rule); and Standard Unique Health Identifier for Health Care Providers (NPI Rule). In addition, the Enforcement Rule applies to the Breach Notification Rule for HIPAA covered entities and business associates.

C. Subparts A and C of Part 164: General Provisions and Modifications to the Security Rule

We proposed implementing modifications to the Security Rule as a result of the HITECH Act and to make certain other changes. Below we respond to comments received on the proposed changes as well as describe the final rule provisions. We also discuss the final technical and conforming changes to the general provisions in Subpart A of Part 164, which applies to the Security, Privacy, and Breach Notification Rules, and respond to comments where substantive comments were received on these changes.

1. Technical Changes to Subpart A—General Provisions

a. Section 164.102—Statutory Basis

This section sets out the statutory basis of Part 164. We proposed and include in this final rule a technical change to include a reference to the provisions of sections 13400 through 13424 of the HITECH Act upon which the regulatory changes discussed below are based.

b. Section 164.104—Applicability

This section sets out to whom Part 164 applies. We proposed to replace the existing paragraph (b) with an applicability statement for business associates, consistent with the provisions of the HITECH Act. Paragraph (b) makes clear that, where provided, the standards, requirements, and implementation specifications of the HIPAA Privacy, Security, and

Breach Notification Rules apply to business associates. We also proposed to remove as unnecessary the existing language in § 164.104(b) regarding the obligation of a health care clearinghouse to comply with § 164.105 relating to organizational requirements of covered entities. This final rule adopts these changes as proposed.

c. Section 164.105—Organizational Requirements

Section 164.105 outlines the organizational requirements and implementation specifications for health care components of covered entities and for affiliated covered entities. As § 164.105 now also applies to Subpart D of Part 164 regarding breach notification for unsecured protected health information, we proposed to remove several specific references to Subparts C and E throughout this section to make clear that the provisions of this section also apply to Subpart D of Part 164. The final rule adopts these modifications.

In addition, we proposed the following modifications to this section.

i. Section 164.105(a)(2)(ii)(C)–(E)

Proposed Rule

As a covered entity's obligation to ensure that a health care component complies with the Privacy and Security Rules is already set out at § 164.105(a)(2)(ii), we proposed to modify this section to remove as unnecessary paragraphs (C) and (D), which pertain to the obligation of a covered entity to ensure that any component that performs business associate-like activities and is included in the health care component complies with the requirements of the Privacy and Security Rules, and to re-designate paragraph (E) as (C). Additionally, we requested comment on whether we should require, rather than permit as was the case at § 164.105(a)(2)(iii)(C), a covered entity that is a hybrid entity to include a component that performs business associate-like activities within its health care component so that such components are directly subject to the Rules.

Overview of Public Comments

Several commenters recommended that hybrid entities should retain the flexibility to either include or exclude business associates from the healthcare component. Two of these commenters stated this option would allow the covered entity to distinguish the functions and responsibilities of the business associate as separate from the health care component, which would result in better compliance, as covered entities would evaluate each business associate separately for compliance purposes. Further, commenters argued that, as the covered entity is ultimately legally liable for compliance on the part of the organization, such a modification is not necessary.

Additionally, several commenters stated that requiring a hybrid entity to include business associate departments is excessive and burdensome. Some of these commenters further stated that business associate departments of a hybrid entity will likely commit limited time, personnel, and staff hours to Privacy and Security Rule compliance and suggested that the hybrid entity should implement applicable entity-wide policies and procedures and separately ensure that business associate departments implement specific practices scaled to the business associate's use or disclosure of protected health information.

In contrast, several commenters supported the proposed change. Several of these commenters suggested that the modification would better facilitate compliance, because requiring the covered entity to include the business associate department in the health care component would better protect the protected health information held by the business associate and would ensure consistent standards within the health care component of the covered entity.

Final Rule

Many covered entities perform both covered and non-covered functions as part of their business operations. For such covered entities, the entire entity is generally required to comply with the Privacy Rule. However, the hybrid entity provisions of the HIPAA Rules permit the entity to limit the application of the Rules to the entity's components that perform functions that would make the component a ''covered entity'' if the component were a separate legal entity. Specifically, this provision allows an entity to designate a health care component by documenting the components of its organization that perform covered entity functions. The effect of such a designation is that most of the requirements of the HIPAA Rules apply only to the designated health care component of the entity and not to the functions the entity performs that are not included in the health care component. While most of the HIPAA Rules' requirements apply only to the health care component, the hybrid entity retains certain oversight, compliance, and enforcement obligations.

We explained in the preamble to the 2002 modifications to the Privacy Rule that the Rule provides hybrid entities with discretion as to whether or not to include business associate divisions within the health care component. However, a disclosure of protected health information from the health care component to any other division that is not part of the health care component, including a business associate division, is treated the same as a disclosure outside the covered entity. As a result, because an entity generally cannot have a business associate agreement with itself, a disclosure from the health care component to the business associate division(s) of the entity likely would require individual authorization. See 67 FR 53182, 53205 (Aug. 14, 2002).

Importantly, after this final rule, business associates, by definition, are separately and directly liable for violations of the Security Rule and for violations of the Privacy Rule for impermissible uses and disclosures pursuant to their business associate contracts. With respect to a hybrid entity, however, not including business associate functions within the health care component of a hybrid entity could avoid direct liability and compliance obligations for the business associate component. Thus, we agree with the commenters that supported requiring inclusion of business associate functions inside the health care component of a hybrid entity. As such, the final rule requires that the health care component of a hybrid entity include all business associate functions within the entity.

Response to Other Public Comments

Comment: One commenter requested that the Department revise the definitions of ''hybrid entity'' to permit business associates to designate a health care component.

Response: A business associate performs one or more functions on behalf of a covered entity (or, in this final rule, another business associate). As a business associate is only subject to the HIPAA Rules with respect to the protected health information it maintains, uses, or discloses on behalf of a covered entity (or business associate) and not to other information it may maintain, including health information, there is no need for a business associate to designate one or more health care components.

Comment: One commenter asked whether an employer that operates an on-site clinic for the treatment of employees functions as a hybrid entity.

Response: An entity that maintains an on-site clinic to provide health care to one or more employees may be a HIPAA covered provider to the extent the clinic performs one or more covered

transactions electronically, such as billing a health plan for the services provided. If covered, the entity need not become a hybrid entity so as to avoid applying the Privacy Rule to health information the entity holds in its role as employer, such as sick leave requests of its employees. Such information is already excluded from the definition of ''protected health information'' as employment records and thus, the Privacy Rule does not apply to this information. However, the identifiable health information the entity holds as a covered health care provider (e.g., the information the clinic holds about employees who have received treatment) is protected health information and generally may not be shared with the employer for employment purposes without the individual's authorization.

ii. Section 164.105(a)(2)(iii)(C)

We proposed to modify this section to re-designate § 164.105(a)(2)(iii)(C) as (D), and to include a new paragraph (C), which makes clear that, with respect to a hybrid entity, the covered entity itself, and not merely the health care component, remains responsible for complying with §§ 164.314 and 164.504 regarding business associate arrangements and other organizational requirements. Hybrid entities may need to execute legal contracts and conduct other organizational matters at the level of the legal entity rather than at the level of the health care component. The final rule adopts this change.

iii. Section 164.105(b)(1)

The final rule fixes a minor typographical error in this paragraph by redesignating the second paragraph (1) as paragraph (2).

iv. Section 164.105(b)(2)(ii)

The final rule simplifies this paragraph by collapsing subparagraphs (A), (B), and (C) regarding the obligations of an affiliated entity to comply with the Privacy and Security Rules into one provision.

d. Section 164.106—Relationship to Other Parts

The final rule adds a reference in this provision to business associates, consistent with their inclusion elsewhere throughout the other HIPAA Rules.

2. Modifications to the HIPAA Security Rule in Subpart C

a. Business Associates

Proposed Rule

Before the HITECH Act, the Security Rule did not directly apply to business associates of covered entities. However, section 13401 of the HITECH Act provides that the Security Rule's administrative, physical, and technical safeguards requirements in §§ 164.308, 164.310, and 164.312, as well as the Rule's policies and procedures and documentation requirements in § 164.316, apply to business associates in the same manner as these requirements apply to covered entities, and that business associates are civilly and criminally liable for violations of these provisions.

To implement section 13401 of the HITECH Act, we proposed to insert references in Subpart C to ''business associate'' following references to ''covered entity,'' as appropriate, to make clear that these provisions of the Security Rule also apply to business associates. In addition, we proposed additional changes to §§ 164.306, 164.308, 164.312, 164.314, and 164.316 of the Security Rule, as discussed below.

Overview of Public Comments

Some commenters argued that the time, implementation expense, transaction cost, and liability cost burdens on business associates and subcontractors to comply with the Security Rule, especially small and mid-size entities, would be significant. Other commenters supported the direct application of the Security Rule to business associates and subcontractors.

Final Rule

We adopt the modifications to the Security Rule as proposed to implement the HITECH Act's provisions extending direct liability for compliance with the Security Rule to business associates. In response to the concerns raised regarding the costs of compliance, we note that the Security Rule currently requires a covered entity to establish a business associate agreement that requires business associates to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that they create, receive, maintain, or transmit on behalf of the covered entity as required by the Security Rule; and to ensure that any agent, including a subcontractor, to whom they provide such information agrees to implement reasonable and appropriate safeguards to protect it. See § 164.314(a). Consequently, business associates and subcontractors should already have in place security practices that either comply with the Security Rule, or that require only modest improvements to come into compliance with the Security Rule requirements.

Moreover, the requirements of the Security Rule were designed to be technology neutral and scalable to all different sizes of covered entities and business associates. Covered entities and business associates have the flexibility to choose security measures appropriate for their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any given Security Rule standard. In deciding which security measures to use, a covered entity or business associate should take into account its size, capabilities, the costs of the specific security measures, and the operational impact. Thus, the costs of implementing the Security Rule for large, mid-sized, or small business associates will be proportional to their size and resources.

Notwithstanding the above, based on the comments, we acknowledge that some business associates, particularly the smaller or less sophisticated business associates that may have access to electronic protected health information for limited purposes, may not have engaged in the formal administrative safeguards such as having performed a risk analysis, established a risk management program, or designated a security official, and may not have written policies and procedures, conducted employee training, or documented compliance as the statute and these regulations would now require. For these business associates, we include an estimate for compliance costs below in the regulatory impact analysis. We also refer these business associates to our educational papers and other guidance on compliance with the HIPAA Security Rule found at: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule*. These materials provide guidance on conducting risk analyses and implementing the other administrative safeguards required by the Security Rule, which may prove helpful to these business associates and facilitate their compliance efforts.

b. Section 164.306—Security Standards: General Rules

Proposed Rule

Section 164.306 sets out the general rules that apply to all of the security

standards and implementation specifications that follow in the Security Rule. We proposed technical revisions to § 164.306(e) to more clearly indicate that covered entities and business associates must review and modify security measures as needed to ensure the continued provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures accordingly.

Final Rule

The Department did not receive substantive public comment on this proposal. The final rule adopts the modifications to § 164.306 as proposed.

c. Section 164.308—Administrative Safeguards

Proposed Rule

We proposed a technical change to § 164.308(a)(3)(ii)(C) regarding security termination procedures for workforce members, to add the words ''or other arrangement with'' after ''employment of'' in recognition of the fact that not all workforce members are employees (e.g., some may be volunteers) of a covered entity or business associate. We also proposed a number of modifications to § 164.308(b) to conform to modifications proposed in the definition of ''business associate.'' Section 164.308(b) provides that a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information only if the covered entity has a contract or other arrangement in place to ensure the business associate will appropriately safeguard the protected health information. Section164.308(b)(2) contains several exceptions to this general rule for certain situations that do not give rise to a business associate relationship, such as where a covered entity discloses electronic protected health information to a health care provider concerning the treatment of an individual. We proposed to remove these exceptions from this provision, since as discussed above, they would now be established as exceptions to the definition of ''business associate.''

In addition, we proposed to modify § 164.308(b)(1) and (2) to clarify that covered entities are not required to obtain satisfactory assurances in the form of a contract or other arrangement with a business associate that is a subcontractor; rather, it is the business associate that must obtain the required satisfactory assurances from the subcontractor to protect the security of electronic protected health information.

Finally, we proposed to remove the provision at § 164.308(b)(3), which provides that a covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the Security Rule's business associate provisions, as a covered entity's actions as a business associate of another covered entity would now be directly regulated by the Security Rule's provisions that apply to business associates.

Overview of Public Comments

One commenter asked for confirmation that the changes to § 164.308 would require a covered entity to enter into a business associate agreement with its own business associate and not any subcontractors of those business associates.

Final Rule

The final rule adopts the proposed modifications to § 164.308. Section 164.308(b) expressly provides that a covered entity is not required to enter into a business associate agreement with a business associate that is a subcontractor; rather, this is the obligation of the business associate that has engaged the subcontractor to perform a function or service that involves the use or disclosure of protected health information.

d. Section 164.314—Organizational Requirements

Proposed Rule

While Section 13401 of the HITECH Act does not expressly include § 164.314 among the provisions for which business associates are directly liable, it states that § 164.308 of the Security Rule applies to business associates ''in the same manner'' that the provision applies to covered entities. Section 164.308(b) requires a covered entity's business associate agreements to conform to the requirements of § 164.314. Accordingly, in order for § 164.308(b) to apply to business associates in the same manner as it applies to covered entities, we proposed to revise § 164.314 to reflect that it is also applicable to agreements between business associates and subcontractors that create, receive, maintain, or transmit electronic protected health information.

We also proposed a number of modifications to streamline the requirements of § 164.314. First, since a business associate for purposes of the Security Rule is also always a business associate for purposes of the Privacy Rule, we proposed to remove contract provisions that were merely duplicative of parallel provisions in the Privacy Rule's business associate contract provisions at § 164.504. We also proposed to remove the specific requirements under § 164.314(a)(2)(ii) for other arrangements, such as a memorandum of understanding when both a covered entity and business associate are governmental entities, and instead simply refer to the parallel Privacy Rule requirements at § 164.504(e)(3).

Second, we proposed conforming modifications to the remaining contract requirements in § 164.314(a)(2)(i) to provide that such contracts must require a business associate to comply with the Security Rule, to ensure any subcontractors enter into a contract or other arrangement to protect the security of electronic protected health information; and with respect to the reporting of security incidents by business associates to covered entities, to report to the covered entity breaches of unsecured protected health information as required by § 164.410 of the breach notification rules.

Third, we proposed to add a provision at § 164.314(a)(2)(iii) that provides that the requirements of this section for contracts or other arrangements between a covered entity and business associate would apply in the same manner to contracts or other arrangements between business associates and subcontractors required by the proposed requirements of § 164.308(b)(4). For example, under these provisions, a business associate contract between a business associate and a business associate subcontractor would need to provide that the subcontractor report any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410, to the business associate. This would mean that if a breach of unsecured protected health information occurs at or by a second tier subcontractor, the subcontractor must notify the business associate subcontractor with which it contracts of the breach, which then must notify the business associate which contracts with the covered entity of the breach, which then must notify the covered entity of the breach. The covered entity then notifies the affected individuals, the Secretary, and, if applicable, the media, of the breach, unless it has delegated such responsibilities to a business associate. Finally, we proposed to remove the reference to subcontractors in § 164.314(b)(2)(iii) regarding amendment of group health plan documents as a condition of disclosure of protected health information to a plan sponsor, as unnecessary and to avoid

confusion with the use of the term subcontractor when referring to subcontractors that are business associates.

Final Rule

The Department did not receive substantive public comment on these proposed changes. The final rule adopts the modifications as proposed.

Response to Other Public Comments

Comment: One commenter suggested that business associate agreements should be an ''addressable'' requirement under the Security Rule.

Response: The HITECH Act does not remove the requirements for business associate agreements under the HIPAA Rules. Therefore, we decline to make the execution of business associate agreements an ''addressable'' requirement under the Security Rule.

Comment: One commenter recommended that the Department remove the ''addressable'' designation from the Security Rule, because such designations lead to ambiguity in the application of the Security Rule in the health care industry.

Response: We decline to adopt this recommendation. The Security Rule is structured to be both scalable and flexible, so that entities of different types and sizes can implement the standards and implementation specifications in a manner that is reasonable and appropriate for their circumstances. We do not mandate the use of specific technologies, or require uniform policies and procedures for compliance, because we recognize the diversity of regulated entities and appreciate the unique characteristics of their environments.

Comment: Two commenters suggested providing subcontractors with additional time to comply with the provisions of the Security Rule.

Response: We decline to delay application of the requirements under the Security Rule to subcontractors beyond the compliance dates provided by this final rule. As we emphasized above, the Security Rule already requires covered entities to establish business associate agreements that require business associates to ensure that their subcontractors implement reasonable and appropriate safeguards to protect the security of electronic protected health information they handle.

Comment: A few commenters proposed alternative ways to apply security requirements to subcontractors, such as exempting subcontractors from compliance with the Security Rule if they have already completed security assessments and met the security requirements under other State and Federal laws or only requiring subcontractors to comply with the minimum necessary standard and to utilize ''reasonable'' security measures with regard to protected health information.

Response: We decline to adopt an exemption or otherwise limit subcontractors' responsibility to safeguard individuals' electronic protected health information. To ensure appropriate and strong security protections for electronic protected health information, subcontractors are required to comply with the Security Rule to the same extent as business associates with a direct relationship with a covered entity.

D. Subpart E of Part 164: Modifications to the Privacy Rule

The NPRM proposed a number of changes to the Privacy Rule to implement certain provisions of the HITECH Act, as well as certain modifications to improve the workability and effectiveness of the Rule and to conform the Privacy Rule to PSQIA. The section-by-section description below of the final rule discusses the proposed and final changes and responds to public comments

1. Section 164.500—Applicability

Section 13404 of the HITECH Act makes specific requirements of the Privacy Rule applicable to business associates and creates direct liability for noncompliance by business associates with regard to those requirements.

Proposed Rule

In accordance with section 13404 of the HITECH Act, we proposed language in § 164.500 to clarify that, where provided, the standards, requirements, and implementation specifications of the Privacy Rule apply to business associates.

Overview of Public Comments

One commenter suggested that the Department expand the applicability of the Privacy Rule to all entities that handle individually identifiable health information. Some commenters requested clarification as to which provisions of the Privacy Rule apply directly to business associates, and one commenter recommended applying all of the provisions of the Privacy Rule to business associates, including requiring business associates to implement reasonable safeguards, train employees, and designate a privacy official.

Final Rule

The final rule implements the proposed revisions to § 164.500. While we understand commenters' concerns regarding the uses and disclosures of health information by entities not covered by the Privacy Rule, the Department is limited to applying the HIPAA Rules to those entities covered by HIPAA (i.e., health plans, health care clearinghouses, and health care providers that conduct covered transactions) and to business associates, as provided under the HITECH Act.

As we discuss further below, section 13404 of the HITECH Act creates direct liability for impermissible uses and disclosures of protected health information by a business associate of a covered entity ''that obtains or creates'' protected health information ''pursuant to a written contract or other arrangement described in § 164.502(e)(2)'' and for compliance with the other privacy provisions in the HITECH Act. Section 13404 does not create direct liability for business associates with regard to compliance with all requirements under the Privacy Rule (i.e., does not treat them as covered entities). Therefore, under the final rule, a business associate is directly liable under the Privacy Rule for uses and disclosures of protected health information that are not in accord with its business associate agreement or the Privacy Rule. In addition, a business associate is directly liable for failing to disclose protected health information when required by the Secretary to do so for the Secretary to investigate and determine the business associate's compliance with the HIPAA Rules, and for failing to disclose protected health information to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of protected health information. See § 164.502(a)(3) and (a)(4). Further, a business associate is directly liable for failing to make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. See § 164.502(b). Finally, business associates are directly liable for failing to enter into business associate agreements with subcontractors that create or receive protected health information on their behalf. See § 164.502(e)(1)(ii). As was the case under the Privacy Rule before the HITECH Act, business associates remain contractually liable for all other Privacy Rule obligations that are included in

their contracts or other arrangements with covered entities.

2. Section 164.501—Definitions

a. Definition of ''Health Care Operations''

Proposed Rule

PSQIA provides, among other things, that Patient Safety Organizations (PSOs) are to be treated as business associates of covered health care providers. Further, PSQIA provides that the patient safety activities of PSOs are deemed to be health care operations of covered health care providers under the Privacy Rule. See 42 U.S.C. 299b–22(i). To conform to these statutory provisions, we proposed to amend paragraph (1) of the definition of ''health care operations'' to include an express reference to patient safety activities, as defined in the PSQIA implementing regulation at 42 CFR 3.20. Many health care providers participating in the voluntary patient safety program authorized by PSQIA are HIPAA covered entities. PSQIA acknowledges that such providers must also comply with the Privacy Rule and deems patient safety activities to be health care operations under the Privacy Rule. While such types of activities are already encompassed within paragraph (1) of the definition, which addresses various quality activities, we proposed to expressly include patient safety activities within paragraph (1) of the definition of health care operations to conform the definition to PSQIA and to eliminate the potential for confusion. This modification also addresses public comments the Department received during the rulemaking period for the PSQIA implementing regulations, which urged the Department to modify the definition of ''health care operations'' in the Privacy Rule to expressly reference patient safety activities so that the intersection of the Privacy and PSQIA Rules would be clear. See 73 FR 70732, 70780 (Nov. 21, 2008).

Overview of Public Comments

The Department received comments supporting the inclusion of patient safety activities in the definition of ''health care operations.''

Final Rule

The final rule adopts the proposed modification.

b. Definition of ''Marketing''

Proposed Rule

The Privacy Rule requires covered entities to obtain a valid authorization from individuals before using or disclosing protected health information to market a product or service to them. See § 164.508(a)(3). Section 164.501 defines ''marketing'' as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Paragraph (1) of the definition includes a number of exceptions to marketing for certain health-related communications: (1) Communications made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communications, including communications about: The entities participating in a healthcare provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (2) communications made for the treatment of the individual; and (3) communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. A covered entity is permitted to make these excepted communications without an individual's authorization as either treatment or health care operations communications, as appropriate, under the Privacy Rule. In addition, the Privacy Rule does not require a covered entity to obtain individual authorization for face-to-face communications or to provide only promotional gifts of nominal value to the individual. See § 164.508(a)(3)(i). However, a covered entity must obtain prior written authorization from an individual to send communications to the individual about non-health related products or services or to give or sell the individual's protected health information to a third party for marketing. Still, concerns have remained about the ability under these provisions for a third party to pay a covered entity to send health-related communications to an individual about the third party's products or services.

Section 13406(a) of the HITECH Act limits the health-related communications that may be considered health care operations and thus, that are excepted from the definition of ''marketing'' under the Privacy Rule, to the extent a covered entity receives or has received direct or indirect payment in exchange for making the communication. In cases where the covered entity would receive such payment, the HITECH Act at section 13406(a)(2)(B) and (C) requires that the covered entity obtain the individual's valid authorization prior to making the communication, or, if applicable, prior to its business associate making the communication on its behalf in accordance with its written contract. Section 13406(a)(2)(A) of the HITECH Act includes an exception to the payment limitation for communications that describe only a drug or biologic that is currently being prescribed to the individual as long as any payment received by the covered entity in exchange for making the communication is reasonable in amount. Section 13406(a)(3) of the Act provides that the term ''reasonable in amount'' shall have the meaning given to such term by the Secretary in regulation. Finally, section 13406(a)(4) of the Act clarifies that the term ''direct or indirect payment'' does not include any payment for treatment of the individual. We believe Congress intended that these provisions curtail a covered entity's ability to use the exceptions to the definition of ''marketing'' in the Privacy Rule to send communications to the individual that are motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's health care, despite the communication being about a health-related product or service.

To implement the marketing limitations of the HITECH Act, we proposed a number of modifications to the definition of ''marketing'' at § 164.501. In paragraph (1) of the definition of ''marketing,'' we proposed to maintain the general concept that ''marketing'' means ''to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.'' In paragraph (2) of the definition, we proposed to include three exceptions to this definition to encompass certain treatment and health care operations communications about health-related products or services. First, we proposed to exclude from the definition of ''marketing'' certain health care operations communications, except where, as provided by the HITECH Act, the covered entity receives financial remuneration in exchange for making the communication. This would encompass communications to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, as well as communications for case management

or care coordination, contacting of individuals with information about treatment alternatives, and related functions (to the extent these activities did not constitute ''treatment'').

Although the HITECH Act uses the term ''direct or indirect payment'' to describe the limitation on permissible health care operations disclosures, the proposed rule substituted the term ''financial remuneration'' to avoid confusion with the term ''payment,'' which is defined in the Privacy Rule to mean payment for health care, and for consistency with the Privacy Rule's current authorization requirement for marketing at § 164.508(a)(3), which uses the term ''remuneration.'' We proposed to define ''financial remuneration'' in paragraph (3) of the definition of ''marketing'' to mean direct or indirect payment from or on behalf of a third party whose product or service is being described. We also proposed to make clear, in accordance with section 13406(a)(4) of the HITECH Act, that financial remuneration does not include any direct or indirect payment for the treatment of an individual.

Additionally, because the HITECH Act refers expressly to ''payment,'' rather than remuneration more generally, the proposed rule specified that only the receipt of financial remuneration in exchange for making a communication, as opposed to in-kind or any other type of remuneration, is relevant for purposes of the definition of marketing. We also proposed a conforming change to the required authorization provisions for marketing communications at § 164.508(a)(3) to add the term ''financial'' before ''remuneration'' and to refer to the new definition of ''financial remuneration.''

The proposed rule emphasized that financial remuneration for purposes of the definition of ''marketing'' must be in exchange for making the communication itself and be from or on behalf of the entity whose product or service is being described. Thus, under these proposed provisions, an authorization would be required prior to a covered entity making a communication to its patients regarding the acquisition of, for example, new state of the art medical equipment if the equipment manufacturer paid the covered entity to send the communication to its patients; but not if a local charitable organization, such as a breast cancer foundation, funded the covered entity's mailing to patients about new state of the art mammography screening equipment. Furthermore, it would not constitute marketing and no authorization would be required if a hospital sent flyers to its patients announcing the opening of a new wing where the funds for the new wing were donated by a third party, since the financial remuneration to the hospital from the third party was not in exchange for the mailing of the flyers.

Second, we proposed to include the statutory exception to marketing at section 13406(a)(2)(A) for communications regarding refill reminders or otherwise about a drug or biologic that is currently being prescribed for the individual, provided any financial remuneration received by the covered entity for making the communication is reasonably related to the covered entity's cost of making the communication. The Act expressly identifies these types of communications as being exempt from the remuneration limitation only to the extent that any payment received for making the communication is reasonable in amount. We requested comment on the scope of this exception, that is, whether communications about drugs that are related to the drug currently being prescribed, such as communications regarding generic alternatives or new formulations of the drug, should fall within the exception. We also requested comment on the types and amount of costs that should be allowed under this provision. We noted that we had considered proposing a requirement that a covered entity could only receive financial remuneration for making such a communication to the extent it did not exceed the actual cost to make the communication. However, because we were concerned that such a requirement would impose the additional burden of calculating the costs of making each communication, we proposed to allow costs that are reasonably related to a covered entity's cost of making the communication.

Third, we proposed to exclude from marketing treatment communications about health-related products or services by a health care provider to an individual, including communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual, provided, however, that if the communications are in writing and financial remuneration is received in exchange for making the communications, certain notice and opt out conditions are met. While section 13406(a) of the HITECH Act expressly provides that a communication to an individual about a health-related product or service where the covered entity receives payment from a third party in exchange for making the communication shall not be considered a *health care operation* (emphasis added) under the Privacy Rule, and thus is marketing, it is unclear how Congress intended these provisions to apply to treatment communications between a health care provider and a patient. Specifically, it is unclear whether Congress intended to restrict only those subsidized communications about products and services that are less essential to an individual's health care (i.e., those classified as health care operations communications) or all subsidized communications about products and services, including treatment communications. Given this ambiguity and to avoid undue interference with treatment communications between the individual and a health care provider, we proposed to continue to allow subsidized treatment communications, but conditioned on providing the individual with notice and an opportunity to opt out of receiving such communications. Specifically, to ensure the individual is aware that he or she may receive subsidized treatment communications from his or her provider and has the opportunity to elect not to receive them, the proposed rule would have required at § 164.514(f)(2) that: (1) The covered health care provider's notice of privacy practices include a statement informing individuals that the provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration from a third party in exchange for making the communication, and the individual has a right to opt out of receiving such communications; and (2) the treatment communication itself disclose the fact of remuneration and provide the individual with a clear and conspicuous opportunity to elect not to receive any further such communications. We requested comment on how the opt out should apply to future subsidized treatment communications (i.e., should the opt out prevent all future subsidized treatment communications by the provider or just those dealing with the particular product or service described in the current communication?). We also requested comment on the workability of requiring health care providers that intend to send subsidized treatment communications to individuals to provide an individual with the opportunity to opt out of receiving such communications prior to the individual receiving the first communication and what mechanisms

could be put into place to implement such a requirement.

Given that the new marketing limitations on the receipt of remuneration by a covered entity would apply differently depending on whether a communication is for treatment or health care operations purposes, and that distinguishing such communications may in many cases call for close judgments, we requested comment on the alternatives of excluding treatment communications altogether even if they involve financial remuneration from a third party or requiring individual authorization for both treatment and health care operations communications made in exchange for financial remuneration.

Finally, we proposed to remove the language defining as marketing an arrangement between a covered entity and any other entity in which the covered entity discloses protected health information to the other entity, in exchange for remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service, since such activity would now constitute a prohibited ''sale'' of protected health information under section 13405(d) of the HITECH Act and the proposed rule.

Overview of Public Comments

Several commenters asked as a general matter that the final rule retain the current definition of ''marketing'' and that no changes to this provision be implemented. With respect to subsidized treatment communications, many commenters expressed support for the decision in the NPRM to not require authorizations for such communications, and several argued for removing even the opt out requirement. Other commenters believed that all communications in which the covered entity receives financial remuneration for making the communication, regardless of whether the communication is for treatment purposes, should be considered marketing and require authorization.

While many commenters were generally in support of not requiring authorization for treatment communications, at the same time, several commenters expressed concern with the difficulty of distinguishing between treatment communications and communications for health care operations purposes. These commenters stated that additional clarification regarding this distinction would be needed to be able to implement the NPRM's marketing provisions. Several commenters stated that while the distinction may be clear in some limited circumstances, there are other circumstances where it may be difficult for covered entities to determine what type of communication they are sending and whether authorization or just disclosure in the notice of privacy practices and the opportunity to opt out would be required. For example, while the NPRM stated that whether a communication is being made for treatment purposes or for health care operations purposes would depend on the extent to which the covered entity is making the communication in a population-based fashion (health care operations) or to further the treatment of a particular individual's health care status or condition (treatment), many commenters stated that there may be circumstances in which a covered entity provides a population-based communication to further the treatment of the health care status or condition of an entire group of individuals. Other commenters suggested that the distinction between communications for treatment and those for health care operations purposes should be made based on the entity providing the communication: If a health care provider is providing the communication, it should be deemed for treatment purposes; however, if the communication is made by a covered entity other than a health care provider, the determination should be based on whether the communication is individual (treatment) or population based (health care operations).

With respect to the subsidized treatment communications, commenters opposed to the opt out notification generally took one of three positions: All such communications should require authorizations to best protect patient privacy; an opt in method would better permit individuals to make more informed choices about whether to receive such communications; or a covered entity should be permitted to make these communications without an opportunity to opt out, because of unintended effects that may adversely affect the quality of care provided. Some commenters asked, if the opt out requirement is retained, that OCR ensure that covered entities are given significant flexibility in determining how best to implement the opt out requirement.

Additionally, the vast majority of commenters did not believe there should be an opportunity to opt out of receiving subsidized treatment communications prior to receipt of the first such communication. The commenters believed that requiring an opportunity to opt out prior to the first communication would be too costly and burdensome for most covered entities. Many also noted that the statement in the notice of privacy practices, which would inform individuals of their option to opt out of receiving subsidized treatment communications, could serve as an opportunity to opt out before the first communication. Some commenters expressed concern even with including a statement in the notice of privacy practices because of the cost associated with modifying notices to do so.

With respect to the scope of the proposed opt out, most commenters believed that the opt out should apply only to subsidized treatment communications related to a specific product or service and should not apply universally to all similar future communications from the covered entity. These commenters stated that it would be difficult for an individual to elect, in a meaningful way, not to receive all future subsidized treatment communications because he or she would not know exactly what he or she is opting out of without receiving at least one communication. Other commenters believed that while a product or service-specific application of the opt out would be ideal, it is simply unrealistic and infeasible for covered entities to be able to implement such a policy. These commenters stated that a universal opt out, which would apply to all future subsidized treatment communications, would be much simpler and easier for covered entities to implement. Additionally, while some commenters believed that individuals should be able to decide whether they want to opt out of specific subsidized treatment communications or all future such communications, most commenters supported giving covered entities the flexibility to determine the scope of this opt out provision based on their own specific capabilities. Many of these commenters also suggested that the final rule permit individuals who have opted out of receiving such communications to opt back in to receive future notices using the same methods through which the individuals had opted out.

The Department also received several comments on the definition of ''financial remuneration.'' Several commenters supported the NPRM's definition of ''financial remuneration''; however, many commenters asked for clarification regarding the scope of the definition and the meaning of the phrase ''direct or indirect payment.'' For example, some commenters asked for confirmation that non-financial benefits did not constitute financial

remuneration, while other commenters wanted the exception for refill reminders (that is, the communication is not marketing as long as the financial remuneration does not exceed the related costs of the communication) to apply more broadly to all marketing communications. Additionally, some commenters suggested that the final rule clarify that only financial remuneration in exchange for sending a communication triggers either the authorization or the statement of notice and opt out requirement and not the exchange of financial remuneration for the development or funding for programs, which may include the sending of a communication. These commenters generally suggested that the final rule give covered entities the flexibility to determine whether the financial remuneration received is truly in exchange for making the communication.

We received a great deal of public comment on the exception to the definition of ''marketing'' for providing refill reminders or to otherwise communicate about a drug or biologic currently being prescribed for the individual where the only financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication. In general, most commenters supported this exception; however, a few commenters disagreed with the exception and felt that refill reminders should be treated as treatment communications requiring a statement in the notice and an opportunity to opt out if the communication is subsidized. Many commenters expressed the need for guidance on the scope of this exception and stated that certain communications should fall into the exception, such as communications about generic alternatives and drug adherence, and communications related to every component of a drug or biologic delivery system (especially where patients must self-administer medication). Some commenters specifically asked that the final rule exclude certain types of communications from this exception.

With respect to the proposed cost limitation on the refill reminder exception, while some commenters suggested that the cost be limited to either the actual cost or the fair market value of providing the communication, generally, most commenters supported the position that reasonably related costs should not be limited to actual costs. Many of the commenters in support of a broad interpretation of costs ''reasonably related'' to providing the communication suggested specific costs that should be permitted under this exception, such as costs of personnel, data storage, data processing, data analysis, data security, software, hardware, employee training, message content development, clinical review, postage, materials, drug adherence program development, formulary development, and the creation and implementation of analytics to measure the effectiveness of the communication. Several commenters noted that it would be unrealistic to expect a covered entity to perform such non-essential functions as sending refill reminders and other related communications if they could not recoup both their direct and indirect costs as well as a modest profit.

Final Rule

The final rule significantly modifies the proposed rule's approach to marketing by requiring authorization for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed. Many of the comments we received in response to the proposed marketing provisions concerned the distinction between communications for treatment and those for health care operations purposes and sought clarification on the line between such communications. We acknowledge that the distinction between what constitutes a treatment versus a health care operations communication may be difficult to make with precision in all cases, placing covered entities at risk for violating the authorization requirement for marketing communications. We, therefore, believe that requiring authorizations for all subsidized communications that market a health related product or service is the best policy. Such a policy will ensure that all such communications are treated as marketing communications, instead of requiring covered entities to have two processes in place based on whether the communication provided to individuals is for a treatment or a health care operations purpose. We decline to retain the Privacy Rule's definition of what constitutes ''marketing'' unchanged, as suggested by some commenters, as doing so would be inconsistent with the provisions of the Section 13406(a) of the HITECH Act.

Because the final rule treats subsidized treatment communications as marketing communications that require authorization, we have not adopted the notice requirement at proposed § 164.520(b)(1)(iii)(A) that a covered entity's notice of privacy practices include a statement informing individuals that the provider may send treatment communications to the individual concerning treatment alternatives or other health-related products or services where the provider receives financial remuneration from a third party in exchange for making the communication, and the individual has a right to opt out of receiving such communications. We also do not retain the notice requirement that existed at § 164.520(b)(1)(iii) prior to this final rule that a covered entity include in its notice of privacy practices a statement that the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual. Where the sending of such communications involves financial remuneration, the individual will be notified of such communications through the authorization process. Other communications for such purposes that do not involve financial remuneration are adequately captured in a covered entity's description in its notice of privacy practices of treatment and health care operations. However, covered entities that wish to continue to include such a specific statement in their notices of privacy practices may do so. For further discussion about the Notice of Privacy Practices, please see the discussion addressing the provisions at § 164.520 below.

We adopt the term ''financial remuneration'' and its definition as proposed without modification in the final rule. Most commenters were generally satisfied with the proposed use of the term and its definition. There was, however, some confusion among commenters as to what constitutes direct or indirect payment from or on behalf of a third party. We clarify that under this provision direct payment means financial remuneration that flows from the third party whose product or service is being described directly to the covered entity. In contrast, indirect payment means financial remuneration that flows from an entity on behalf of the third party whose product or service is being described to a covered entity.

We also clarify that where a business associate (including a subcontractor), as opposed to the covered entity itself, receives financial remuneration from a third party in exchange for making a communication about a product or service, such communication also requires prior authorization from the individual. The HITECH Act at Section 13406(a)(2)(C) provides that a business

associate may make such communications on behalf of a covered entity if consistent with the written contract required by the Privacy Rule between the business associate and covered entity. The Privacy Rule a § 164.504(e)(2)(i) provides that the contract may not authorize the business associate to further use or disclose the protected health information in a manner that would violate the Rule if done by the covered entity (except in two limited circumstances not relevant here). Thus, individual authorization also must be obtained if a business associate is to send these communications instead of the covered entity.

We also confirm, in response to comments, that the term ''financial remuneration'' does not include non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for making a communication about a product or service. Rather, financial remuneration includes only payments made in exchange for making such communications. In addition, we continue to emphasize that the financial remuneration a covered entity receives from a third party must be for the purpose of making a communication and such communication must encourage individuals to purchase or use the third party's product or service. If the financial remuneration received by the covered entity is for any purpose other than for making the communication, then this marketing provision does not apply. For example, if a third party provides financial remuneration to a covered entity to implement a program, such as a disease management program, the covered entity could provide individuals with communications about the program without obtaining individual authorization as long as the communications are about the covered entity's program itself. There, the communications would only be encouraging individuals to participate in the covered entity's disease management program and would not be encouraging individuals to use or purchase the third party's product or service.

Under the final rule, for marketing communications that involve financial remuneration, the covered entity must obtain a valid authorization from the individual before using or disclosing protected health information for such purposes, and such authorization must disclose the fact that the covered entity is receiving financial remuneration from a third party. See § 164.508(a)(3). The scope of the authorization need not be limited only to subsidized communications related to a single product or service or the products or services of one third party, but rather may apply more broadly to subsidized communications generally so long as the authorization adequately describes the intended purposes of the requested uses and disclosures (i.e., the scope of the authorization) and otherwise contains the elements and statements of a valid authorization under § 164.508. This includes making clear in the authorization that the individual may revoke the authorization at any time he or she wishes to stop receiving the marketing material.

Because the final rule will treat all subsidized treatment communications as marketing communications for which an authorization is required, the final rule also removes the language at proposed § 164.514(f)(2), which proposed to require that such communications be accompanied by a statement in the notice and an opportunity for the individual to opt out of receiving such communications. We believe that the removal of the notice and opt out requirements for such communications and the addition of the requirement to obtain an authorization will provide covered entities with a more uniform system for treating all remunerated communications. Because the individual must now sign an authorization before the covered entity can make subsidized treatment communications, there is no longer any need to require each such communication to contain a clear and conspicuous opportunity for the individual to elect not to receive any more of these communications. Where the individual signs an authorization to receive such communications, the covered entity may use and disclose the individual's protected health information for the purposes of making such communications unless or until the individual revokes the authorization pursuant to § 164.508(a)(5). If the individual does not authorize the covered entity to use and disclose the individual's protected health information for the purposes of making subsidized treatment communications, then the covered entity is prohibited from doing so.

We clarify that the final rule does nothing to modify the exceptions to the authorization requirement for marketing communications at § 164.508(a)(3)(i)(A) and (B). Therefore, no authorization is required where a covered entity receives financial remuneration from a third party to make a treatment or health care operations communication (or other marketing communication), if the communication is made face-to-face by a covered entity to an individual or consists of a promotional gift of nominal value provided by the covered entity. For example, a health care provider could, in a face to face conversation with the individual, recommend, verbally or by handing the individual written materials such as a pamphlet, that the individual take a specific alternative medication, even if the provider is otherwise paid by a third party to make such communications. However, communications made over the phone (as well as all communications sent through the mail or via email) do not constitute face to face communications, and as such, these communications require individual authorization where the covered entity receives remuneration in exchange for making the communications.

With respect to the exception for refill reminders or to otherwise communicate about a drug or biologic currently being prescribed to the individual, we adopt the exception as proposed. We continue to provide a stand-alone exception for refill reminders, given that the HITECH Act expressly does so. We therefore decline to adopt the suggestions of commenters to consider these communications to specifically be treatment communications (which would have required, under the provisions of the proposed rule, notice and an opportunity to opt out where the covered entity receives financial remuneration), or health care operations communications (which require authorization if financial remuneration is received).

Many commenters asked for guidance and clarification regarding the scope of this exception, and we received a wide array of examples of communications that commenters suggested should fall within this exception. At this time, we clarify that we consider communications about the generic equivalent of a drug being prescribed to an individual as well as adherence communications encouraging individuals to take their prescribed medication as directed fall within the scope of this exception. Additionally, we clarify that where an individual is prescribed a self-administered drug or biologic, communications regarding all aspects of a drug delivery system, including, for example, an insulin pump, fall under this exception. With respect to the array of other examples and suggestions provided by commenters as to what should fall within or outside of the exception, we intend to provide future guidance to address these questions.

The proposed rule contained the Act's limitation that the financial

remuneration received in exchange for providing a refill reminder or to otherwise communicate about a drug or biologic currently being prescribed to the individual must be ''reasonable in amount,'' by providing that such remuneration must be reasonably related to the covered entity's cost of making the communication for the exception from marketing to apply. We adopt this provision in the final rule. In response to comments regarding what types of costs fall within permissible remuneration, we clarify that we consider permissible costs for which a covered entity may receive remuneration under this exception are those which cover only the costs of labor, supplies, and postage to make the communication. Where the financial remuneration a covered entity receives in exchange for making the communication generates a profit or includes payment for other costs, such financial remuneration would run afoul of the Act's ''reasonable in amount'' language. Thus, under this final rule, if a pharmacy receives financial remuneration from a drug manufacturer to provide refill reminders to individuals taking a particular drug that covers only the pharmacy's cost of drafting, printing, and mailing the refill reminders, the exception would apply and no authorization would be required. However, where the drug manufacturer also provides the pharmacy with a financial incentive beyond the cost of making the communication to encourage the pharmacy's continued willingness to send such communications on behalf of the drug manufacturer, the exception would not apply and the pharmacy must obtain individual authorization. We note, however, that if a pharmacy provides refill reminders to individuals only when they visit the pharmacy (in face to face encounters), such communications would be permitted under § 164.508(a)(3)(i)(A) and thus, authorization would not be required even if the pharmacy receives financial remuneration above and beyond what is reasonably related to the pharmacy's cost of making the communication.

Finally, in addition to the communications that fall within the refill reminder exception, two other types of communications continue to be exempt from the marketing provisions. First, as explained in the NPRM, communications promoting health in general and that do not promote a product or service from a particular provider, such as communications promoting a healthy diet or encouraging individuals to get certain routine diagnostic tests, such as annual mammograms, do not constitute marketing and thus, do not require individual authorization.

Second, communications about government and government-sponsored programs do not fall within the definition of ''marketing'' as there is no commercial component to communications about benefits through public programs. Therefore, a covered entity may use and disclose protected health information to communicate with individuals about eligibility for programs, such as Medicare, Medicaid, or the State Children's Health Insurance Program (CHIP) without obtaining individual authorization.

Response to Other Public Comments

Comment: One commenter asked whether it is marketing where an entity promotes its discounts on covered benefits or member-exclusive value-added health products and services by paying a mailing house that is the health plan's business associate to send its written promotional material to health plan members. The commenter stated that only the mailing house, and not the covered entity, is paid to send the communications.

Response: Even where a business associate of a covered entity, such as a mailing house, rather than the covered entity itself, receives the financial remuneration from the entity whose product or service is being promoted to health plan members, the communication is a marketing communication for which prior authorization is required. As stated above, under the Privacy Rule, a business associate generally may not use or disclose protected health information in a manner that would be impermissible if done by the covered entity. We note, however, that non-financial or in-kind remuneration may be received by the covered entity or its business associate and it would not implicate the new marketing restrictions. Thus, if the materials describing a member-exclusive value-added health product or service were provided by the entity to the health plan or its business associate and no payment was made by the entity relating to the mailing or distribution of the materials, the covered entity or its business associate would be able to provide the material to its members without requiring an authorization.

3. Business Associates

a. Section 164.502(a) and (b)—Permitted and Required Uses and Disclosures and Minimum Necessary

Before the HITECH Act, the Privacy Rule did not govern business associates directly. However, section 13404 of the HITECH Act makes specific requirements of the Privacy Rule applicable to business associates, and creates direct liability for noncompliance by business associates with regard to those Privacy Rule requirements. Specifically, section 13404(a) of the HITECH Act creates direct liability for uses and disclosures of protected health information by business associates that do not comply with its business associate contract or other arrangement under the Privacy Rule. Additionally, section 13404(a) applies the other privacy requirements of the HITECH Act directly to business associates just as they apply to covered entities. Section 13404(b) applies the provision of § 164.504(e)(1)(ii) regarding knowledge of a pattern of activity or practice that constitutes a material breach or violation of a contract to business associates. Finally, section 13404(c) applies the HIPAA civil and criminal penalties to business associates. We discuss the modifications to the Privacy Rule pursuant to paragraphs (a) and (b) of section 13404 of the HITECH Act below. We address the modifications made to the Enforcement Rule by section 13404(c) regarding the application of penalties to violations by business associates above in the discussion of the changes to the Enforcement Rule.

We note that we have not added references to ''business associate'' to all provisions of the Privacy Rule that address uses and disclosures by covered entities. Such additions to the Privacy Rule are unnecessary, as a business associate generally may only use or disclose protected health information in the same manner as a covered entity. Therefore, any Privacy Rule limitation on how a covered entity may use or disclose protected health information automatically extends to a business associate.

i. Permitted and Required Uses and Disclosures

Proposed Rule

We proposed to modify § 164.502(a) of the Privacy Rule containing the general rules for uses and disclosures of protected health information to address the permitted and required uses and disclosures of protected health information by business associates. First, we proposed to modify

§ 164.502(a) to provide that a business associate, like a covered entity, may not use or disclose protected health information except as permitted or required by the Privacy Rule or the Enforcement Rule. Second, we proposed to add new provisions at § 164.502(a)(4) and (5) to specify the permitted and required uses and disclosures of protected health information by business associates.

In accordance with section 13404(a) of the HITECH Act, we proposed in § 164.502(a)(4) to allow business associates to use or disclose protected health information only as permitted or required by their business associate contracts or other arrangements pursuant to § 164.504(e) or as required by law. Any other use or disclosure would violate the Privacy Rule. Proposed § 164.502(a)(4) also provided that a business associate would not be permitted to use or disclose protected health information in a manner that would violate the Privacy Rule if done by the covered entity, except that the business associate would be permitted to use or disclose protected health information for the proper management and administration of the business associate and to provide data aggregation services for the covered entity, as specified at § 164.504(e)(2)(i)(A) and (B), if such uses and disclosures are permitted by its business associate contract or other arrangement.

In § 164.502(a)(5), we proposed to require that a business associate disclose protected health information either: (1) When required by the Secretary under Subpart C of Part 160 to investigate or determine the business associate's compliance with this subchapter; or (2) to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii), as modified, with respect to an individual's request for an electronic copy of protected health information. Section 13405(e) of the HITECH Act requires covered entities that maintain protected health information in an electronic health record to provide an individual, or the individual's designee, with a copy of such information in an electronic format, if the individual so chooses. We proposed to include a similar direct requirement on business associates in § 164.502(a)(5), as section 13404(a) of the HITECH Act also applies section 13405(e) to business associates.

We also proposed a conforming change to revise the titles of § 164.502(a)(1) and (a)(2) to make clear that these provisions setting out permitted uses and disclosures of protected health information apply only to covered entities, as well as a technical change to § 164.502(a)(2)(ii) to replace the term ''subpart'' with ''subchapter'' to make clear that a covered entity is required to disclose protected health information to the Secretary as needed to determine compliance with any of the HIPAA Rules and not just the Privacy Rule.

Overview of Public Comments

Several commenters expressed concern about the increased liability for business associates under the rule and requested clarification on when business associate liability for impermissible uses and disclosures would attach. Several commenters asked for clarification as to what a business associate is directly liable for under the Privacy Rule, and some expressed specific confusion regarding the liability of business associates for the provision of e-access under the rule.

Final Rule

The final rule adopts the proposed modifications to § 164.502(a). The provisions specifying a business associate's permitted and required uses and disclosures of protected health information are renumbered from § 164.502(a)(4) and (a)(5), as proposed, to § 164.502(a)(3) and (a)(4), as § 164.502(a)(5) of the final rule now includes provisions to address prohibited uses and disclosures. Section 164.502(a)(5) is discussed below in the sections describing the prohibitions on the sale of protected health information and the use or disclosure of genetic information for underwriting purposes.

In response to specific comments asking for clarification regarding when business associate liability would attach, we provide the following. As we discussed above, the final rule provides that a business associate is a person who performs functions or activities on behalf of, or certain services for, a covered entity or another business associate that involve the use or disclosure of protected health information. The final rule establishes that a person becomes a business associate by definition, not by the act of contracting with a covered entity or otherwise. Therefore, liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate.

Liability also does not depend on the type of protected health information that a business associate creates, receives, maintains, or transmits on behalf of a covered entity or another business associate, or on the type of entity performing the function or service, except to the extent the entity falls within one of the exceptions at paragraph 4 of the definition of business associate. First, protected health information created, received, maintained, or transmitted by a business associate may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected by the business associate in accordance with the HIPAA Rules and its business associate agreement. Second, the definition of business associate is contingent on the fact that the business associate performs certain activities or functions on behalf of, or provides certain services to, a covered entity or another business associate that involve the use or disclosure of protected health information. Therefore, any person, defined in the HIPAA Rules as a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private, who performs these functions or activities or services is a business associate for purposes of the HIPAA Rules, regardless of whether such person has other professional or privilege-based duties or responsibilities.

Finally, while we understand commenters' concerns about the increased liability for business associates under the HIPAA Rules, such direct liability for violations of certain HIPAA provisions is expressly provided for by the HITECH Act.

In response to comments requesting clarification on with which HIPAA provisions a business associate is directly liable for compliance, we provide the following. Business associates are directly liable under the HIPAA Rules for impermissible uses and disclosures,[4] for a failure to provide breach notification to the covered entity,[5] for a failure to provide access to a copy of electronic protected health information to either the covered entity, the individual, or the individual's designee (whichever is specified in the

[4] See § 164.502(a)(3).

[5] See § 164.410.

business associate agreement),[6] for a failure to disclose protected health information where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules,[7] for a failure to provide an accounting of disclosures,[8] and for a failure to comply with the requirements of the Security Rule.[9] Business associates remain contractually liable for other requirements of the business associate agreement (see below for a discussion of the business associate agreement provisions).

With respect to a business associate's direct liability for a failure to provide access to a copy of electronic protected health information, business associates are liable for providing electronic access in accordance with their business associate agreements. Therefore, business associates may provide electronic access directly to individuals or their designees, or may provide the electronic protected health information to the covered entity (which then provides the electronic access to individuals or their designees). As with many other provisions in the HIPAA Rules, the Department leaves the details to the contracting parties, and is concerned only that access is provided to the individual, not with which party provides the access.

ii. Minimum Necessary

Proposed Rule

We proposed to modify the minimum necessary standard at § 164.502(b) to require that when business associates use, disclose, or request protected health information from another covered entity, they limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Applying the minimum necessary standard is a condition of the permissibility of many uses and disclosures of protected health information. Thus, a business associate is not making a permitted use or disclosure under the Privacy Rule if it does not apply the minimum necessary standard, where appropriate. Additionally, the HITECH Act at section 13405(b) addresses the application of minimum necessary and, in accordance with 13404(a), also applies such requirements to business associates.

Overview of Public Comments

While the Department received general support for application of the minimum necessary standard to requests and uses and disclosures by business associates, several commenters requested clarification on such application.

Final Rule

The final rule adopts the proposal to apply the minimum necessary standard directly to business associates when using or disclosing protected health information or when requesting protected health information from another covered entity. The final rule also makes clear that requests directed to another business associate, in addition to those directed to another covered entity, must also be limited to the minimum necessary. Covered entities and business associates disclosing protected health information in response may reasonably rely on such requests as requesting the minimum necessary for the disclosure.

How a business associate will apply the minimum necessary standard will vary based on the circumstances. As is the case today, a business associate agreement must limit the business associate's uses and disclosures of protected health information to be consistent with the covered entity's minimum necessary policies and procedures. We leave it to the discretion of the parties to determine to what extent the business associate agreement will include specific minimum necessary provisions to ensure a business associate's uses and disclosures and requests for protected health information are consistent with the covered entity's minimum necessary policies and procedures. The Department intends to issue future guidance on the minimum necessary standard in accordance with section 13405(b) of the HITECH Act that will consider the specific questions posed by commenters with respect to business associates' application of the minimum necessary standard.

b. Sections 164.502(e) and 164.504(e)—Business Associate Agreements

Proposed Rule

Section 164.502(e) permits a covered entity to disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains satisfactory assurances, in the form of a written contract or other written arrangement with the business associate that meets the requirements of § 164.504(e), that the business associate will appropriately safeguard the information. We proposed a parallel provision in § 164.502(e) that would allow a business associate to disclose protected health information to a business associate that is a subcontractor, and to allow the subcontractor to create or receive protected health information on its behalf, if the business associate obtains similar satisfactory assurances that the subcontractor will appropriately safeguard the information. Consistent with the proposal with respect to Security Rule requirements and business associates, we proposed to make clear in § 164.502(e) that a covered entity would not be required to obtain satisfactory assurances from business associates that are subcontractors. Rather, a business associate would be required to obtain such assurances from a subcontractor. Thus, the proposed provisions would not change the parties to the contracts. For example, a covered entity may choose to contract with a business associate (contractor) to use or disclose protected health information on its behalf, the business associate may choose to obtain the services of (and exchange protected health information with) a subcontractor (subcontractor 1), and that subcontractor may, in turn, contract with another subcontractor (subcontractor 2) for services involving protected health information. The contractor and subcontractors 1 and 2 would now be business associates with direct liability under the HIPAA Rules, and would be required to obtain business associate agreements with the parties with whom they contract for services that involve access to protected health information. (Note, however, as discussed above with respect to the definition of ''business associate,'' direct liability under the HIPAA Rules would attach regardless of whether the contractor and subcontractors have entered into the required business associate agreements.)

We also proposed to remove § 164.502(e)(1)(iii), which provides that a covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the Privacy Rule's business associate agreement provisions, given that proposed changes to § 164.502 would now restrict directly the uses and disclosures of protected health information by a business associate, including a covered entity acting as a business associate, to those uses and disclosures permitted by its business associate agreement.

[6] See § 164.502(a)(4)(ii).

[7] See § 164.502(a)(4)(i).

[8] *See* 76 FR 31426 (May 31, 2011).

[9] See Subpart C of Part 164.

Finally, as discussed above with respect to the definition of business associate, we proposed to move the current exceptions to business associate to the definition itself in § 160.103.

Section 164.504(e) contains the specific requirements for business associate contracts and other arrangements. We proposed a number of modifications to § 164.504(e) to implement section 13404 of the HITECH Act and to reflect the Department's new regulatory authority with respect to business associates, as well as to reflect a covered entity's and business associate's new obligations under Subpart D of Part 164 of the Privacy Rule to provide for notification in the case of breaches of unsecured protected health information.

Section 164.504(e)(1)(ii) provides that a covered entity is not in compliance with the business associate requirements if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful, terminated the contract or arrangement or, if termination is not feasible, reported the problem to the Secretary. We proposed to remove the requirement that covered entities report to the Secretary when termination of a business associate agreement is not feasible. In light of a business associate's direct liability for civil money penalties for certain violations of the business associate agreement and both a covered entity's and business associate's obligations under Subpart D to report breaches of unsecured protected health information to the Secretary, we have other mechanisms through which we expect to learn of such breaches and misuses of protected health information by a business associate.

We also proposed to add a new provision at § 164.504(e)(1)(iii) applicable to business associates with respect to subcontractors to mirror the requirements on covered entities at § 164.504(e)(1)(ii) (minus the requirement to report to the Secretary if termination of a contract is not feasible). Thus, a business associate that is aware of noncompliance by its business associate subcontractor would be required to respond to the situation in the same manner as a covered entity that is aware of noncompliance by its business associate. We believe this provision would implement section 13404(b) of the HITECH Act, and would align the requirements for business associates with regard to business associate subcontractors with the requirements for covered entities with regard to their business associates.

We also proposed changes to the specific business associate agreement provisions at § 164.504(e). First, we proposed to revise § 164.504(e)(2)(ii)(B) through (D) to provide that the contract will require that: in (B), business associates comply, where applicable, with the Security Rule with regard to electronic protected health information; in (C), business associates report breaches of unsecured protected health information to covered entities, as required by § 164.410; and in (D), in accordance with § 164.502(e)(1)(ii), business associates ensure that any subcontractors that create or receive protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information. These revisions were proposed to align the requirements for the business associate agreement with the requirements in the HITECH Act and elsewhere within the HIPAA Rules.

Additionally, we proposed to add a new agreement provision at § 164.504(e)(2)(ii)(H) (and to renumber the current paragraphs (H) and (I) accordingly) to requires that, to the extent the business associate is to carry out a covered entity's obligation under this subpart, the business associate must comply with the requirements of the Privacy Rule that apply to the covered entity in the performance of such obligation. This provision would clarify that when a covered entity delegates a responsibility under the Privacy Rule to the business associate, the business associate would be contractually required to comply with the requirements of the Privacy Rule in the same manner as they apply to the covered entity. For example, if a third party administrator, as a business associate of a group health plan, fails to distribute the plan's notice of privacy practices to participants on a timely basis, the third party administrator would not be directly liable under the HIPAA Rules, but would be contractually liable, for the failure. However, even though the business associate is not directly liable under the HIPAA Rules for failure to provide the notice, the covered entity remains directly liable for failure to provide the individuals with its notice of privacy practices because it is the covered entity's ultimate responsibility to do so, despite its having hired a business associate to perform the function.

We also proposed to add a new § 164.504(e)(5) that would apply the requirements at § 164.504(e)(2) through (e)(4) to the contract or other arrangement between a business associate and its business associate subcontractor as required by § 164.502(e)(1)(ii) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and its business associate. Thus, a business associate would be required by § 164.502(e)(1)(ii) and by this section to enter into business associate agreements or other arrangements that comply with the Privacy and Security Rules with their business associate subcontractors, in the same manner that covered entities are required to enter into contracts or other arrangements with their business associates.

Finally, we proposed a few other minor changes. We proposed in § 164.504(e)(3) regarding other arrangements for governmental entities to include references to the Security Rule requirements for business associates to avoid having to repeat such provisions in the Security Rule. We also proposed to remove the reference to subcontractors in § 164.504(f)(2)(ii)(B) (regarding disclosures to plan sponsors) and in § 164.514(e)(4)(ii)(C)(4) (regarding data use agreements for limited data sets) to avoid confusion since the term ''subcontractor'' is now a defined term under the HIPAA Rules with a particular meaning that is related to business associates. The proposed removal of the term was not intended as a substantive change to the provisions.

Overview of Public Comments

Several commenters expressed confusion regarding the need for business associate agreements, considering the provisions for direct liability from the HITECH Act and in the proposed rule. Many of these commenters suggested that all of the requirements of the Privacy Rule apply to business associates, as is the case with the Security Rule.

A few commenters requested clarification about what constitutes ''satisfactory assurances'' pursuant to the rule, asking whether, for example, there were expectations on covered entities to ensure that business associates (including subcontractors) have appropriate controls in place besides business associate agreements or whether a covered entity must obtain from a business associate satisfactory assurance that any business associate subcontractors are complying with the Rules. Several commenters requested clarification on the appropriateness of

indemnification clauses in business associate agreements.

Finally, several commenters requested that the Department provide a model business associate agreement.

Final Rule

The final rule adopts the proposed modifications to §§ 164.502(e) and 164.504(e). As we discussed above, while section 13404 of the HITECH Act provides that business associates are now directly liable for civil money penalties under the HIPAA Privacy Rule for impermissible uses and disclosures and for the additional HITECH requirements in Subtitle D that are made applicable to covered entities, it does not apply all of the requirements of the Privacy Rule to business associates and thus, the final rule does not. Therefore, business associates are not required to comply with other provisions of the Privacy Rule, such as providing a notice of privacy practices or designating a privacy official, unless the covered entity has chosen to delegate such a responsibility to the business associate, which would then make it a contractual requirement for which contractual liability would attach.

Concerning commenters' questions about the continued need for business associate agreements given the new direct liability on business associates for compliance, we note that section 13404 of the HITECH Act expressly refers and ties business associate liability to making uses and disclosures in accordance with the uses and disclosures laid out in such agreements, rather than liability for compliance with the Privacy Rule generally. Further, section 13408 of the HITECH Act requires certain data transmission and personal health record vendors to have in place business associate agreements with the covered entities they serve. We also continue to believe that, despite the business associate's direct liability for certain provisions of the HIPAA Rules, the business associate agreement is necessary to clarify and limit, as appropriate, the permissible uses and disclosures by the business associate, given the relationship between the parties and the activities or services being performed by the business associate. The business associate agreement is also necessary to ensure that the business associate is contractually required to perform certain activities for which direct liability does not attach (such as amending protected health information in accordance with § 164.526). In addition, the agreement represents an opportunity for the parties to clarify their respective responsibilities under the HIPAA Rules, such as by establishing how the business associate should handle a request for access to protected health information that it directly receives from an individual. Finally, the business associate agreement serves to notify the business associate of its status under the HIPAA Rules, so that it is fully aware of its obligations and potential liabilities.

With respect to questions about ''satisfactory assurances,'' § 164.502(e) provides that covered entities and business associates must obtain and document the ''satisfactory assurances'' of a business associate through a written contract or other agreement, such as a memorandum of understanding, with the business associate that meets the applicable requirements of § 164.504(e). As discussed above, § 164.504(e) specifies the provisions required in the written agreement between covered entities and business associates, including a requirement that a business associate ensure that any subcontractors agree to the same restrictions and conditions that apply to the business associate by providing similar satisfactory assurances. Beyond the required elements at § 164.504(e), as with any contracting relationship, business associates and covered entities may include other provisions or requirements that dictate and describe their business relationship, and that are outside the governance of the Privacy and Security Rules. These may or may not include additional assurances of compliance or indemnification clauses or other risk-shifting provisions.

We also clarify with respect to the satisfactory assurances to be provided by subcontractors, that the agreement between a business associate and a business associate that is a subcontractor may not permit the subcontractor to use or disclose protected health information in a manner that would not be permissible if done by the business associate. For example, if a business associate agreement between a covered entity and a contractor does not permit the contractor to de-identify protected health information, then the business associate agreement between the contractor and a subcontractor (and the agreement between the subcontractor and another subcontractor) cannot permit the de-identification of protected health information. Such a use may be permissible if done by the covered entity, but is not permitted by the contractor or any subcontractors if it is not permitted by the covered entity's business associate agreement with the contractor. In short, each agreement in the business associate chain must be as stringent or more stringent as the agreement above with respect to the permissible uses and disclosures.

Finally, in response to the comments requesting a model business associate agreement, we note that the Department has published sample business associate provisions on its web site. The sample language is designed to help covered entities comply with the business associate agreement requirements of the Privacy and Security Rules. However, use of these sample provisions is not required for compliance with the Rules, and the language should be amended as appropriate to reflect actual business arrangements between the covered entity and the business associate (or a business associate and a subcontractor).

Response to Other Public Comments

Comment: Commenters requested guidance on whether a contract that complies with the requirements of the Graham Leach Bliley Act (GLBA) and incorporates the required elements of the HIPAA Rules may satisfy both sets of regulatory requirements. The commenters urged the Department to permit a single agreement rather than requiring business associates and business associate subcontractors to enter into separate GLBA agreements and business associate agreements.

Response: While meeting the requirements of the GLBA does not satisfy the requirements of the HIPAA Rules, covered entities may use one agreement to satisfy the requirements of both the GLBA and the HIPAA Rules.

Comment: A few commenters recommended adding an exception to having a business associate agreement for a person that receives a limited dataset and executes a data use agreement for research, health care operations, or public health purposes.

Response: We have prior guidance that clarifies that if only a limited dataset is released to a business associate for a health care operations purpose, then a data use agreement suffices and a business associate agreement is not necessary. To make this clear in the regulation itself, we are adding to § 164.504(e)(3) a new paragraph (iv) that recognizes that a data use agreement may qualify as a business associate's satisfactory assurance that it will appropriately safeguard the covered entity's protected health information when the protected health information disclosed for a health care operations purpose is a limited data set. A similar provision is not necessary or appropriate for disclosures of limited data sets for research or public health purposes since such disclosures would

not otherwise require business associate agreements.

Comment: A few commenters requested that the Department delete § 164.504(e)(2)(ii)(H), which provides that to the extent the business associate is to carry out a covered entity's obligation under the HIPAA Rules, the business associate must comply with the requirements of the HIPAA Rules that apply to the covered entity in the performance of the obligation on behalf of the covered entity. Alternatively, commenters suggested that the Department clarify that the requirements of the section need not be included in business associate agreements and that this section does not limit the ability of covered entities and business associates to negotiate responsibilities with regard to other sections of the Privacy Rule.

Response: The Department declines to delete § 164.504(e)(2)(ii)(H). If a business associate contracts to provide services to the covered entity with regard to fulfilling individual rights or other obligations of the covered entity under the Privacy Rule, then the business associate agreement must require the business associate to fulfill such obligation in accordance with the Privacy Rule's requirements. We do clarify, however, that if the covered entity does not delegate any of its responsibilities under the Privacy Rule to the business associate, then § 164.504(e)(2)(ii)(H) is not applicable and the parties are not required to include such language.

Comment: One commenter requested that the Department modify § 164.502(a)(4)(i) to permit business associates to use and disclose protected health information for their own health care operations purposes, and another commenter requested that the Department clarify whether § 164.504(e)(4) provides that a business associate may use or disclose protected health information as a covered entity would use or disclose the information.

Response: The Department declines to make the suggested modification. Business associates do not have their own health care operations (see the definition of health care operations at § 164.501, which is limited to activities of the covered entity). While a business associate does not have health care operations, it is permitted by § 164.504(e)(2)(i)(A) to use and disclose protected health information as necessary for its own management and administration if the business associate agreement permits such activities, or to carry out its legal responsibilities. Other than the exceptions for the business associate's management and administration and for data aggregation services relating to the health care operations of the covered entity, the business associate may not use or disclose protected health information in a manner that would not be permissible if done by the covered entity (even if such a use or disclosure is permitted by the business associate agreement).

Comment: One commenter suggested requiring subcontractors to return or destroy all protected health information received from or created for a business associate when the contract with the business associate is terminated.

Response: The final rule at § 164.504(e)(5) does apply the requirements at § 164.504(e)(2) through (4) (which set forth the requirements for agreements between covered entities and their business associates) to agreements between business associates and their subcontractors. This includes § 164.504(e)(2)(ii)(J), which requires the business associate to return or destroy all protected health information received from, or created or received on behalf of, the covered entity at the termination of the contract, if feasible. When this requirement is applied to the agreement between the business associate and its business associate subcontractor, the effect is a contractual obligation for the business associate subcontractor to similarly return or destroy protected health information at the termination of the contract, if feasible.

Comment: One commenter suggested requiring a business associate to disclose all subcontractors of the business associate to a covered entity within thirty days of the covered entity's request.

Response: The Department declines to adopt this suggestion as a requirement of the HIPAA Rules, because such a requirement would impose an undue disclosure burden on business associates. However, covered entities and business associates may include additional terms and conditions in their contracts beyond those required by § 164.504.

Comment: One commenter suggested establishing a certification process of business associates and subcontractors with regard to HIPAA compliance.

Response: The Department declines to establish or endorse a certification process for HIPAA compliance for business associates and subcontractors. Business associates and subcontractors are free to enlist the services of outside entities to assess their compliance with the HIPAA Rules and certification may be a useful compliance tool for entities, depending on the rigor of the program. However, certification does not guarantee compliance and therefore ''certified'' entities may still be subject to enforcement by OCR.

Comment: One commenter requested clarification on when it is not feasible for a business associate to terminate a contract with a subcontractor.

Response: Whether it is feasible for a business associate to terminate an agreement with a business associate subcontractor is a very fact-specific inquiry that must be examined on a case-by-case basis. For example, termination is not feasible for a business associate with regard to a subcontractor relationship where there are no other viable business alternatives for the business associate (when the subcontractor, for example, provides a unique service that is necessary for the business associate's operations). See our prior guidance on this issue as it applies to covered entities and business associates in Frequently Asked Question #236, available at *http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/236.html.*

c. Section 164.532—Transition Provisions

Proposed Rule

We understand that covered entities and business associates are concerned with the anticipated administrative burden and cost to implement the revised business associate agreement provisions of the Privacy and Security Rules. Covered entities may have existing contracts that are not set to terminate or expire until after the compliance date of the modifications to the Rules, and we understand that a six month compliance period may not provide enough time to reopen and renegotiate all contracts. In response to these concerns, we proposed to relieve some of the burden on covered entities and business associates in complying with the revised business associate provisions by adding a transition provision to grandfather certain existing contracts for a specified period of time. The Department's authority to add the transition provision is set forth in § 160.104(c), which allows the Secretary to establish the compliance date for any modified standard or implementation specification, taking into account the extent of the modification and the time needed to comply with the modification. The proposed transition period would prevent rushed and hasty changes to thousands of on-going existing business associate agreements. We addressed the issue of the business associate transition provisions as follows.

We proposed new transition provisions at § 164.532(d) and (e) to allow covered entities and business associates (and business associates and business associate subcontractors) to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the Rules. The additional transition period would be available to a covered entity or business associate if, prior to the publication date of the modified Rules, the covered entity or business associate had an existing contract or other written arrangement with a business associate or subcontractor, respectively, that complied with the prior provisions of the HIPAA Rules and such contract or arrangement was not renewed or modified between the effective date and the compliance date of the modifications to the Rules. The proposed provisions were intended to allow those covered entities and business associates with valid contracts with business associates and subcontractors, respectively, to continue to disclose protected health information to the business associate or subcontractor, or to allow the business associate or subcontractor to continue to create or receive protected health information on behalf of the covered entity or business associate, for up to one year beyond the compliance date of the modifications, regardless of whether the contract meets the applicable contract requirements in the modifications to the Rules. With respect to business associates and subcontractors, the proposal would grandfather existing written agreements between business associates and subcontractors entered into pursuant to § 164.504(e)(2)(ii)(D) (which requires the business associate to ensure that its agents with access to protected health information agree to the same restrictions and conditions that apply to the business associate). The Department proposed to deem such contracts to be compliant with the modifications to the Rules until either the covered entity or business associate has renewed or modified the contract following the compliance date of the modifications, or until the date that is one year after the compliance date, whichever is sooner.

In cases where a contract renews automatically without any change in terms or other action by the parties (also known as ''evergreen contracts''), the Department intended that such evergreen contracts would be eligible for the extension and that deemed compliance would not terminate when these contracts automatically rolled over. These transition provisions would have applied to covered entities and business associates only with respect to written contracts or other written arrangements as specified above, and not to oral contracts or other arrangements.

These transition provisions would have only applied to the requirement to amend contracts; they would not affect any other compliance obligations under the HIPAA Rules. For example, beginning on the compliance date of this rule, a business associate may not use or disclose protected health information in a manner that is contrary to the Privacy Rule, even if the business associate's contract with the covered entity has not yet been amended.

Overview of Public Comments

Many commenters supported the 1-year extended timeframe for compliance with the business associate agreement provisions. Some commenters suggested longer timeframes, citing cost and resource limitations. Some commenters suggested that the Department should deem compliant all business associate agreements that have been renegotiated in good faith to meet the February 2010 effective date of the applicable provisions in the HITECH Act. Some commenters suggested that the Department recognize as compliant business associate agreements with provisions requiring compliance with all applicable laws.

Final Rule

The final rule adopts the proposal, adding new transition provisions at § 164.532(d) and (e) to allow covered entities and business associates (and business associates and business associate subcontractors) to continue to operate under certain existing contracts for up to one year beyond the compliance date of the revisions to the Rules.

We decline to provide a longer time for compliance with the business associate agreement provisions. We provided a similar transition period for revising agreements in the 2002 modifications to the HIPAA Rules, and it was our experience that such time was sufficient to ease burden on the entities and allow most agreements to be modified at the time they would otherwise come up for renewal or renegotiation.

With respect to those business associate agreements that already have been renegotiated in good faith to meet the applicable provisions in the HITECH Act, covered entities should review such agreements to determine whether they meet the final rule's provisions. If they do not, these covered entities then have the transition period to make whatever additional changes are necessary to conform to the final rule. The transition period is also available to those agreements that require compliance with all applicable laws (to the extent the agreements were otherwise in compliance with the HIPAA Rules prior to this final rule), but that do not fully meet the new requirements in this final rule. However, we do not deem such contracts as compliant beyond the transition period because they would not sufficiently reflect the new requirements.

4. Section 164.508—Uses and Disclosures for Which an Authorization Is Required

a. Sale of Protected Health Information

Proposed Rule

Section 164.508 of the Privacy Rule permits a covered entity to use and disclose protected health information for purposes not otherwise permitted by the Rule if it has obtained a valid written authorization from the individual who is the subject of the information. This section also specifies two circumstances in which authorization from the individual must be obtained: (1) Most uses and disclosures of psychotherapy notes; and (2) uses and disclosures for marketing purposes.

Section 13405(d) of the HITECH Act added a third circumstance that requires authorization, specifically the sale of protected health information. Section 13405(d)(1) prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of protected health information unless the covered entity has obtained an individual's authorization pursuant to § 164.508 that states whether the protected health information can be further exchanged for remuneration by the entity receiving the information.

Section 13405(d)(2) contains several exceptions to the authorization requirement for circumstances where the purpose of the exchange is for: (1) Public health activities, as described at § 164.512(b) of the Privacy Rule; (2) research purposes as described at §§ 164.501 and 164.512(i) of the Rule, if the price charged for the information reflects the cost of preparation and transmittal of the data; (3) treatment of the individual; (4) the sale, transfer, merger or consolidation of all or part of a covered entity and for related due diligence; (5) services rendered by a business associate pursuant to a

business associate agreement and at the specific request of the covered entity; (6) providing an individual with access to his or her protected health information pursuant to § 164.524; and (7) other purposes as the Secretary deems necessary and appropriate by regulation. Section 13405(d)(4) of the Act provides that the prohibition on sale of protected health information applies to disclosures occurring six months after the date of the promulgation of the final regulations implementing this section.

To implement section 13405(d) of the HITECH Act, we proposed to add a general rule at § 164.508(a)(4) requiring a covered entity to obtain an authorization for any disclosure of protected health information in exchange for direct or indirect remuneration from or on behalf of the recipient of the information and to require that the authorization state that the disclosure will result in remuneration to the covered entity. Consistent with the HITECH Act, the NPRM proposed to exclude several disclosures of protected health information made in exchange for remuneration from this general rule. As provided in the Act, these requirements would also apply to business associates of covered entities.

In the NPRM we did not include language at § 164.508(a)(4) to require that the authorization under § 164.508 specify whether the protected health information disclosed by the covered entity for remuneration could be further exchanged for remuneration by the entity receiving the information. The statute refers to obtaining a valid authorization that includes a remuneration statement in accordance with § 164.508. The remuneration statement required by § 164.508 is whether remuneration will be received by the covered entity with respect to the disclosures subject to the authorization. This puts the individual on notice that the disclosure involves remuneration and thus, enables the individual to make an informed decision as to whether to sign the authorization. Thus, we interpreted the statute to mean that the authorization must include a statement that the covered entity is receiving direct or indirect remuneration in exchange for the protected health information. We note that these exact words do not need to be used in the statement. We provide discretion for covered entities to craft appropriate language that reflects, for example, the specific type of remuneration they receive. As we explained in the NPRM, with respect to the recipient of the information, if protected health information is disclosed for remuneration by a covered entity or business associate to another covered entity or business associate in compliance with the authorization requirements at proposed § 164.508(a)(4)(i), the recipient covered entity or business associate could not redisclose the protected health information in exchange for remuneration unless a valid authorization was obtained in accordance with proposed § 164.508(a)(4)(i). We requested comment on these provisions.

At proposed § 164.508(a)(4)(ii), we set forth the exceptions to the authorization requirement. We proposed the exceptions provided for by section 13405(d)(2) of the HITECH Act, and also proposed to exercise the authority granted to the Secretary in section 13405(d)(2)(G) to include additional exceptions that we deemed to be similarly necessary and appropriate. These exceptions are discussed below. We requested comment on whether there were additional exceptions that should be included in the final regulation.

First, we proposed to include an exception to cover exchanges for remuneration for public health activities pursuant to §§ 164.512(b) or 164.514(e). We added the reference to § 164.514(e) of the Privacy Rule to ensure that disclosures of protected health information for public health activities in limited data set form would also be excepted from the authorization requirement, in addition to disclosures that may occur under § 164.512(b) with more identifiable information. With respect to the exception for public health disclosures, section 13405(d)(3)(A) of the HITECH Act requires that the Secretary evaluate the impact on public health activities of restricting this exception to require that the price charged for the data reflects only the costs of preparation and transmittal of the data, including those conducted by or for the use of the Food and Drug Administration (FDA). Section 13405(d)(3)(B) further provides that if the Secretary finds that such further restriction will not impede public health activities, the restriction may then be included in the regulations. We did not propose to include such a restriction on remuneration in the Rule, but requested public comment to assist us in evaluating the impact of doing so.

The NPRM also included an exception for disclosures of protected health information for research purposes, pursuant to §§ 164.512(i) or 164.514(e), in exchange for which the covered entity receives only a reasonable, cost based fee to cover the cost to prepare and transmit the information for research purposes. Like the public health exception, we proposed to add a reference to § 164.514(e) to ensure that this exception would also apply to the disclosure of protected health information in limited data set form for research purposes. We requested public comment on the types of costs that should be permitted under this provision.

We proposed to create an exception from the authorization requirement for disclosures of protected health information for treatment and payment purposes. Though the Act only addressed treatment, we proposed to also except disclosures for payment for health care from the remuneration prohibition to make clear that the exchange of protected health information to obtain ''payment,'' as such term is defined in the Privacy Rule at § 164.501, would not be considered a sale of protected health information.

Consistent with section 13405(d)(2)(D) of the HITECH Act, we proposed to except from the authorization requirement disclosures described in paragraph (6)(iv) of the definition of health care operations at § 164.501, that is, disclosures for the sale, transfer, merger, or consolidation of all or part of a covered entity, or an entity that following such activity will become a covered entity, and due diligence related to such activity.

We proposed to provide an exception from the authorization requirement for disclosures of protected health information to or by a business associate for activities that the business associate undertakes on behalf of a covered entity pursuant to §§ 164.502(e) and 164.504(e) of the Privacy Rule, as long as the only remuneration provided is by the covered entity to the business associate for the performance of such activities. This exception would exempt from the authorization requirement at § 164.508(a)(4)(i) a disclosure of protected health information by a covered entity to a business associate or by a business associate to a third party on behalf of the covered entity as long as any remuneration received by the business associate was for the activities performed by the business associate pursuant to a business associate contract.

We proposed to except from the authorization requirement disclosures of protected health information by a covered entity to an individual when requested under §§ 164.524 (providing a right to access protected health information) or 164.528 (providing a right to receive an accounting of

disclosures). While section 13405(d)(2)(F) of the HITECH Act explicitly refers only to disclosures under § 164.524, we exercised our authority under section 13405(d)(2)(G) of the HITECH Act to likewise include in the exception disclosures to the individual under § 164.528. Section 164.524 permits a covered entity to impose a reasonable, cost-based fee for the provision of access to an individual's protected health information upon request. Section 164.528 requires a covered entity to provide a requesting individual with an accounting of disclosures without charge in any 12-month period but permits a covered entity to impose a reasonable, cost-based fee for each subsequent request for an accounting of disclosures during that 12-month period. Therefore, a disclosure of protected health information under § 164.528 is similar to a disclosure under § 164.524 in that a covered entity may be paid a fee for making the disclosure.

Pursuant to the authority granted to the Secretary in section 13405(d)(2)(G) of the HITECH Act, we proposed an additional exception for disclosures that are required by law as permitted under § 164.512(a) of the Privacy Rule.

Finally, we proposed an exception, pursuant to the authority granted to the Secretary in section 13405(d)(2)(G), for disclosures of protected health information for any other purpose permitted by and in accordance with the applicable requirements of the Privacy Rule, as long as the only remuneration received by the covered entity is a reasonable, cost based fee to cover the cost to prepare and transmit the protected health information for such purpose or is a fee otherwise expressly permitted by other law. We proposed this exception to ensure that the authorization requirement would not deter covered entities from disclosing protected health information for permissible purposes under the Privacy Rule just because they routinely receive payment equal to the cost of preparing, producing, and transmitting the protected health information. We emphasized that this proposed exception would not apply if a covered entity received remuneration above the actual cost incurred to prepare, produce, and transmit the protected health information for the permitted purpose, unless such fee is expressly permitted by other law.

As explained in the NPRM, we recognize that many States have laws in place to limit the fees a health care provider can charge to prepare, copy, and transmit medical records. Under these laws, there is great variation regarding the types of document preparation activities for which a provider can charge as well as the permissible fee schedules for such preparation activities. Some States simply require any reasonable costs incurred by the provider in making copies of the medical records to be paid for by the requesting party, while other States set forth specific cost limitations with respect to retrieval, labor, supplies, and copying costs and allow charges equal to actual mailing or shipping costs. Many of these State laws set different cost limitations based on the amount and type of information to be provided, taking into account whether the information is in paper or electronic form as well as whether the requested material includes x-rays, films, disks, tapes, or other diagnostic imaging. The proposed exception would permit recoupment of fees expressly permitted by these other laws.

Overview of Public Comments

Many commenters asked for clarification on the scope of activities that constitute a ''sale of protected health information.'' Several of these commenters asked that the final rule include a definition of ''sale of protected health information'' and argued that the proposed language at § 164.508(a)(4) was too broad and had the potential to capture a number of activities that should not constitute a ''sale'' of protected health information. Commenters made a variety of suggestions in this regard, including suggesting that a definition of sale should focus on the transfer of ownership of protected health information and thus exclude disclosures pursuant to an access agreement, license, or lease that appropriately limits a recipient's uses or disclosures of the information; or that a definition of sale should more clearly capture those disclosures where remuneration is provided in exchange for protected health information, rather than all disclosures that may involve remuneration. A number of commenters were concerned that fees paid for services or programs that involve the disclosure of protected health information but that are not fees to purchase the data themselves nonetheless would turn such disclosure into a sale of protected health information. For example, some commenters were concerned that the disclosure of research results to a research sponsor would be a sale of protected health information because the sponsor paid the covered entity for its services in conducting the research study or project. Other commenters expressed concern about the authorization requirements for the sale of protected health information applying to programs for which a covered entity receives funding and, as a condition of that funding, is required to report data, such as under the Medicare and Medicaid incentive payment programs for meaningful users of certified electronic health record technology and certain State grant programs. A few commenters were concerned that the exchange of protected health information through a health information exchange (HIE) that is paid for through fees assessed on HIE participants could be considered sale of protected health information.

Commenters also asked for clarification on the meaning and scope of the term ''direct and indirect remuneration,'' and some were particularly concerned that ''indirect remuneration'' meant nonfinancial benefits provided in exchange for protected health information could turn a disclosure into a sale of protected health information. Some commenters stated that prohibiting the receipt of indirect remuneration or nonfinancial benefits may eliminate any incentive for covered entities to participate in certain collaborative research or quality activities, in which covered entities contribute data to a centralized database to create aggregate data sets and in return may receive a number of nonfinancial benefits, such as the ability to use the aggregated information for research or access to quality assurance/quality improvement tools. Certain commenters argued that the term indirect in the statute modifies the ''receipt'' of remuneration (i.e., that the statute also applies to the situation where the remuneration is provided by a third party on behalf of the recipient of the protected health information) and not the type of remuneration.

The public health exception to the remuneration prohibition received a significant amount of support from commenters. Several commenters expressed specific support for the proposal to expand the exception to also apply to disclosures of limited data sets for public health purposes. With respect to the request for comment on the impact of restricting this exception to require that the price charged for the data reflects on the costs of preparing and transmitting the data, commenters were generally opposed to imposing such a restriction. Commenters stated that it may be difficult and burdensome to determine if some of a covered entity's routine public health reporting involve any type of remuneration and

that a cost-based restriction on remuneration would discourage and impede covered entities from making important public health disclosures. One commenter was opposed to the public health exception altogether, stating that it is a privacy loophole that eliminates consumer control over their protected health information.

Many respondents to the proposed sale prohibition commented on the proposed exception for research. While most commenters supported including an exception for research disclosures, including disclosures of limited data sets for research, many argued that the exception should not be limited to the receipt of a reasonable cost-based fee to prepare and transmit the data as such a fee limitation could impede important research efforts. A number of commenters specifically opposed imposing a fee limitation on the disclosure of limited data sets. If a fee limitation were retained, commenters argued that it should be broadly construed. The majority of commenters on this issue supported the proposed exceptions to the remuneration prohibition for treatment and health care payment purposes, as necessary so as not to impede these core health care functions. Overall, support was also expressed by those who commented on the exception for the sale, transfer, merger, or consolidation of a covered entity. Further, commenters generally agreed that a covered entity should be permitted to disclose protected health information without individual authorization as required by law, even if remuneration is received in exchange for the disclosure.

Commenters also submitted a number of comments and questions regarding the ability of business associates to receive fees under both the proposed exception specifically for fees paid by a covered entity to a business associate and the general exception that would allow a covered entity to receive a reasonable, cost-based fee to cover the costs to prepare and transmit the data or a fee otherwise expressly permitted by other law for any disclosure permitted by the Privacy Rule. While commenters generally supported these exceptions, commenters were concerned that these exceptions appeared not to cover the common situation where a business associate, rather than the covered entity, receives remuneration from a third party for making a permitted disclosure under the Privacy Rule. For example, a number of commenters stated that covered entities often outsource to release of information (ROI) vendors the processing of requests for copies of medical records from third parties and that these vendors and not the covered entities bill for the reasonable costs of providing the records to the requestors. Commenters asked that the final rule clarify that business associates can continue to receive payment of costs from third parties for providing this service on behalf of covered entities. Another commenter requested that the final rule clarify that the exception for remuneration to a business associate for activities performed on behalf of a covered entity also applies to remuneration received by subcontractors performing services on behalf of business associates.

Finally, several commenters also responded to the proposed rule's request for comment on the general exception at § 164.508(a)(4)(ii)(H) by suggesting costs that they believed should be permitted, including but not limited to costs for: preparing, producing, and transmitting protected health information; retrieval, labor, supplies, and copying costs; personnel and overhead costs; investments and indirect costs; and any costs that are in compliance with State law.

Final Rule

The final rule adopts the HITECH Act's prohibition on the sale of protected health information but makes certain changes to the provisions in the proposed rule to clarify the scope of the provisions and otherwise address certain of commenters' concerns. First, we have moved the general prohibition on the sale of protected health information by a covered entity or business associate to § 164.502(a)(5)(ii) and created a definition of ''sale of protected health information.'' Numerous commenters requested that the Privacy Rule include a definition of sale to better clarify what types of transactions fall within the scope of the provisions. Accordingly, § 164.502(a)(5)(ii)(B)(*1*) defines ''sale of protected health information'' to generally mean ''a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.'' Section 164.502(a)(5)(ii)(B)(*2*) then excludes from the definition the various exceptions that were in the proposed rule (discussed further below).

We do not limit a ''sale'' to those transactions where there is a transfer of ownership of protected health information as some commenters suggested. The HITECH Act does not include such a limitation and the Privacy Rule rights and protections apply to protected health information without regard to ownership interests over the data. Thus, the sale provisions apply to disclosures in exchange for remuneration including those that are the result of access, license, or lease agreements.

In addition, we do not consider sale of protected health information in this provision to encompass payments a covered entity may receive in the form of grants, or contracts or other arrangements to perform programs or activities, such as a research study, because any provision of protected health information to the payer is a byproduct of the service being provided. Thus, the payment by a research sponsor to a covered entity to conduct a research study is not considered a sale of protected health information even if research results that may include protected health information are disclosed to the sponsor in the course of the study. Further, the receipt of a grant or funding from a government agency to conduct a program is not a sale of protected health information, even if, as a condition of receiving the funding, the covered entity is required to report protected health information to the agency for program oversight or other purposes. (Certain of these disclosures would also be exempt from the sale requirements, depending on whether the requirement to report data was included in regulation or other law.) Similarly, we clarify that the exchange of protected health information through a health information exchange (HIE) that is paid for through fees assessed on HIE participants is not a sale of protected health information; rather the remuneration is for the services provided by the HIE and not for the data itself. (Such disclosures may also be exempt from these provisions under the exception for disclosures to or by a business associate that is being compensated by a covered entity for its services.) In contrast, a sale of protected health information occurs when the covered entity primarily is being compensated to supply data it maintains in its role as a covered entity (or business associate). Thus, such disclosures require the individual's authorization unless they otherwise fall within an exception at § 164.502(a)(5)(ii)(B)(*2*). For example, a disclosure of protected health information by a covered entity to a third party researcher that is conducting the research in exchange for remuneration would fall within these provisions, unless the only

remuneration received is a reasonable, cost-based fee to cover the cost to prepare and transmit the data for such purposes (see below).

In response to questions by commenters, we also clarify the scope of the term ''remuneration.'' The statute uses the term ''remuneration,'' and not ''payment,'' as it does in the marketing provisions at section 13406(a). Because the statute uses different terms, we do not believe that remuneration as applied to the sale provisions is limited to financial payment in the same way it is so limited in the marketing provisions. Thus, the prohibition on sale of protected health information applies to the receipt of nonfinancial as well as financial benefits. In response to commenters who indicated that the statute's terms ''direct and indirect'' apply to how the remuneration is received rather than the remuneration itself, we agree and have moved the terms in the definition to further make clear that the provisions prohibit the receipt of remuneration not only from the third party that receives the protected health information but also from another party on behalf of the recipient of the protected health information. However, this does not change the scope of the term ''remuneration.'' As discussed above, we interpret the statute to mean that nonfinancial benefits are included in the prohibition. Thus, a covered entity or business associate may not disclose protected health information in exchange for in kind benefits, unless the disclosure falls within one of the exceptions discussed below. Consider, for example, a covered entity that is offered computers in exchange for disclosing protected health information. The provision of protected health information in exchange for the computers would not be considered a sale of protected health information if the computers were solely used for the purpose of preparing and transmitting protected health information to the person collecting it and were returned when such disclosure was completed. However, if the covered entity is permitted to use the computers for other purposes or to keep the computers even after the disclosures have been made, then the covered entity has received in kind remuneration in exchange for the protected health information above what is needed to make the actual disclosures.

We retain in the final rule the broad exception for disclosures for public health purposes made pursuant to §§ 164.512(b) and 164.514(e). Based on the concerns from the public comment that narrowing the exception could discourage voluntary public health reporting, we do not limit the exception to only those disclosures where all the covered entity receives as remuneration is a cost-based fee to cover the cost to prepare and transmit the data.

With respect to the exception for research disclosures, the final rule adopts the language as proposed, including the cost-based fee limitation provided for in the HITECH Act. Thus, disclosures for research purposes are excepted from the remuneration prohibition to the extent that the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes. We do not remove the fee limitation as requested by some commenters; the statutory language included in Section 13405(d)(2)(B) of the HITECH Act clearly states that any remuneration received in exchange for research disclosures must reflect only the cost of preparation and transmittal of the data for such purpose.

In response to comments about the types of costs that are permitted in the reasonable cost-based fee to prepare and transmit the data, we clarify that this may include both direct and indirect costs, including labor, materials, and supplies for generating, storing, retrieving, and transmitting the protected health information; labor and supplies to ensure the protected health information is disclosed in a permissible manner; as well as related capital and overhead costs. However, fees charged to incur a profit from the disclosure of protected health information are not allowed. We believe allowing a profit margin would not be consistent with the language contained in Section 13405 of the HITECH Act. We intend to work with the research community to provide guidance and help the research community reach a common understanding of appropriate cost-based limitations on remuneration.

We retain the exceptions proposed for treatment and payment disclosures without modification and agree with commenters that these exceptions are necessary to make clear that these core health care functions may continue. Similarly, we retain the exception to the remuneration prohibition for disclosures for the transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or an entity that following such activity will become a covered entity, and related due diligence, to ensure that such disclosures may continue to occur in accordance with the Privacy Rule. We retain the proposed exception for disclosures that are otherwise required by law to ensure a covered entity can continue to meet its legal obligations without imposing an authorization requirement. We also retain the exception for disclosures to the individual to provide the individual with access to protected health information or an accounting of disclosures, where the fees charged for doing so are in accord with the Privacy Rule.

We adopt the exceptions for remuneration paid by a covered entity to a business associate for activities performed on behalf of a covered entity, as well as the general exception permitting a covered entity to receive remuneration in the form of a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for any disclosure otherwise permitted by the Privacy Rule. However, we make a number of clarifications to address commenters questions and concerns regarding the ability of a business associate rather than a covered entity to receive the permitted remuneration. First, we add the term ''business associate'' in the general exception permitting reasonable, cost-based fees to prepare and transmit data (or fees permitted by State laws) to make clear that business associates may continue to recoup fees from third party record requestors for preparing and transmitting records on behalf of a covered entity, to the extent such fees are reasonable, cost-based fees to cover the cost to prepare and transmit the protected health information or otherwise expressly permitted by other law. Second, we clarify in the business associate exception that the exception would also cover remuneration by a business associate to its subcontractor for activities performed by the subcontractor on behalf of the business associate. Finally, we add the term ''business associate'' to the general prohibition on sale of protected health information for consistency, even though, without the addition, a business associate still would not be permitted to sell protected health information as a business associate may generally only make uses and disclosures of protected health information in manners in which a covered entity would be permitted under the Privacy Rule.

With respect to the types of costs that would be permitted as part of a reasonable, cost-based fee under this provision, we clarify that the final rule permits the same types of costs under this exception as the research exception, as well as costs that are in compliance with a fee schedule provided by State

law or otherwise expressly permitted by other applicable law. Thus, costs may include the direct and indirect costs to prepare and transmit the data, including labor, materials, and supplies, but not a profit margin. We intend to continue to work with interested stakeholders to develop more guidance on direct and indirect costs and on remuneration.

Response to Other Public Comments

Comment: Several commenters suggested that we make clear in the final rule that redisclosures of information by a recipient covered entity or business associate even for remuneration that are set forth in the original authorization are not restricted by this provision. Another commenter argued that the original authorization form should indicate whether the recipient of the protected health information will further exchange the information for remuneration.

Response: It is expected to be the usual case that if a covered entity or business associate that receives protected health information in exchange for remuneration wishes to further disclose that information in exchange for remuneration, then an additional authorization in accordance with § 164.508 must be obtained because such disclosures will not be encompassed by the original authorization. However, it may be possible that redisclosures of information for remuneration by a recipient covered entity or business associate do not require an additional authorization, provided it is sufficiently clear to the individual in the original authorization that the recipient covered entity or business associate will further disclose the individual's protected health information in exchange for remuneration. In response to the commenter that argued that the original authorization form should indicate whether the recipient of the protected health information will further exchange the information for remuneration, as explained above we believe the language included in Section 13405 of the HITECH Act was to alert the individual as to whether the disclosures he or she was authorizing at the time involved remuneration. Where the recipient of protected health information pursuant to an authorization is a third party that is not a covered entity or business associate, we do not have authority to require that entity to disclose to the disclosing covered entity or business associate whether it plans to further exchange the protected health information for remuneration for purposes of including such information on the authorization form. However, covered entities that are informed of such information may include it on the authorization form if they wish to. In any event, the Privacy Rule retains the requirement that an authorization inform the individual of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and to no longer be subject to the Privacy Rule.

Comment: Several commenters asked for clarification on the effect the final rule will have on existing research efforts and some suggested that HHS should grandfather in all Privacy Rule authorizations for research obtained under existing law before the effective date of the final rule. These commenters believed addressing current research would be necessary to ensure the rule would not frustrate ongoing research efforts.

Response: We agree that ongoing research studies that are based on a prior permission under the Privacy Rule for the research use or disclosure of protected health information should be grandfathered so as not to disrupt these ongoing studies. We have added a reference to the authorization requirements that apply to the sale of protected health information at § 164.508(a)(4) to make clear that the transition provisions in § 164.532 apply to permissions existing prior to the applicable compliance date of the Rule. Thus, a covered entity may continue to rely on an authorization obtained from an individual prior to the compliance date even if remuneration is involved but the authorization does not indicate that the disclosure is in exchange for remuneration. This would apply to authorizations for any permissible purpose under the Rule and not just for research purposes. Further, in the research context, where a covered entity obtained documentation of a waiver of authorization from an Institutional Review Board or Privacy Board prior to the compliance date for this final rule, the covered entity may continue to rely on that documentation to release protected health information to a researcher, even if the covered entity receives remuneration in the form of more than a reasonable, cost based fee to prepare and transmit the data. Finally, we also provide at new § 164.532(f) that a covered entity may continue to use or disclose a limited data set in accordance with an existing data use agreement that meets the requirements of § 164.514(e), including for research purposes, until the data use agreement is renewed or modified or until one year from the compliance date of this final rule, whichever is earlier, even if such disclosure would otherwise constitute a sale of protected health information upon the effective date of this rule.

Comment: Some commenters were concerned that the sale prohibition would apply to a covered entity's sale of accounts receivable including protected health information to a collection agency, arguing that such disclosures should remain permissible without authorization as a payment disclosure.

Response: Disclosures of protected health information for payment collection activities are permitted without authorization as a payment disclosure under the Privacy Rule (see §§ 164.501 and 164.506(a)) and thus, are excepted from the remuneration prohibition at § 164.502(a)(5)(ii)(B)(*2*)(*iii*).

Comment: A few commenters asked that the final rule clarify that transfers of value among entities under common control does not implicate the authorization requirements. Similarly, some commenters sought clarification on whether business transfers on the books for internal reorganization would also be excluded under the transfer, merger, and consolidation exception to the final rule.

Response: First, we clarify that uses of protected health information within a covered entity that is a single legal entity are not implicated by the remuneration prohibition as the prohibition applies only to disclosures outside of a covered entity. Second, the use of protected health information among legally separate covered entities under common ownership or control that have designated themselves as an affiliated covered entity (i.e., a single covered entity for purposes of compliance with the HIPAA Rules) is not implicated. See the requirements for affiliated covered entities at § 164.105(b). Thus, to the extent that what the commenters contemplate is an otherwise permissible use of protected health information within a single legal entity that is a covered entity or an affiliated covered entity, such use of data is not impacted by these provisions. Third, disclosures of protected health information for the sale, transfer, merger, or consolidation of all or part of a covered entity with another covered entity, or with an entity that following such activity will become a covered entity and due diligence related to such activity are excepted from the definition of sale of protected health information at § 164.502(a)(5)(ii)(B)(*2*)(*iv*).

Comment: Some commenters expressed concern over the role the

Institutional Review Board will play in determining reasonable costs, and several commenters asked that the final rule clarify that the Institutional Review Board is not responsible for making a determination regarding the permissibility of the fees paid in exchange for a disclosure of protected health information for research purposes.

Response: We clarify that a covered entity, or business associate if applicable, is responsible for determining whether any fees paid to the entity in exchange for protected health information covers the covered entity's or business associate's costs to prepare and transmit protected health information for research.

Comment: A few commenters sought clarification on how to differentiate access to protected health information from access to statistical data, particularly when remuneration is provided for access to a database but the party is solely interested in a population study, not an individual's protected health information.

Response: Disclosures of health information that has been de-identified in accordance with the Privacy Rule at § 164.514(b)–(d) are not subject to the remuneration prohibition as such information is not protected health information under the Rule. However, a covered entity that allows a third party access to a database containing protected health information in exchange for remuneration is subject to these provisions unless an exception applies (e.g., the remuneration received is limited to a reasonable, cost-based fee to prepare and make available the data).

Comment: A number of commenters argued that limited data sets should be exempted entirely from the remuneration prohibition because they are not fully identifiable data sets and are subject to protections under data use agreements.

Response: We decline to completely exempt limited data sets from these provisions as, unlike de-identified data, they are still protected health information. However, disclosures of limited data sets for purposes permitted under the Rule would be exempt from the authorization requirements to the extent the only remuneration received in exchange for the data is a reasonable, cost-based fee to prepare and transmit the data or a fee otherwise expressly permitted by other law. We also provide at new § 164.532(f) that a covered entity may continue to use or disclose a limited data set in accordance with an existing data use agreement that meets the requirements of § 164.514(e), including for research purposes, until the data use agreement is renewed or modified or until one year from the compliance date of this final rule, whichever is earlier, even if such disclosure would otherwise constitute a sale of protected health information upon the effective date of this rule.

b. Research

i. Compound Authorizations

Proposed Rule

Section 164.508(b)(4) of the Privacy Rule prohibits covered entities from conditioning treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an authorization. This limitation is intended to ensure that authorization from an individual for a use or disclosure of protected health information is voluntarily provided. However, there are exceptions to this general rule for certain circumstances, including in the research context, where a covered entity may condition the provision of research-related treatment, such as in a clinical trial, on obtaining the individual's authorization for the use or disclosure of protected health information for such research. Permitting the use of protected health information is part of the decision to receive care through a clinical trial, and health care providers conducting such trials are able to condition research-related treatment on the individual's willingness to authorize the use or disclosure of protected health information for research associated with the trial.

Section 164.508(b)(3) generally prohibits what are termed ''compound authorizations,'' i.e., where an authorization for the use and disclosure of protected health information is combined with any other legal permission. However, § 164.508(b)(3)(i) carves out an exception to this general prohibition, permitting the combining of an authorization for a research study with any other written permission for the same study, including another authorization or informed consent to participate in the research. Nonetheless, § 164.508(b)(3)(iii) prohibits combining an authorization that conditions treatment, payment, enrollment in a health plan, or eligibility for benefits (conditioned authorization) with an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned (unconditioned authorization). This limitation on certain compound authorizations was intended to help ensure that individuals understand that they may decline the activity described in the unconditioned authorization yet still receive treatment or other benefits or services by agreeing to the conditioned authorization.

The impact of these authorization requirements and limitations can be seen during clinical trials that are associated with a corollary research activity, such as when protected health information is used or disclosed to create or to contribute to a central research database or repository. For example, § 164.508(b)(3)(iii) prohibits covered entities from obtaining a single authorization for the use or disclosure of protected health information for a research study that includes both treatment as part of a clinical trial and tissue banking of specimens (and associated protected health information) collected, since the individual generally must sign the authorization for the use of his or her protected health information in the clinical trial in order to receive the research-related treatment (conditioned authorization) but whether the individual also signs the tissue banking authorization is completely voluntary and will not affect the individual receiving the research-related treatment (unconditioned authorization). Thus, covered entities must obtain separate authorizations from research participants for a clinical trial that also collects specimens with associated protected health information for a central repository.

As stated in the NPRM, various groups, including researchers and professional organizations, have expressed concern at this lack of integration. A number of persons in the research community have stated that requiring separate forms for these corollary research activities is inconsistent with current practice under the Common Rule (45 CFR Part 46) with respect to obtaining informed consent and creates unnecessary documentation burdens. Persons have also indicated that the multiple authorization forms are potentially confusing to research subjects and/or may dissuade them altogether from participating in a clinical trial, and that redundant information on the forms diverts an individual's attention from other content that describes how and why the personal health information may be used. In light of these concerns, the Secretary's Advisory Committee on Human Research Protections in 2004 (Recommendation V, in a letter to the Secretary of HHS, available at *http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html*), as well as the Institute of Medicine in its 2009 Report, ''Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research''

(Recommendation II.B.2), made specific recommendations to allow combined authorizations for clinical trials and biospecimen storage.

To address these concerns and streamline the process in the Privacy Rule for obtaining an individual's authorization for research, we proposed to amend § 164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. These provisions would allow covered entities to combine authorizations for the use and disclosure of protected health information for clinical trials and related biospecimen banking activities, as well as other scenarios that often occur in research studies.

While we did not propose to alter the core elements or required statements integral to a valid authorization, we stated that covered entities would have some flexibility with respect to how they met the authorization requirements. For example, covered entities could facilitate an individual's understanding of a compound authorization by describing the unconditioned research activity on a separate page of a compound authorization and could also cross-reference relevant sections of a compound authorization to minimize the potential for redundant language. In addition, a covered entity could use a separate check-box for the unconditioned research activity to signify whether an individual has opted-in to the unconditioned research activity, while maintaining one signature line for the authorization, or alternatively provide a distinct signature line for the unconditioned authorization to signal that the individual is authorizing optional research that will not affect research-related treatment. We requested comment on additional methods that would clearly differentiate to the individual the conditioned and unconditioned research activities on the compound authorization.

Overview of Public Comments

Almost all commenters on this topic strongly supported the proposal to allow combined authorizations for conditioned and unconditioned research activities. Many commenters supported allowing flexibility for institutions to determine how best to differentiate the unconditioned authorization for the voluntary research activity, including whether to use a check box with a single signature line, or separate signature lines. Several commenters suggested that an opt out method should be permitted as an alternative to an opt in approach.

A few commenters opposed the proposal to allow compound authorizations for conditioned and unconditioned research activities. These commenters generally felt that separate authorizations are appropriate and that there is not sufficient evidence to suggest that combining the forms will be beneficial to individuals.

The Secretary's Advisory Committee on Human Research Protections, in its letter of comment on the Department's NPRM, indicated its support for the proposal to permit compound authorizations for conditioned and unconditioned research activities, and expressed particular appreciation for the goal of harmonization with the Common Rule. The Secretary's Advisory Committee on Human Research Protections also supported flexibility in the manner that the conditioned and unconditioned research activities are differentiated. The Secretary's Advisory Committee on Human Research Protections requested clarification that the compound authorizations permitted under this proposal would be permissible for any type of combined research studies, and not exclusively for clinical trials with a biospecimen banking component.

Final Rule

The final rule adopts the proposal to amend § 164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. We intend this provision to allow for the use of compound authorizations for any type of research activities, and not solely to clinical trials and biospecimen banking, except to the extent the research involves the use or disclosure of psychotherapy notes. For research that involves the use or disclosure of psychotherapy notes, an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes. See § 164.508(b)(3)(ii). Thus, aside from the use of psychotherapy notes, combined authorizations could be obtained for the use of protected health information in a clinical trial and optional sub-studies, as well as for biospecimen banking that also permits future secondary use of the data (to the extent the future use authorization is aligned with the discussion in the following section regarding authorizations for future research). Also, this provision continues to allow for a covered entity to combine such authorizations with informed consent documents for the research studies.

The final rule provides covered entities, institutions, and Institutional Review Boards with flexibility to determine the best approach for clearly differentiating the conditioned and unconditioned research activities and giving research participants the option to opt in to the unconditioned research activities. We decline to permit a combined authorization that only allows the individual the option to opt out of the unconditioned research activities (e.g., ''check here if you do NOT want your data provided to the biospecimen bank'') because an opt out option does not provide individuals with a clear ability to authorize the optional research activity, and may be viewed as coercive by individuals. The final rule does not remove the requirement that an individual affirmatively authorize the unconditioned research activities; it merely provides flexibility to streamline the authorization process by combining the forms.

With respect to the commenters that believed there is insufficient evidence that combining conditioned and unconditioned research activities into a compound authorization would be beneficial, and that such compound authorizations may be confusing for patients, as indicated above, there have been anecdotal reports to the Department that the use of multiple authorization forms has caused confusion among research subjects. Further, we note that these modifications do not remove the required elements of an authorization that are necessary to inform the individual about the study (e.g., description of the information to be used or disclosed, description of the purpose, etc.); they merely introduce flexibility to avoid redundant language that would otherwise be necessary to include in the authorizations for the multiple research activities. In addition, these changes are intended to align the HIPAA Privacy Rule's authorization requirements with what has been common and ongoing practice in terms of the informed consent form under the Common Rule.

We note that covered entities are permitted but not required by the modifications adopted at

§ 164.508(b)(3)(i) and (iii) to create compound authorizations for conditioned and unconditioned research activities. Previously approved, ongoing studies may continue to rely on the separate authorization forms that were obtained under the prior provisions. For new studies, covered entities and researchers may continue to use separate authorizations for conditioned and unconditioned research activities, or may transition to compound authorizations as they deem appropriate, which can be used beginning on the effective date of this rule.

Response to Other Public Comments

Comment: The Secretary's Advisory Committee on Human Research Protections asked whether the following approaches for distinguishing between conditioned and unconditioned research activities would be acceptable: Using (1) a combined consent/authorization form for a clinical trial and optional banking component, with a check-box for the individual to have the choice to opt in to the optional banking component, and one signature; (2) a combined consent/authorization form for a clinical trial and optional banking component, with one signature for the clinical trial and another signature to indicate the individual agrees to the optional banking component; and (3) a combined consent/authorization form for a clinical trial and optional banking component, with a check box for the individual to have the choice to opt in to the banking component, and one signature, but with detailed information about the banking component presented in a separate brochure or information sheet that is referenced directly in the consent/authorization form.

Response: Covered entities and researchers have flexibility in the methods used to distinguish the conditioned and unconditioned research activities and to provide the individual with a clear opportunity to opt in to the unconditioned portion, and all of the above approaches would be acceptable provided, with respect to the third approach, that the brochure or information sheet is incorporated by reference into the authorization/consent form such that it is considered to be part of the form (even if not physically attached to the form). In addition, if the brochure or information sheet includes required elements of the authorization (or informed consent), and authorization/consent has not been altered by an Institutional Review Board, then the brochure or information sheet must be made available to potential research participants before they are asked to sign the authorization/consent document (unless the authorization form itself includes the required elements). Finally, in such cases, a covered entity must keep not only the signed authorization/consent form, but also a copy of the brochure or information sheet, in order to be in compliance with the documentation requirements at § 164.530(j).

Comment: The Secretary's Advisory Committee on Human Research Protections requested confirmation that the compound authorization proposal would not affect the waiver provisions currently existing in the Privacy Rule, such that such provisions could be used, if appropriate, for new studies distinct from both the original study and the banking activity.

Response: The new compound authorization provision does not affect the waiver of authorization provisions in the Privacy Rule. A covered entity may continue to use or disclose protected health information for research purposes based on documentation that meets the requirements at § 164.512(i), indicating that an Institutional Review Board or Privacy Board has waived the obtaining of individual authorization for such purposes, based on a determination that (1) the use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals; (2) the research could not practicably be conducted without the waiver; and (3) the research could not practicably be conducted without access to and use of the protected health information.

Comment: The Secretary's Advisory Committee on Human Research Protections requested clarification on the effect of revoking only one part of a compound authorization. For example, if an individual signs a combined authorization for conditioned and unconditioned research activities and later specifically revokes only the unconditioned research activity (e.g., the banking component), then the covered entity may continue to act in reliance on the authorization for the conditioned component (e.g., the clinical trial).

Response: Where it is clear that an individual is revoking only one part of a compound authorization, such revocation does not equate to a revocation of the entire authorization to include the other studies. However, where it is not clear exactly to which research activities the individual's revocation applies, written clarification must be obtained from the individual in order for the revocation to apply only to certain of the research activities identified in the authorization, or the entire authorization must be treated as revoked. Further, such revocations must be maintained and documented in a manner that will ensure uses and disclosures of protected health information for the activity to which the revocation applies discontinue, except to the extent the covered entity has already acted in reliance on the authorization, which would permit certain limited, continued use and disclosure, such as necessary to maintain the integrity of the research study.

ii. Authorizing Future Research Use or Disclosure

Prior Interpretation

Research often involves obtaining health information and biological specimens to create a research database or repository for future research. For example, this frequently occurs where clinical trials are paired with corollary research activities, such as the creation of a research database or repository where information and specimens obtained from a research participant during the trial are transferred and maintained for future research. It is our understanding that Institutional Review Boards in some cases may approve an informed consent document for a clinical trial that also asks research participants to permit future research on their identifiable information or specimens obtained during the course of the trial. It is also our understanding that an Institutional Review Board may in some cases review an informed consent for a prior clinical trial to determine whether a subsequent research use is encompassed within the original consent.

The Department has previously interpreted the Privacy Rule, however, to require that authorizations for research be study specific for purposes of complying with the Rule's requirement at § 164.508(c)(1)(iv) that an authorization must include a description of each purpose of the requested use or disclosure. See 67 FR 53182, 53226, Aug. 14, 2002. In part, the Department's interpretation was based on a concern that patients could lack necessary information in the authorization to make an informed decision about the future research. In addition, it was recognized that not all uses and disclosures of protected health information for a future research purpose would require a covered entity to re-contact the individual to obtain another authorization (e.g., uses or disclosures with a waiver of

authorization from an Institutional Review Board or Privacy Board as provided under § 164.512(i) or of a limited data set pursuant to a data use agreement under § 164.514(e) for the future research purpose).

Subsequent to issuing this interpretation, the Department heard concerns from covered entities and researchers that the Department's interpretation encumbers secondary research, and limits an individual's ability to agree to the use or disclosure of their protected health information for future research. In addition, many commenters noted that the Department's interpretation limiting the scope of a HIPAA authorization for research appeared to diverge from the current practice under the Common Rule with respect to the ability of a researcher to seek subjects' informed consent to future research so long as the future research uses are described in sufficient detail to allow an informed consent. These commenters, as well as the Secretary's Advisory Committee on Human Research Protections in 2004 (Recommendation IV, in a letter to the Secretary of HHS, available at *http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html*) and the Institute of Medicine in its 2009 Report entitled ''Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research'' (Recommendation II.B.1), had urged the Department to allow the HIPAA authorization to permit future research use and disclosure of protected health information.

Given these concerns, the Department explained in the NPRM that it was considering a number of options regarding authorizations for future research, including whether the Privacy Rule should: permit an authorization for uses and disclosures of protected health information for future research purposes to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research; or permit an authorization for future research but require certain specific elements or statements with respect to the future research, particularly where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or mental health research, that may alter an individual's willingness to participate in the research. We requested comment on these options and on how a revocation would operate with respect to future downstream research studies.

Overview of Public Comments

Almost all commenters on this topic supported the proposal to allow authorizations for future research. Many commenters indicated this flexibility to be important, particularly considering evolving technologies and discoveries.

About half of these commenters specifically advocated for providing investigators and Institutional Review Boards with the maximum flexibility to determine the appropriateness of the descriptions for future research and felt that this would best align with the Common Rule. These commenters were thus against requiring specific statements in the Privacy Rule about the future research, including for sensitive research. Other commenters were in favor of requiring the additional statements about sensitive categories of research, stating that this would better inform individuals and give them greater choice in determining their willingness to participate in certain types of future research. A couple of these commenters recommended working with National Committee on Vital and Health Statistics on the categories of sensitive research, however no further examples of specific types of research were given beyond the examples provided in the proposed rule (genetic analyses or mental health research). Several commenters specifically advised against requiring specific statements for sensitive research, citing concerns of variability in what is considered sensitive information and practicality challenges due to the changing nature of the concept over time.

A few commenters opposed the proposal to allow authorizations for future research altogether. Some of these commenters felt strongly that study-specific authorizations are critical to protect patients, and are the only way that individuals can make a truly informed decision. These commenters suggested that outreach to patients and potential research participants to solicit feedback, as well as a study on the potential burdens that enhanced authorizations may have on stakeholders, were necessary before any changes were made.

In its comment letter on the NPRM, the Secretary's Advisory Committee on Human Research Protections supported the proposal to harmonize HIPAA authorizations with the Common Rule informed consent requirements, and also requested consultation with the FDA to ensure that authorizations for future research align not only with the Common Rule standards but also FDA standards for informed consent. They indicated that the authorization should be reasonably specific such that individuals are aware of the types of research that may be conducted. However, the Secretary's Advisory Committee on Human Research Protections emphasized the need for flexibility to rely on Institutional Review Board judgment and recommended against requiring prescribed statements about certain types of ''sensitive'' research, since these concepts change over time and requiring prescribed authorization statements may conflict with Institutional Review Boards' judgments about how to appropriately describe the research in the informed consent.

Modified Interpretation

We modify the prior Departmental interpretation that research authorizations must be study specific. This modification does not make any changes to the authorization requirements at § 164.508. A HIPAA authorization for future research must still address each of the core elements and statements required at § 164.508(c). However, the Department no longer interprets the ''purpose'' provision at § 164.508(c)(1)(iv) as requiring that an authorization for the use or disclosure of protected health information for research purposes be study specific. In order to satisfy the requirement that an authorization include a description of each purpose of the requested use or disclosure, an authorization for uses and disclosures of protected health information for future research purposes must adequately describe such purposes such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research. This could include specific statements with respect to sensitive research to the extent such research is contemplated. However, we do not prescribe specific statements in the Rule. We agree that it is difficult to define what is sensitive and that this concept changes over time. We also agree with commenters that this approach best harmonizes with practice under the Common Rule regarding informed consent for future research, and allows covered entities, researchers and Institutional Review Boards to have flexibility in determining what adequately describes a future research purpose depending on the circumstances. We have consulted with Office for Human Research Protections (OHRP) and the FDA on this approach to ensure consistency and

harmonization with the HHS and FDA human subjects protections regulations, where appropriate.

With respect to commenters that stated it is impossible for individuals to be truly informed about future research, we note that we are aligning with existing practice under the Common Rule in regard to informed consent and still require that all required elements of authorization be included in an authorization for future research, even if they are to be described in a more general manner than is done for specific studies.

Pursuant to this modified interpretation, covered entities that wish to obtain individual authorization for the use or disclosure of protected health information for future research may do so at any time after the effective date of this final rule. Alternatively, covered entities may continue to use only study-specific authorizations for research if they choose.

Response to Other Public Comments

Comment: The Secretary's Advisory Committee on Human Research Protections requested flexibility regarding the description in the authorization of the information to be used or disclosed for future research as well as to whom the covered entity may make the requested use or disclosure as there may be some uncertainty of the identity of future researchers. The Secretary's Advisory Committee on Human Research Protections also suggested that the description of information to be collected be allowed to reference information beyond the time of the original study, for example ''your future medical records [at Hospital]'' or ''your future medical records [relating to diseases/conditions].''

Response: Covered entities and researchers have flexibility to describe the information to be used or disclosed for the future research, so long as it is reasonable from such description to believe that the individual would expect the information to be used or disclosed for the future research. We also clarify that a description of the protected health information to be used for the future research may include information collected beyond the time of the original study. Further, the Privacy Rule authorization requirements allow a ''class of persons'' to be described for purposes of identifying in the authorization the recipients of the protected health information. Thus, covered entities and researchers have flexibility in the manner in which they describe the recipients of the protected health information for the future research, so long as it is reasonable from such description to believe that the individual would expect his or her protected health information to be shared with such persons for the future research.

Comment: The Secretary's Advisory Committee on Human Research Protections requested that the Department allow for grandfathering of existing, ongoing studies that involve the possibility of future/secondary research, if an Institutional Review Board-approved consent reasonably informed the individuals of the future research. In these situations, researchers would have needed to obtain a study-specific authorization or waiver of authorization before commencing the future/secondary research that was encompassed in the original informed consent.

Response: Covered entities and researchers may rely on an Institutional Review Board-approved consent obtained prior to the effective date of this final rule that reasonably informed individuals of the future research, provided the informed consent was combined with a HIPAA authorization (even though the authorization itself was specific to the original study or creation and maintenance of a repository).

Comment: One commenter advocated for the use of time-limited authorizations for future research.

Response: This modification in Departmental interpretation does not change the requirement at § 164.508(c)(1)(v), which states that an authorization must contain an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. This statement may be a specific time limit, or be ''end of the research study,'' ''none,'' or similar language for a research study.

Comment: Several commenters suggested that revocation of authorizations should continue to be permitted in the same manner that it is currently allowed under the Privacy Rule. The Secretary's Advisory Committee on Human Research Protections recommended that revocations of authorization for future research be permitted orally, rather than in writing, as is currently required for all authorizations under §§ 164.508(b)(5) and (c)(2)(i) of the Rule.

Response: Covered entities may continue to rely on existing guidance regarding how revocations of authorizations operate in the research context. Such guidance is published in several materials available at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/research/index.html* (see, e.g., the fact sheet entitled, ''Health Services Research and the HIPAA Privacy Rule''). The Department may issue additional guidance in the future with respect to revocation policies in the context of authorizations that specify, and under which protected health information has been disclosed for, future research uses.

In response to the Secretary's Advisory Committee on Human Research Protections recommendation, we also clarify that while the Privacy Rule requires that a revocation of authorization from an individual be in writing, uses and disclosures pursuant to an authorization are permissive and not required, and thus, a covered entity may cease using or disclosing protected health information pursuant to an authorization based on an individual's oral request if it chooses to do so.

5. Protected Health Information About Decedents

a. Section 164.502(f)—Period of Protection for Decedent Information

Proposed Rule

Section 164.502(f) requires covered entities to protect the privacy of a decedent's protected health information generally in the same manner and to the same extent that is required for the protected health information of living individuals. Thus, if an authorization is required for a particular use or disclosure of protected health information, a covered entity may use or disclose a decedent's protected health information in that situation only if the covered entity obtains an authorization from the decedent's personal representative. The personal representative for a decedent is the executor, administrator, or other person who has authority under applicable law to act on behalf of the decedent or the decedent's estate. The Department heard a number of concerns since the publication of the Privacy Rule that it can be difficult to locate a personal representative to authorize the use or disclosure of the decedent's protected health information, particularly after an estate is closed. Furthermore, archivists, biographers, and historians had expressed frustration regarding the lack of access to ancient or old records of historical value held by covered entities, even when there are likely few surviving individuals concerned with the privacy of such information. Archives and libraries may hold medical records, as well as correspondence files, physician diaries and casebooks, and photograph collections containing fragments of

identifiable health information, that are centuries old. Currently, to the extent such information is maintained by a covered entity, it is subject to the Privacy Rule.

Accordingly, we proposed to amend § 164.502(f) to require a covered entity to comply with the requirements of the Privacy Rule with regard to the protected health information of a deceased individual for a period of 50 years following the date of death. We also proposed to modify the definition of ''protected health information'' at § 160.103 to make clear that the individually identifiable health information of a person who has been deceased for more than 50 years is not protected health information under the Privacy Rule. We proposed 50 years to balance the privacy interests of living relatives or other affected individuals with a relationship to the decedent, with the difficulty of obtaining authorizations from personal representatives as time passes. A 50-year period of protection had also been suggested at a National Committee for Vital and Health Statistics (the public advisory committee which advises the Secretary on the implementation of the Administrative Simplification provisions of HIPAA, among other issues) meeting, at which committee members heard testimony from archivists regarding the problems associated with applying the Privacy Rule to very old records. See *http://ncvhs.hhs.gov/050111mn.htm*. We requested public comment on the appropriateness of this time period.

Overview of Public Comments

The majority of public comment on this proposal was in favor of limiting the period of protection for decedent health information to 50 years past the date of death. Some of these commenters specifically cited the potential benefits to research. A few commenters stated that the 50-year period was too long and should be shortened to, for example, 25 years. Some supporters of limiting privacy protection for decedent information indicated that the date of death is often difficult to determine, and thus suggested an alternative time period (e.g., 75, 100, 120, 125 years) starting from the last date in the medical record, if the date of death is unknown.

Some commenters were opposed to limiting the period of protection for decedent health information due to the continued privacy interests of living relatives as well as the decedent, particularly when highly sensitive information is involved, including HIV/AIDS status, or psychiatric or substance abuse treatment. A couple of commenters recommended that there should be no time limit on the protection of psychotherapy notes. One commenter expressed concern that this modification may encourage covered entities to retain records that they would not have otherwise in order to profit from the data after the 50-year period. One commenter suggested that the period of protection should be extended to 100 years, if protections are to be limited at all. A few commenters were opposed to the 50-year period of protection because they interpreted this provision to be a proposed record retention requirement.

Final Rule

After considering the public comments, the final rule adopts the proposal. We believe 50 years is an appropriate period of protection for decedent health information, taking into account the remaining privacy interests of living individuals after the span of approximately two generations have passed, and the difficulty of obtaining authorizations from a personal representative of a decedent as the same amount of time passes. For the same reason, we decline to shorten the period of protection as suggested by some commenters or to adopt a 100-year period of protection for decedent information. We also believe the 50-year period of protection to be long enough so as not to provide an incentive for covered entities to change their record retention policies in order to profit from the data about a decedent once 50 years has elapsed.

With respect to commenters' concerns regarding protected health information about decedents that is sensitive, such as HIV/AIDS, substance abuse, or mental health information, or that involves psychotherapy notes, we emphasize that the 50-year period of protection for decedent health information under the Privacy Rule does not override or interfere with State or other laws that provide greater protection for such information, or the professional responsibilities of mental health or other providers. Covered entities may continue to provide privacy protections to decedent information beyond the 50-year period, and may be required to do so under other applicable laws or as part of their professional responsibility. Alternatively, covered entities may choose to destroy decedent information although other applicable law may prescribe or limit such destruction.

We also decline to limit protections under the Privacy Rule to a certain period beyond the last date in the medical record. While we appreciate the challenges that may be present in determining the date of death of an individual in cases in which it is not sufficiently clear from the age of the record whether the individual is deceased, we believe that this determination is necessary in closer cases to protect the individual, as well as living relatives and others, who may be affected by disclosure of the information. Further, as we stated in the NPRM, this modification has no impact on a covered entity's disclosures permitted under other provisions of the Privacy Rule. For example, a covered entity is permitted to disclose protected health information of decedents for research that is solely on the information of decedents in accordance with § 164.512(i)(1)(iii), without regard to how long the individual has been deceased.

Finally, we clarify that the 50-year period of protection is not a record retention requirement. The HIPAA Privacy Rule does not include medical record retention requirements and covered entities may destroy such records at the time permitted by State or other applicable law. (We note that covered entities are subject to the accounting requirements at § 164.528 and, thus, would need to retain or record certain information regarding their disclosures of protected health information.) However, if a covered entity does maintain decedent health information for longer than 50 years following the date of death of the individual, this information will no longer be subject to the Privacy Rule.

b. Section 164.510(b)—Disclosures About a Decedent to Family Members and Others Involved in Care

Proposed Rule

Section 164.510(b) describes how a covered entity may use or disclose protected health information to persons, such as family members or others, who are involved in an individual's care or payment related to the individual's health care. The Department had received a number of questions about the scope of the section, specifically with regard to disclosing protected health information when the individual who is the subject of the information was deceased. We had additionally heard concerns that family members, relatives, and others, many of whom may have had access to the health information of the deceased individual prior to death, have had difficulty obtaining access to such information after the death of the individual, because many do not qualify as a

''personal representative'' of the decedent under the Privacy Rule at § 164.502(g)(4).

As such, we proposed to amend § 164.510(b) to add a new paragraph (5), which would permit covered entities to disclose a decedent's information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. We emphasized that these modifications would not change the authority of a decedent's personal representative with regard to the decedent's protected health information. Thus, a personal representative would continue to have a right to access the decedent's protected health information relevant to such personal representation, and have authority to authorize uses and disclosures of the decedent's protected health information that are not otherwise permitted or required by the Privacy Rule. We requested comment on any unintended consequences that this proposed disclosure provision might cause.

Overview of Public Comments

Most commenters supported the proposal to permit disclosures to family members and others involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. These commenters felt that such permissive disclosures would help facilitate important and appropriate communications with family members and others who had been involved in the individual's care or payment for health care prior to the individual's death but who may not rise to the level of personal representative. Some commenters stated that the provision recognizes the legitimate interest that family members may have in a decedent's health information as it affects their own health care.

A few commenters opposed the proposal to expressly permit communications with family members and other persons who had been involved with the individual's care or payment for care prior to death. Two commenters felt it would be a large burden on covered entities to determine the legitimacy of a requestor as a family member or individual involved in the care or payment for care. One commenter questioned the need for family members to have access to decedent health information and the likelihood of anyone other than the personal representative to have been meaningfully involved in the care or payment for care of the decedent.

Final Rule

The final rule adopts the proposal to amend § 164.510(b) to permit covered entities to disclose a decedent's protected health information to family members and others who were involved in the care or payment for care of the decedent prior to death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

In response to commenters who opposed this provision, we believe the provision strikes the appropriate balance in allowing communications with family members and other persons who were involved in the individual's care or payment for care prior to death, unless doing so is inconsistent with the prior expressed wishes of the individual. This will ensure family members and others can find out about the circumstances surrounding the death of their loved ones, unless the individual prior to his or her death objected to the covered entity making such communications. Further, the Privacy Rule limits such disclosures, similar to the other disclosures permitted under § 164.510(b), to the protected health information relevant to the family member or other person's involvement in the individual's health care or payment for health care. For example, a covered health care provider could describe the circumstances that led to an individual's passing with the decedent's sister who is asking about her sibling's death. In addition, a covered health care provider could disclose billing information to a family member of a decedent who is assisting with wrapping up the decedent's estate. However, in both of these cases, the provider generally should not share information about past, unrelated medical problems. Finally, these disclosures are permitted and not required, and thus, a covered entity that questions the relationship of the person to the decedent or otherwise believes, based on the circumstances, that disclosure of the decedent's protected health information would not be appropriate, is not required to make the disclosure.

Response to Other Public Comments

Comment: Commenters requested guidance on what it means for a person to have been ''involved in the care'' of the decedent prior to death. One commenter suggested including language in the final rule that would put the burden of proof of ''involvement in the individual's care'' on the requestor and not the covered entity, and would hold the covered entity harmless when disclosing decedent information in good faith in accordance with this new permission.

Response: We interpret this phrase in the same manner as we have with respect to disclosures of protected health information of living individuals under § 164.510(b). See the Department's existing guidance at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/provider_ffg.pdf*. Subject to the specified conditions, disclosures may be made under this provision to family members, as well as to other persons provided the covered entity has reasonable assurance the individual prior to death was involved in the individual's care or payment for care. Depending on the circumstances, this could include disclosures to spouses, parents, children, domestic partners, other relatives, or friends of a decedent. As with similar disclosures concerning living individuals under § 164.510(b)(1)(i), this provision does not generally apply to disclosures to health care providers, health plans, public health authorities, law enforcement officials, and others whose access to protected health information is governed by other provisions of the Privacy Rule.

We decline to include language in the final rule placing the burden of proof on the requestor to demonstrate they were involved in the individual's care. In some cases, it will be readily apparent to the covered entity that a person is a family member or was involved in the individual's care prior to death because the person would have made themselves known to the covered entity prior to the individual's death by either visiting with or inquiring about the individual, or the individual would have identified such person as being involved in their care or payment for care to a member of the covered entity's workforce. In other cases, the covered entity need just have reasonable assurance that the person is a family member of the decedent or other person who was involved in the individual's care or payment for care prior to death. For example, the person may indicate to the covered entity how he or she is related to the decedent or offer sufficient details about the decedent's circumstances prior to death to indicate involvement in the decedent's care prior to death. As stated above, a covered entity that is uncomfortable disclosing protected health information under this provision because of questions about the person's

relationship to the decedent is not required to do so.

Comment: Several commenters requested and offered suggested clarifications on the scope of the terms ''personal representative'' and ''family member.''

Response: The Privacy Rule already identifies the persons who qualify as a personal representative of a decedent at § 164.502(g)(4). Further, this final rule includes a definition of ''family member'' at § 160.103.

Comment: A few commenters suggested extending this provision to allow disclosures to the decedent's health care ''proxy,'' ''medical power of attorney,'' ''power of attorney,'' and ''estate executor.''

Response: We decline to expand the provision as suggested. Under the Privacy Rule, a person with authority under applicable law to act on behalf of the decedent or the decedent's estate is the personal representative of the decedent. Thus, certain of these persons, such as the executor of the estate, already have a right of access to the decedent's protected health information. In cases where a person does not rise to the level of a personal representative, the final rule at § 164.510(b) permits, subject to any prior expressed preference of the individual, a covered entity to disclose relevant protected health information of the decedent to family members of the decedent or persons who otherwise were involved in the individual's care or payment for care prior to the individual's death, which may include persons who held a health care proxy for the individual or a medical power of attorney.

6. Section 164.512(b)—Disclosure of Student Immunizations to Schools

Proposed Rule

The Privacy Rule, at § 164.512(b), recognizes that covered entities must balance protecting the privacy of health information with sharing health information with those responsible for ensuring public health and safety, and permits covered entities to disclose the minimum necessary protected health information to public health authorities or other designated persons or entities without an authorization for public health purposes specified by the Rule.

Schools play an important role in preventing the spread of communicable diseases among students by ensuring that students entering classes have been immunized. Most States have ''school entry laws'' which prohibit a child from attending school unless the school has proof that the child has been appropriately immunized. Some States allow a child to enter school provisionally for a certain period of time while the school waits for the necessary immunization information. Typically, schools ensure compliance with those requirements by requesting the immunization records from parents (rather than directly from a health care provider). However, where a covered health care provider is requested to send the immunization records directly to a school, the Privacy Rule generally requires written authorization by the child's parent before a covered health care provider may do so.

Since the Privacy Rule went into effect, we had heard concerns that the requirement for covered entities to obtain authorization before disclosing student immunization information may make it more difficult for parents to provide, and for schools to obtain, the necessary immunization documentation for students, which may prevent students' admittance to school. The National Committee on Vital and Health Statistics submitted these concerns to the HHS Secretary and recommended that HHS regard disclosure of immunization records to schools to be a public health disclosure, thus eliminating the requirement for authorization. See *http://www.ncvhs.hhs.gov/04061712.html.* As such, we proposed to amend § 164.512(b)(1) by adding a new paragraph that permits covered entities to disclose proof of immunization to schools in States that have school entry or similar laws.[10] While written authorization that complies with § 164.508 would no longer have been required for disclosure of such information under the proposal, the covered entity would still have been required to obtain agreement, which may have been oral, from a parent, guardian or other person acting *in loco parentis* for the individual, or from the individual him- or herself, if the individual is an adult or emancipated minor. Because the proposed provision would have permitted a provider to accept a parent's oral agreement to disclose immunization results to a school—as opposed to a written agreement—the NPRM acknowledged a potential for a miscommunication and later objection by the parent. We, therefore, requested comment on whether the Privacy Rule should require that a provider document any oral agreement under this provision to help avoid such problems, or whether a requirement for written documentation would be overly cumbersome, on balance. We also requested comment on whether the rule should mandate that the disclosures go to a particular school official and if so, who that should be.

In addition, the Privacy Rule does not define the term ''school'' and the types of schools subject to the school entry laws may vary by State. For example, depending on the State, such laws may apply to public and private elementary or primary schools and secondary schools (kindergarten through 12th grade), as well as daycare and preschool facilities, and post-secondary institutions. Thus, we requested comment on the scope of the term ''school'' for the purposes of this section and whether we should include a specific definition of ''school'' within the regulation itself. In addition, we requested comment on the extent to which schools that may not be subject to these school entry laws but that may also require proof of immunization have experienced problems that would warrant their being included in this category of public health disclosures.

Overview of Public Comments

Most commenters were generally in favor of permitting covered entities to disclose student immunization records based on obtaining agreement, which may be oral, from a parent, guardian or other person acting *in loco parentis* for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor, rather than written authorization. Commenters supported the intent to facilitate the transmission of immunization records to ease the burden on parents, schools and covered entities, and to minimize the amount of school missed by students.

Some commenters opposed the proposal to require oral or written agreement, claiming that a new form of ''agreement'' would introduce unnecessary complexity and confusion, and would not help to reduce burden. These commenters asserted that covered entities would document the verbal agreements for their own liability purposes, even if not required by the Privacy Rule. In this manner, the documentation burden would still be

[10] We note that once a student's immunization records are obtained and maintained by an educational institution or agency to which the Family Educational Rights and Privacy Act (FERPA) applies, the records are protected by FERPA, rather than the HIPAA Privacy Rule. See paragraphs (2)(i) and (2)(ii) of the definition of ''protected health information'' at § 160.103, which exclude from coverage under the Privacy Rule student records protected by FERPA. In addition, for more information on the intersection of FERPA and HIPAA, readers are encouraged to consult the Joint HHS/ED Guidance on the Application of FERPA and HIPAA to Student Health Records, available at *http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hipaaferpajointguide.pdf.*

present. Some commenters recommended that instead of an oral agreement or authorization requirement, disclosure of immunization records to schools should be considered an exempt public health disclosure. A small minority of commenters felt that the current authorization system should be maintained as it is the best way to ensure patient safety and privacy while avoiding miscommunications and misunderstandings.

Commenters were divided on the issue of requiring written documentation of the agreement. Some commenters were in favor of documenting oral agreements, citing that the documentation would be less cumbersome than obtaining written authorizations while also helping to avoid miscommunications. On the other hand, some commenters felt that requiring written documentation would be burdensome and would eliminate the benefits introduced by permitting oral agreements. Some commenters also requested flexibility for covered entities to determine whether or not written documentation is appropriate and necessary for their purposes.

The majority of commenters requested that a designated recipient of the student immunization records not be defined, and that schools be allowed flexibility to identify the appropriate individual(s) that can act as the school official permitted to receive the records. Commenters indicated that while the disclosures would ideally be made to a nurse or licensed health professional at the school, such a health professional may not always be present. In such instances, it should be permissible that the immunization records be disclosed to another official designated by the school as a suitable representative. One commenter recommended that the school nurse be designated as the recipient and custodian of the records.

Most commenters recommended that the definition of ''school'' be interpreted broadly in order to best support public health efforts. Commenters provided suggestions on the types of schools that should be included, for example, K–12 schools, public and private schools, and post-secondary schools. Many commenters also suggested that daycare, preschool and nursery school facilities be encompassed in the definition of school. One commenter expressly recommended that child care facilities or day care programs not be included in the definition of school, despite acknowledging the need to protect the health of these children, due to the fact that many States have different laws for these settings and are separate from school systems. Two commenters suggested defining schools as being open to children up to age 18, since students become adults at age 18 and can authorize the disclosure of their own information. A few commenters suggested that the definition include all schools that require immunization documentation as a prerequisite to enrollment, not just those that are subject to State entry laws, in order to protect public health in all school settings, since the threat of un-immunized children exists regardless of State school entry laws. Additionally, some commenters recommended that the term ''school'' not be defined in the Privacy Rule due to the variation across States in the types of schools that are subject to the entry laws.

Final Rule

The final rule adopts the proposal to amend § 164.512(b)(1) by adding a new paragraph that permits a covered entity to disclose proof of immunization to a school where State or other law requires the school to have such information prior to admitting the student. While written authorization will no longer be required to permit this disclosure, covered entities will still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting *in loco parentis* for the individual, or from the individual himself or herself, if the individual is an adult or emancipated minor. We believe that the option to provide oral agreement for the disclosure of student immunization records will relieve burden on parents, schools, and covered entities, and greatly facilitate the role that schools play in public health, while still giving parents the opportunity to consider whether to agree to the disclosure of this information.

The final rule additionally requires that covered entities document the agreement obtained under this provision. The final rule does not prescribe the nature of the documentation and does not require signature by the parent, allowing covered entities the flexibility to determine what is appropriate for their purposes. The documentation must only make clear that agreement was obtained as permitted under this provision. For example, if a parent or guardian submits a written or email request to a covered entity to disclose his or her child's immunization records to the child's school, a copy of the request would suffice as documentation of the agreement. Likewise, if a parent or guardian calls the covered entity and requests over the phone that his or her child's immunization records be disclosed to the child's school, a notation in the child's medical record or elsewhere of the phone call would suffice as documentation of the agreement. We emphasize that the agreement is not equivalent to a HIPAA-compliant authorization, and covered entities are not required to document a signature as part of this requirement. We disagree with comments that documentation would be as burdensome on covered entities as written authorization, since an authorization form contains many required statements and elements, including a signature by the appropriate individual, which are not required for the agreement and documentation contemplated here. Furthermore, we believe that documentation of oral agreements will help to prevent miscommunications and potential future objections by parents or individuals, and the concerns that covered entities may have regarding liability, penalty or other enforcement actions for disclosures made pursuant to an oral agreement.

Several commenters recommended that in lieu of an oral agreement, disclosure of immunization records to schools are presumed to be permitted, while giving individuals the option to opt out of this presumption or request a restriction to the disclosure. One commenter advocated for this public health exemption for disclosure of immunization records as being particularly critical for children who may be, for example, homeless, living with someone other than a parent or legal guardian, or living with a parent that does not speak English. We remove the written authorization requirement to help facilitate these disclosures with as much flexibility as possible. However, we do not intend this provision to change the current practice of parents, guardians, or other persons acting *in loco parentis* contacting a child's health care provider to request proof of immunization be sent to the child's school. Therefore, we still require active agreement from the appropriate individual, and a health care provider may not disclose immunization records to a school under this provision without such agreement. The agreement must be an affirmative assent or request by a parent, guardian, or other person acting *in loco parentis* (or by an adult individual or emancipated minor, if applicable) to the covered entity, which may be oral and over the phone, to allow the disclosure of the immunization records. A mere request by a school to a health care provider for the immunization records of a student would not be sufficient to permit disclosure under this provision (and

such a request by a school might also raise implications under other laws, such as FERPA).

We decline to include definitions of ''school official'' and ''school'' in the final rule. The motivation for this new permissive disclosure is to promote public health by reducing the burden associated with providing schools with student immunization records and we do not wish to create additional difficulties or confusion in doing so. We therefore agree with commenters that schools are best equipped to determine the appropriate individual to receive student immunization records at their location and will benefit from having this flexibility. We also agree with commenters that ''school'' should remain undefined in the Privacy Rule due to the variation across States in the types of schools that are subject to the entry laws. We believe that this will best align with State law and cause the least amount of confusion. We did not receive sufficient comment regarding the breadth of schools that are not subject to school entry laws or the burden that these institutions face to justify expanding this provision to allow disclosure of proof of immunization to such schools without an authorization.

Response to Other Public Comments

Comment: Several commenters raised concerns about the dynamic between the Privacy Rule requirements and State law requirements regarding immunization disclosures. Commenters indicated that some State laws require providers to directly share immunization records with schools and provide parents with the opportunity to opt out of this direct sharing. Commenters also indicated the use of State immunization registries in many States, to which schools are permitted direct access. One commenter suggested that the Privacy Rule permit State law to determine what is the minimum necessary for proof of immunization.

Response: We take this opportunity to clarify that the Privacy Rule at § 164.512(a) permits a covered entity to use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law. As such, the Privacy Rule does not prohibit immunization disclosures that are mandated by State law, nor does it require authorization for such disclosures. With regard to State laws that require covered entities to disclose immunization records to schools and allow parents to opt out, this is not in any way prohibited by the Privacy Rule. However, with regard to State laws that permit but do not require covered entities to disclose immunization records to schools, this does not meet the requirements of the provisions at § 164.512(a), and disclosures of immunization records are subject to the Privacy Rule agreement and documentation requirements described in this part. We also note that the Privacy Rule at § 164.512(b) permits a covered entity to disclose protected health information for public health activities. Disclosures of protected health information to State immunization registries are therefore permitted by the Privacy Rule and also do not require authorization. The Privacy Rule at § 164.514(d)(3)(iii)(A) provides that a covered entity, when making a permitted disclosure pursuant to § 164.512 to a public official, may determine, if such a determination is reasonable under the circumstances, that information requested by a public official is the minimum necessary information for the stated purpose, if the public official represents that the information requested is the minimum necessary for the stated purpose(s). Under this provision, a covered entity may rely on State law or a State official's determination of the minimum necessary information required for proof of immunization, unless such determination is unreasonable.

Comment: Commenters requested guidance on when and how often to obtain agreement for immunization disclosures.

Response: We anticipate that covered entities will obtain agreement for the disclosure of immunization records on a case-by-case basis as needed. For example, a parent may call and request that a covered entity provide his or her child's immunization records before the child begins elementary school, if required by State school entry laws. If that child moves to a different school and is unable to transfer their immunization records to the new school, the parent may need to request that the covered entity provide his or her child's immunization records to the new school, if required by State school entry laws. A parent might also generally indicate to a covered entity that he or she affirmatively agrees to the immediate or future disclosure of his or her child's immunization records to the child's school as necessary, or the continued disclosure of such information if, for example, updates are required by the school when a series of vaccinations have been completed.

Comment: Commenters requested clarification on the length of time an agreement may be relied upon.

Response: An agreement to permit the disclosure of immunization records is considered effective until revoked by the parent, guardian or other person acting *in loco parentis* for the individual, or by the individual himself or herself, if the individual is an adult or emancipated minor.

Comment: Commenters requested clarification regarding any requirement for schools to maintain the immunization records.

Response: The Privacy Rule does not require schools to keep student immunization records; however individual State or other laws may require this.

7. Section 164.514(f)—Fundraising

Proposed Rule

Section 164.514(f)(1) of the Privacy Rule permits a covered entity to use, or disclose to a business associate or an institutionally related foundation, the following protected health information about an individual for the covered entity's fundraising from that individual without the individual's authorization: (1) Demographic information relating to an individual; and (2) the dates of health care provided to an individual. Section 164.514(f)(2) of the Privacy Rule requires a covered entity that plans to use or disclose protected health information for fundraising under this paragraph to inform individuals in its notice of privacy practices that it may contact them to raise funds for the covered entity. In addition, § 164.514(f)(2) requires that a covered entity include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving future fundraising communications and that a covered entity must make reasonable efforts to ensure that individuals who do opt out are not sent future fundraising communications.

Section 13406(b) of the HITECH Act requires the Secretary to provide by rule that a covered entity provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications. Additionally, section 13406(b) states that if an individual does opt out of receiving further fundraising communications, the individual's choice to opt out must be treated as a revocation of authorization under § 164.508 of the Privacy Rule.

In the NPRM, we proposed a number of changes to the Privacy Rule's fundraising requirements to implement the statutory provisions. First, we proposed to strengthen the opt out by

requiring that a covered entity provide, with each fundraising communication sent to an individual under these provisions, a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications. To satisfy this requirement, we also proposed to require that the method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than nominal cost. We encouraged covered entities to consider the use of a toll-free phone number, an email address, or similar opt out mechanism that would provide individuals with a simple, quick, and inexpensive way to opt out of receiving future communications. We noted that we considered requiring individuals to write a letter to opt out to constitute an undue burden on the individual.

We also proposed to provide that a covered entity may not condition treatment or payment on an individual's choice with respect to receiving fundraising communications. We believed this modification would implement the language in section 13406(b) of the HITECH Act that provides that an election by an individual not to receive further fundraising communications shall be treated as a revocation of authorization under the Privacy Rule.

Further, we proposed to provide that a covered entity may not send fundraising communications to an individual who has elected not to receive such communications. This would strengthen the current requirement at § 164.514(f)(2)(iii) that a covered entity make ''reasonable efforts'' to ensure that those individuals who have opted out of receiving fundraising communications are not sent such communications. The NPRM proposed stronger language to make clear the expectation that covered entities abide by an individual's decision not to receive fundraising communications, as well as to make the fundraising opt out operate more like a revocation of authorization, consistent with the statutory language and legislative history of section 13406(b) of the HITECH Act discussed above.

With respect to the operation of the opt out, we requested comment regarding to what fundraising communications the opt out should apply (i.e., should the opt out apply to all future fundraising communications or should and can the opt out be structured in a way to apply only to the particular fundraising campaign described in the letter). We also requested comment on whether the Rule should allow a similar method, short of the individual signing an authorization, by which an individual who has previously opted out can put his or her name back on an institution's fundraising list.

We proposed to retain the requirement that a covered entity that intends to contact the individual to raise funds under these provisions include a statement to that effect in its notice of privacy practices. However, we proposed that the required statement also inform individuals that they have a right to opt out of receiving such communications.

In addition to the above modifications, we requested public comment on the requirement at § 164.514(f)(1) which limits the information a covered entity may use or disclose for fundraising to demographic information about and dates of health care service provided to an individual. Since the promulgation of the Privacy Rule, we acknowledged that certain covered entities have raised concerns regarding this limitation, maintaining that the Privacy Rule's prohibition on the use or disclosure of certain treatment information without an authorization, such as the department of service where care was received and outcomes information, impedes their ability to raise funds from often willing and grateful patients because they are unable to target their fundraising efforts and avoid inappropriate solicitations to individuals who may have had a bad treatment outcome. Such entities have argued that obtaining an individual's authorization for fundraising as the individual enters or leaves the hospital for treatment is often impracticable or inappropriate. The proposed rule also discussed the fact that the National Committee on Vital and Health Statistics held a hearing and heard public testimony on this issue in July 2004 and recommended to the Secretary that the Privacy Rule should allow covered entities to use or disclose information related to the patient's department of service (broad designations, such as surgery or oncology, but not narrower designations or information relating to diagnosis or treating physician) for fundraising activities without patient authorization. The National Committee on Vital and Health Statistics also recommended that a covered entity's notice of privacy practices inform patients that their department of service information may be used in fundraising, and that patients should be afforded the opportunity to opt out of the use of their department of service information for fundraising or all fundraising contacts altogether. See *http://www.ncvhs.hhs.gov/040902lt1.htm*.

In light of these concerns and the prior recommendation of the National Committee on Vital and Health Statistics, we asked for public comment on whether and how the current restriction on what information may be used and disclosed should be modified to allow covered entities to more effectively target fundraising and avoid inappropriate solicitations to individuals, as well as to reduce the need to send solicitations to all patients. In particular, we solicited comment on: (1) Whether the Privacy Rule should allow additional categories of protected health information to be used or disclosed for fundraising, such as department of service or similar information, and if so, what those categories should be; (2) the adequacy of the minimum necessary standard to appropriately limit the amount of protected health information that may be used or disclosed for fundraising purposes; or (3) whether the current limitation should remain unchanged. We also solicited comment on whether, if additional information is permitted to be used or disclosed for fundraising absent an authorization, covered entities should be required to provide individuals with an opportunity to opt out of receiving any fundraising communications before making the first fundraising solicitation, in addition to the opportunity to opt out with every subsequent communication. We invited public comment on whether such a pre-solicitation opt out would be workable for covered entities and individuals and what mechanisms could be put into place to implement the requirement.

Overview of Public Comments

In general, the public comments received in response to the NPRM were supportive of the proposed modifications but many asked that the final rule give covered entities flexibility with respect to operationalizing these requirements. Several commenters provided examples of routine communications and expressed the need for guidance and clarification about what constitutes a fundraising communication.

Generally, most commenters supported the NPRM's proposed requirement that the method through which the covered entity permits individuals to opt out of receiving future fundraising communications not cause individuals to incur an undue burden or more than a nominal cost. Many commenters stated that the final rule should give covered entities the flexibility to determine which opt out

methods will work best given their circumstances, instead of requiring all covered entities to employ specific opt out methods. These commenters noted that depending on the size of the covered entity and type of population it serves, certain opt out methods might not be feasible, such as one that requires the establishment of a toll-free number, which may be cost prohibitive for some small entities. Similarly, some commenters noted that because not all individuals have access to a computer and the Internet, providing individuals with the opportunity to opt out via email alone may not be sufficient.

With respect to the scope of the opt out, the commenters were generally split on whether the opt out should apply to communications related to a specific fundraising campaign or to all future fundraising communications. The commenters in support of applying the opt out to a specific fundraising campaign stated that it would be too difficult for individuals to make a meaningful decision about whether they wanted to opt out of all future fundraising communications, and allowing individuals to opt out of all futurefundraising communications would greatly hinder a covered entity's ability to raise funds. Those commenters in favor of implementing an all or nothing opt out stated that it would be too difficult for covered entities, especially large facilities, to track campaign-specific opt outs for each individual, so applying the opt out universally would make it much easier for covered entities to implement. Other commenters asked that the final rule take a flexible approach and permit covered entities to decide the scope of the opt out, while others stated that the final rule should require covered entities to include both opt out options on each fundraising communication leaving the decision to individuals.

Additionally, while most commenters supported the prohibition on conditioning treatment or payment on an individual's choice regarding the receipt of fundraising communications, most commenters opposed the NPRM's proposal that prohibited covered entities from sending future fundraising communications to those individuals who had opted out and stated that it was too strict. The majority of these commenters suggested that the final rule retain the Privacy Rule's original ''reasonable efforts'' language and stated that while covered entities have every incentive not to send fundraising communications to those individuals who have opted out of receiving them, it is very difficult for covered entities to ensure 100 percent accuracy with this policy. Several commenters stated that there are lag times between the period of time in which a fundraising mailing list is compiled and the time in which a fundraising communication is sent out, so if an individual has opted out during the interim time period, covered entities may not be able to prevent the prepared fundraising communication from being sent. Other commenters stated that it may be difficult to implement an opt out across all records belonging to that individual where complications, such as name changes and variation, address changes, and multiple addresses are involved.

For those individuals who have opted out of receiving fundraising communications, commenters generally supported allowing those individuals to opt back in to receiving such communications. Some suggested that individuals be able to opt back in using the same methods they used to opt out, while others suggested that any communication indicating a willingness to resume receiving fundraising communications, such as making a donation to the covered entity, should function as an opt in. Other commenters suggested that the final rule limit the amount of time that an individual can opt out, such that after this period of time the individual automatically begins receiving fundraising communications again. A few commenters were opposed to permitting individuals to opt back in to receive fundraising communications, stating that this would be too costly and burdensome for covered entities to track.

With respect to the requests for public comments regarding the potential use or disclosure of additional protected health information to provide more targeted fundraising communications, the vast majority of commenters supported allowing the use or disclosure of additional protected health information for fundraising. These commenters stated that the use of additional protected health information would streamline their fundraising efforts and ensure that individuals were sent communications about campaigns that would be meaningful to their experiences. These commenters also stated that it would eliminate the concern of sending a communication to an individual or family that suffered a negative outcome. Commenters suggested several categories of protected health information that covered entities should be able to use to target their fundraising efforts, including department or site of service, generic area of treatment, department where last seen, outcome information, treating physician, diagnosis, whether the individual was a pediatric or adult patient, medical record number, Social Security number, or other unique identifier, and any other information that reflects the fact that the individual was served by the covered entity.

With respect to the minimum necessary standard, a few commenters supported its use to limit any additional categories of protected health information that can be used to target a covered entity's fundraising efforts. These commenters supported the use of the standard because of how familiar and comfortable most covered entities are at applying the minimum necessary standard. However, another commenter was opposed to the use of the minimum necessary standard, stating that it is not uniformly applied across covered entities.

Despite the general support for the use of additional protected health information, a small minority of commenters opposed allowing the use of additional protected health information to target fundraising efforts, citing privacy concerns with doing so. One commenter opposed expanding the information that could be used for fundraising in cases where outside fundraising entities are used, including those with whom the covered entity has executed business associate agreements.

All commenters were opposed to requiring covered entities to provide a pre-solicitation opt out to individuals and stated that permitting individuals to opt out in the first fundraising communication is sufficient. Several commenters noted that the proposed revision to the notice of privacy practices to require a covered entity to inform individuals of their right to opt out of receiving fundraising communications effectively functions as a pre-solicitation opt out, so individuals who wish to opt out of receiving such communications immediately can do so upon receipt of the notice.

Final Rule

We generally adopt the proposals in the final rule, as well as allow certain additional types of protected health information to be used or disclosed for fundraising purposes.

With respect to the commenters who expressed confusion over what constitutes a fundraising communication, we emphasize that the final rule does nothing to modify the types of communications that are currently considered to be for fundraising purposes. A communication to an individual that is made by a covered entity, an institutionally related foundation, or a business associate on behalf of the covered entity for the

purpose of raising funds for the covered entity is a fundraising communication for purposes of § 164.514(f). The Department has stated that ''[p]ermissible fundraising activities include appeals for money, sponsorship of events, etc. They do not include royalties or remittances for the sale of products of third parties (except auctions, rummage sales, etc.).'' See 65 FR 82718. Additionally, the Privacy Rule has always required that such communications contain a description of how the individual may opt out of receiving further fundraising communications (§ 164.514(f)(2)(ii)).

With respect to the proposed requirement that the method for an individual to elect not to receive further fundraising communications should not cause the individual to incur an undue burden or more than a nominal cost, we generally agree with the commenters who suggested that the final rule be flexible and not prescriptive. Under the final rule, covered entities are free to decide what methods individuals can use to opt out of receiving further fundraising communications, as long as the chosen methods do not impose an undue burden or more than a nominal cost on individuals. Covered entities should consider the use of a toll-free phone number, an email address, or similar opt out mechanisms that provide individuals with simple, quick, and inexpensive ways to opt out of receiving further fundraising communications. Covered entities may employ multiple opt out methods, allowing individuals to determine which opt out method is the simplest and most convenient for them, or a single method that is reasonably accessible to all individuals wishing to opt out.

In response to commenters who expressed concern about the cost of setting up a toll-free phone number, we clarify that covered entities may require individuals who wish to opt out of further fundraising communications to do so through other methods, (e.g., through the use of a local phone number), where appropriate, as long as the method or methods adopted do not impose an undue burden or cost on the individual. We encourage covered entities to consider the size of the population to which they are sending the communications, the geographic distribution, and any other factors that may help determine which opt out method(s) is most appropriate and least burdensome to individuals.

We continue to consider requiring individuals to write and send a letter to the covered entity asking not to receive further fundraising communications to constitute an undue burden. However, requiring that individuals opt out of further fundraising communications by simply mailing a pre-printed, pre-paid postcard would not constitute an undue burden under the final rule and is an appropriate alternative to the use of a phone number or email address.

Regarding the scope of the opt out, the commenters were split on whether the opt out should apply to all future fundraising communications or to a specific fundraising campaign. The final rule leaves the scope of the opt out to the discretion of covered entities. For those covered entities that expressed concern about the ability to track campaign-specific opt outs, they have the discretion to apply the opt out to all future fundraising communications. Likewise, those covered entities that prefer, and have the ability to track, campaign-specific opt outs are free to apply the opt out to specific fundraising campaigns only. Covered entities are also free to provide individuals with the choice of opting out of all future fundraising communications or just campaign-specific communications. Whatever method is employed, the communication should clearly inform individuals of their options and any consequences of electing to opt out of further fundraising communications.

Despite the commenters who did not support the strengthened language in the NPRM prohibiting covered entities from sending further fundraising communications to those individuals who have already opted out, the final rule adopts this provision without modification. While many commenters supported the current ''reasonable efforts'' standard and cited several reasons that may make it difficult to attain the proposed standard, we adopt the proposed standard because it is consistent with the statute and more protective of an individual's right to elect not to receive further fundraising communications. For example, some commenters cited lag times between the creation of mailing lists and the receipt or update of opt out lists and difficulty in accurately identifying individuals on the fundraising lists due to name changes or variations and multiple addresses. These issues are common to the management of the medical or billing records and effectuating revocations of authorization, requests for access, and other general communications between the entity and the individual. We expect the same care and attention to the handling of protected health information in fundraising communications as is necessary for the proper handling of this information in all other health care operations performed by the covered entity. Covered entities voluntarily choosing to send fundraising communications to individuals must have data management systems and processes in place to timely track and flag those individuals who have opted out of receiving fundraising communications to ensure that they are not sent additional fundraising communications.

The majority of commenters supported allowing a process for individuals who have opted out of receiving further fundraising communications to opt back in and the final rule at § 164.514(f)(2)(v) permits covered entities have one. Like the discretion given to covered entities regarding the methods through which an individual can opt out, the final rule gives covered entities the discretion to determine how individuals should be able to opt back in. For example, a covered entity could include as a part of a routine newsletter sent to all patients a phone number individuals can call to be put on a fundraising list.

While some commenters suggested that opt outs should be time limited such that an individual automatically opts back in after a certain period of time, we do not believe that an individual's election not to receive further fundraising communications is something that should automatically lapse. Because the individual has actively chosen to opt out, only a similar active decision by the individual to opt back in will suffice. Additionally, where an individual who has opted out of fundraising communications makes a donation to a covered entity, it does not serve, absent a separate election to opt back in, to automatically add the individual back onto the mailing list for fundraising communications.

The Privacy Rule currently permits covered entities to use or disclose only demographic information relating to the individual and dates of health care provided to the individual for fundraising communications. In response to several commenters who asked for clarification regarding the scope of demographic information, the final rule, at § 164.514(f)(1)(i), clarifies that demographic information relating to an individual includes names, addresses, other contact information, age, gender, and dates of birth. Although much of this information was listed in the preamble to the 2000 final rule (65 FR 82718) as being demographic information with respect to the fundraising provisions, we have added this information to the regulatory text for clarity. Additionally, we have included date of birth as demographic information, instead of merely age. We

believe that date of birth may be useful to covered entities because they are more likely to maintain a record of an individual's date of birth, rather than his or her static age. We also note that the 2000 preamble identifies insurance status as falling within the category of demographic information. The final rule continues to allow covered entities to use or disclose information about an individual's health insurance status for fundraising purposes; however, we list this category of information separately in the regulatory text, as we do not believe this information truly constitutes demographic information.

In addition to demographic information, health insurance status, and dates of health care provided to the individual (which is currently permitted under the Rule), this final rule also allows covered entities to use and disclose department of service information, treating physician information, and outcome information for fundraising purposes. These three categories of information were most frequently identified by commenters as the most needed for covered entities to further target fundraising communications to appropriate individuals. Although we do not define these terms, we clarify that department of service information includes information about the general department of treatment, such as cardiology, oncology, or pediatrics. Additionally, we clarify that outcome information includes information regarding the death of the patient or any sub-optimal result of treatment or services. In permitting its use for fundraising purposes, we intend for it to be used by the covered entity itself to screen and eliminate from fundraising solicitations those individuals experiencing a sub-optimum outcome, and for its disclosure to a business associate or institutionally related foundation only where such screening function is done by those parties. We also emphasize that as with any use or disclosure under the Privacy Rule, a covered entity must apply the minimum necessary standard at § 164.502(b) to ensure that only the minimum amount of protected health information necessary to accomplish the intended purpose is used or disclosed.

We adopt in the final rule the provision prohibiting the conditioning of treatment or payment on an individual's choice with respect to the receipt of fundraising communications. We also adopt at § 164.520(b)(1)(iii)(A) the requirement that the notice of privacy practices inform individuals that a covered entity may contact them to raise funds for the covered entity and an individual has a right to opt out of receiving such communications. The final rule does not require covered entities to send pre-solicitation opt outs to individuals prior to the first fundraising communication. We believe that because the individual will be on notice of the opportunity to opt out of receiving fundraising communications through the notice of privacy practices and the first fundraising communication itself will contain a clear and conspicuous opportunity to opt out, there is no need to require covered entities to incur the additional burden and cost of sending pre-solicitation opt outs.

Under the Privacy Rule fundraising communications can take many forms, including communications made over the phone. Despite the fact that the HITECH Act refers only to written fundraising communications, because the Privacy Rule applies to communications made over the phone, we believe it would be counterintuitive to apply the strengthened opt out requirement to only written fundraising communications. Therefore, like fundraising communications made in writing, covered entities that make fundraising communications over the phone must clearly inform individuals that they have a right to opt out of further solicitations. Accordingly, to make clear that the opt out requirement applies to fundraising solicitations made over the phone, the final rule provides that the opt out requirement applies to each fundraising communication ''made'' rather than ''sent'' to an individual.

We also emphasize that the notice and opt out requirements for fundraising communications apply only where the covered entity is using or disclosing protected health information to target the fundraising communication. If the covered entity does not use protected health information to send fundraising materials, then the notice and opt out requirements do not apply. For example, if a covered entity uses a public directory to mail fundraising communications to all residents in a particular geographic service area, the notice and opt out requirements are not applicable.

Response to Other Public Comments

Comment: A few commenters suggested that, to better protect an individual's privacy, particularly where sensitive health information may be used to target solicitations, the final rule should require an opt in process rather than an opt out process for consenting to fundraising communications.

Response: We decline to require an opt in process. The HITECH Act did not replace the right to opt out of fundraising communications with an opt in process. Further, we continue to believe that the opt out process, particularly as it has been strengthened by the HITECH Act and this final rule, provides individuals with appropriate control over the use of their information for these purposes.

Comment: One commenter asked that if an individual opts out of receiving further fundraising communications through a mailed communication, must the covered entity also remove the individual's name from the list through which the covered entity sends email fundraising communications, or must the individual opt out of receiving such email communications separately.

Response: A covered entity may choose to provide individuals with the opportunity to select their preferred method for receiving fundraising communications. If an individual elects to opt out of future fundraising communications, then the opt out is effective for all forms of fundraising communications. Thus, the individual must be removed from all such lists.

8. Section 164.520—Notice of Privacy Practices for Protected Health Information

Proposed Rule

Section 164.520 of the Privacy Rule sets out the requirements for most covered entities to have and distribute a notice of privacy practices (NPP). The NPP must describe the uses and disclosures of protected health information a covered entity is permitted to make, the covered entity's legal duties and privacy practices with respect to protected health information, and the individual's rights concerning protected health information.

Section 164.520(b)(1)(ii) requires a covered entity to include separate statements about permitted uses and disclosures that the covered entity intends to make, including uses and disclosures for certain treatment, payment, or health care operations purposes. Further, § 164.520(b)(1)(ii)(E) currently requires that the NPP contain a statement that any uses and disclosures other than those permitted by the Privacy Rule will be made only with the written authorization of the individual, and that the individual has the right to revoke an authorization pursuant to § 164.508(b)(5).

We proposed to amend § 164.520(b)(1)(ii)(E) to require that the NPP describe the uses and disclosures of protected health information that

require an authorization under § 164.508(a)(2) through (a)(4) (i.e., including a statement that most uses and disclosures of psychotherapy notes and of protected health information for marketing purposes and the sale of protected health information require an authorization), and provide that other uses and disclosures not described in the notice will be made only with the individual's authorization.

Section 164.520(b)(1)(iii) requires a covered entity to include in its NPP separate statements about certain activities if the covered entity intends to engage in any of the activities. In particular, § 164.520(b)(1)(iii) requires a separate statement in the notice if the covered entity intends to contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits or services; to contact the individual to fundraise for the covered entity; or, with respect to a group health plan, to disclose protected health information to the plan sponsor.

First, with respect to this provision, the NPRM proposed to modify § 164.520(b)(1)(iii)(A) to align the required statement with the proposed modifications related to marketing and subsidized treatment communications. The provision would have required a covered health care provider that intends to send treatment communications to individuals and has received financial remuneration in exchange for making the communication to, in its NPP, notify individuals of this intention and to inform them that they can opt out of receiving such communications. Second, at § 164.520(b)(1)(iii)(B) we proposed to require that if a covered entity intends to contact the individual to raise funds for the entity as permitted under § 164.514(f)(1), the covered entity must not only inform the individual in the NPP of this intention but also must inform the individual that he or she has the right to opt out of receiving such communications.

Section 164.520(b)(1)(iv) requires that the NPP contain statements regarding the rights of individuals with respect to their protected health information and a brief description of how individuals may exercise such rights. Section 164.520(b)(1)(iv)(A) currently requires a statement and a brief description addressing an individual's right to request restrictions on the uses and disclosures of protected health information pursuant to § 164.522(a), including the fact that the covered entity is not required to agree to this request.

The NPRM proposed to modify § 164.520(b)(1)(iv)(A) to require a statement explaining that the covered entity is required to agree to a request to restrict disclosure of protected health information to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full, as provided at § 164.522(a)(1)(vi).

Under Subpart D of Part 164, covered entities now have new breach notification obligations. We requested comment on whether the Privacy Rule should require a specific statement regarding this new legal duty and what particular aspects of this new duty would be important for individuals to be notified of in the NPP.

The NPRM stated that modifications to § 164.520 would represent material changes to covered entities' NPPs. Section 164.520(b)(3) requires that when there is a material change to the NPP, covered entities must promptly revise and distribute the NPP as outlined at § 164.520(c). Section 164.520(c)(1)(i)(C) requires that health plans provide notice to individuals covered by the plan within 60 days of any material revision to the NPP. Because we acknowledged that revising and redistributing a NPP may be costly for health plans, we requested comment on ways to inform individuals of this change to privacy practices without unduly burdening health plans. We requested comment on options for informing individuals in a timely manner of this proposed or other material changes to the NPP. We also requested comment on this issue in the proposed changes to the Privacy Rule pursuant to the Genetic Information Nondiscrimination Act (GINA), as discussed below in Section VI. In particular, the Department requested comment on the following options: (1) Replace the 60-day requirement with a requirement for health plans to revise their NPPs and redistribute them (or at least notify members of the material change to the NPP and how to obtain the revised NPP) in their next annual mailing to members after a material revision to the NPP, such as at the beginning of the plan year or during the open enrollment period; (2) provide a specified delay or extension of the 60-day timeframe for health plans (3) retain the provision generally to require health plans to provide notice within 60 days of a material revision but provide that the Secretary will waive the 60-day timeframe in cases where the timing or substance of modifications to the Privacy Rule call for such a waiver; or (4) make no change and thus, require that health plans that perform underwriting provide notice to individuals within 60 days of the material change to the NPP that would be required by this proposed rule. The Department requested comment on these options, as well as any other options for informing individuals in a timely manner of material changes to the NPP.

Section 164.520(c)(2)(iv) requires that when a health care provider with a direct treatment relationship with an individual revises the NPP, the health care provider must make the NPP available upon request on or after the effective date of the revision and must comply with the requirements of § 164.520(c)(2)(iii) to have the NPP available at the delivery site and to post the notice in a clear and prominent location. We did not propose changes to these provisions because we did not believe these requirements to be overly burdensome but we requested comment on the issue.

Overview of Public Comments

We received several comments expressing support for the proposed requirement that the NPP include a statement about the uses and disclosures that require authorization. However, other commenters opposed this requirement, arguing that because not all uses and disclosures will apply to every individual, the statement will cause confusion and unnecessary concern. Additionally, these commenters argued that the cost of listing all of the situations requiring authorization would be significant.

We received several comments in support of the proposed requirement that the NPP include a specific statement about authorization for uses and disclosures of psychotherapy notes. Some of these commenters requested that the final rule require covered providers to describe in their NPPs their recordkeeping practices with regard to psychotherapy notes and how those practices affect what information can be used and disclosed. Several commenters argued that only covered entities that record psychotherapy notes should be required to include a statement about the authorization requirement for psychotherapy notes in their NPPs.

We also received several comments expressing concern regarding the proposed requirement to include information in the NPP about the individual's right to opt out of receiving certain communications. These commenters argued that information notifying individuals that they could opt out of receiving further subsidized treatment or fundraising communications would provide little

value to individuals at a significant cost to covered entities. These commenters felt that including this information would be unnecessary because all subsidized treatment and fundraising communications themselves will include an opt-out mechanism, and as such, including the information in the NPP may cause unnecessary concern for consumers.

We received one comment in support of the requirement to include in the NPP a statement about an individual's right to restrict certain uses and disclosures of protected health information if the individual pays for treatment or services out-of-pocket in full. We also received one comment suggesting that only health care providers should be required to include such a statement in their NPP.

We received a number of comments supporting a requirement to include a statement in the NPP about the right to be notified following a breach of unsecured protected health information. One commenter suggested that explaining breach notification requirements in the NPP would help entities handle customer service issues that arise when customers become upset upon receipt of such a breach notification. However, a number of other commenters expressed opposition to this proposal due to concern that such a statement would cause unnecessary concern and fear among individuals who may believe that covered entities cannot appropriately secure their protected health information. Finally, we received one comment requesting that HHS specify the required elements of a breach notification statement for a NPP.

We also received several comments arguing that the proposed changes should not constitute material changes to privacy practices requiring a new NPP, particularly where covered entities have already revised their NPPs to comply with the HITECH Act or State law requirements. Two additional commenters argued that each covered entity should determine whether a change is material or not, depending on its existing privacy practices.

We received a number of comments regarding the appropriate timing and manner for distributing new NPPs. The majority of the comments received generally fell into three categories: (1) Support for a requirement to revise and distribute notices within 60 days of a material change; (2) a recommendation for HHS to require that covered entities promptly post a revised NPP on their Web site in conjunction with a requirement to send a notice of the change by mail within a specified period; and (3) a request for HHS to extend the compliance deadline and permit the distribution of the revised NPP through a quarterly newsletter, annual mailing, after 18 months of transition, or in a triennial mailing. In addition, many commenters supported electronic distribution of an NPP or a notice of material changes to the NPP.

While not proposed, some commenters suggested eliminating or alternatives to the current requirements for health care providers with direct treatment relationships to hand the NPP to every individual patient and make a good faith attempt to obtain acknowledgement of receipt.

A few commenters also expressed concern regarding the cost burden associated with revising and distributing a new NPP. One commenter argued that considerations of cost do not justify a delay in distributing a revised NPP.

Final Rule

First, the final rule adopts the modification to § 164.520(b)(1)(ii)(E), which requires certain statements in the NPP regarding uses and disclosures that require authorization. We note that, contrary to some commenter concerns, the final rule does not require the NPP to include a list of all situations requiring authorization. Instead, the NPP must contain a statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of protected health information for marketing purposes, and disclosures that constitute a sale of protected health information require authorization, as well as a statement that other uses and disclosures not described in the NPP will be made only with authorization from the individual.

The final rule does not require the NPP to include a description of a covered entity's recordkeeping practices with respect to psychotherapy notes; however, covered entities are free to include such additional information in their NPP if they choose. Additionally, in response to requests by some commenters, we clarify that covered entities that do not record or maintain psychotherapy notes are not required to include a statement in their NPPs about the authorization requirement for uses and disclosures of psychotherapy notes.

Second, because the final rule treats all subsidized treatment communications as marketing communications, we have not adopted the proposal to require a statement in the NPP about such communications and the ability of an individual to opt out. For further discussion on the decision to treat all subsidized treatment communications as marketing communications requiring an authorization, please see the above discussion regarding § 164.501.

The final rule, however, adopts the proposed requirement for a statement in the NPP regarding fundraising communications and an individual's right to opt out of receiving such communications, if a covered entity intends to contact an individual to raise funds for the covered entity. Because individuals will be provided the opportunity to opt out of fundraising communications with each solicitation, the final rule does not require the NPP to include the mechanism for individuals to opt out of receiving fundraising communications, although covered entities are free to include such information if they choose to do so.

The final rule also adopts the proposal that the NPP inform individuals of their new right to restrict certain disclosures of protected health information to a health plan where the individual pays out of pocket in full for the health care item or service. Only health care providers are required to include such a statement in the NPP; other covered entities may retain the existing language indicating that a covered entity is not required to agree to a requested restriction.

The final rule also requires covered entities to include in their NPP a statement of the right of affected individuals to be notified following a breach of unsecured protected health information. We believe that individuals should be informed of their right to receive and the obligations of covered entities to provide notification following a breach. We disagree with the commenters who argued that such a statement would cause individuals unnecessary concern and would create unfounded fear that covered entities cannot appropriately secure protected health information. Such advance notice of their rights should provide helpful context for individuals should they later receive a breach notification. In response to comments, we also clarify that a simple statement in the NPP that an individual has a right to or will receive notifications of breaches of his or her unsecured protected health information will suffice for purposes of this requirement. We do not intend for this requirement to add undue complexity or length to a covered entity's NPP. Thus, the statement need not be entity-specific, such as by describing how the covered entity will conduct a risk assessment, include the regulatory descriptions of ''breach'' or ''unsecured PHI,'' or describe the types

of information to be provided in the actual breach notification to the individual. However, covered entities that wish to include additional or more detailed information may do so.

These changes represent material changes to the NPP of covered entities. We disagree with the few commenters who argued that such modifications to § 164.520 do not constitute material changes of privacy practices requiring the distribution of new NPPs. The modifications to § 164.520 are significant and are important to ensure that individuals are aware of the HITECH Act changes that affect privacy protections and individual rights regarding protected health information.

Section 164.520(c)(1) of the final rule requires a health plan that currently posts its NPP on its Web site in accordance with § 164.520(c)(3)(i) to: (1) Prominently post the material change or its revised notice on its web site by the effective date of the material change to the notice (e.g., the compliance date of this final rule) and (2) provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan, such as at the beginning of the plan year or during the open enrollment period. Health plans that do not have customer service web sites are required to provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the material revision to the notice. These requirements apply to all material changes including, where applicable, the rule change adopted pursuant to GINA to prohibit most health plans from using or disclosing genetic information for underwriting purposes.

We believe these distribution requirements best balance the right of individuals to be informed of their privacy rights with the burden on health plans to provide the revised NPP. We also note that health plans should provide both paper- and web-based notices in a way accessible to all beneficiaries, including those individuals with disabilities. These modifications provide an avenue for an individual to be informed of material changes upon their effective date while better aligning the NPP distribution with health plans' normal mailings to individuals.

For health care providers, the final rule does not modify the current requirements to distribute revisions to the NPP. As such, § 164.520(c)(2)(iv) requires that when a health care provider with a direct treatment relationship with an individual revises the NPP, the health care provider must make the NPP available upon request on or after the effective date of the revision and must comply with the requirements of § 164.520(c)(2)(iii) to have the NPP available at the delivery site and to post the notice in a clear and prominent location. In response to several comments expressing concern about printing costs for new NPPs, we clarify that providers are not required to print and hand out a revised NPP to all individuals seeking treatment; providers must post the revised NPP in a clear and prominent location and have copies of the NPP at the delivery site for individuals to request to take with them. Providers are only required to give a copy of the NPP to, and obtain a good faith acknowledgment of receipt from, new patients. As a result, we do not believe that the current requirement is overly burdensome to providers, nor is it overly costly. We also clarify that while health care providers are required to post the NPP in a clear and prominent location at the delivery site, providers may post a summary of the notice in such a location as long as the full notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on their part. It would not be appropriate, however, to require the individual to have to ask the receptionist for a copy of the full NPP.

To the extent that some covered entities have already revised their NPPs in response to the enactment of the HITECH Act or State law requirements, we clarify that as long as a covered entity's current NPP is consistent with this final rule and individuals have been informed of all material revisions made to the NPP, the covered entity is not required to revise and distribute another NPP upon publication of this final rule. Finally, we note that to the extent a covered entity is required to comply with Section 504 of the Rehabilitation Act of 1973 or the Americans with Disabilities Act of 1990, the covered entity has an obligation to take steps that may be necessary to ensure effective communication with individuals with disabilities, which could include making the revised NPP or notice of material changes to the NPP available in alternate formats, such as Braille, large print, or audio.

Response to Other Public Comments

Comment: One commenter expressed concern about the addition of more information to the NPP when it is already very long and complex, while several commenters recommended that the final rule require NPPs to be shortened, simplified, and written in a clear, easily understandable manner. In addition, while a few commenters suggested that HHS provide a sample or standard NPP, many more commenters requested flexibility in developing the content of their respective NPPs.

Response: We believe that the additions to the NPP required by the final rule are necessary to fully inform individuals of the covered entity's privacy practices and their rights. The NPP should be provided in a clear, concise, and easy to understand manner, and we clarify that covered entities may use a ''layered notice'' to implement the Rule's provisions, so long as the elements required at § 164.520(b) are included in the document that is provided for the individual. For example, a covered entity may satisfy the NPP provisions by providing the individual with both a short notice that briefly summarizes the individual's rights, as well as other information, and a longer notice, layered beneath the short notice that contains all the elements required by the Rule. Additionally, the Privacy Rule requires that the NPP be written in plain language, and we note that some covered entities may have obligations under other laws with respect to their communication with affected individuals. For example, to the extent a covered entity is obligated to comply with Title VI of the Civil Rights Act of 1964, the covered entity must take reasonable steps to ensure meaningful access for Limited English Proficient persons to the services of the covered entity, which could include translating the NPP into frequently encountered languages. In addition, we agree with the commenters who suggested that covered entities have flexibility and discretion to determine how to draft and prepare their NPPs. Because each NPP will vary based on the functions of the individual covered entity, there is no ''one size fits all'' approach. However, we continue to explore options for making model or best practice language available.

Comment: One commenter requested elimination of the requirement that covered entities obtain agreement from individuals (an opt in) before electronic distribution while another commenter requested that HHS clarify that a covered entity may obtain an electronic agreement from an individual to receive an NPP electronically.

Response: The Privacy Rule permits covered entities to distribute their NPPs or notices of material changes by email, provided the individual has agreed to receive an electronic copy. Although

internet access is a convenience of daily life for many individuals, maintaining the opt-in requirement ensures that individuals who are not able to or choose not to receive information electronically are fully informed of how their protected health information is being used and disclosed and of their individual rights with respect to this information. We clarify that agreement to receive electronic notice can be obtained electronically pursuant to the requirements at § 164.520(c)(3).

9. Section 164.522(a)—Right To Request a Restriction of Uses and Disclosures

Section 164.522(a) of the Privacy Rule requires covered entities to permit individuals to request that a covered entity restrict uses or disclosures of their protected health information for treatment, payment, and health care operations purposes, as well as for disclosures to family members and certain others permitted under § 164.510(b). While covered entities are not required to agree to such requests for restrictions, if a covered entity does agree to restrict the use or disclosure of an individual's protected health information, the covered entity must abide by that restriction, except in emergency circumstances when the information is required for the treatment of the individual. Section 164.522 also includes provisions for the termination of such a restriction and requires that covered entities that have agreed to a restriction document the restriction in writing.

Proposed Rule

Section 13405(a) of the HITECH Act sets forth certain circumstances in which a covered entity now must comply with an individual's request for restriction of disclosure of his or her protected health information. Specifically, section 13405(a) of the HITECH Act requires that when an individual requests a restriction on disclosure pursuant to § 164.522, the covered entity must agree to the requested restriction unless the disclosure is otherwise required by law, if the request for restriction is on disclosures of protected health information to a health plan for the purpose of carrying out payment or health care operations and if the restriction applies to protected health information that pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full.

To implement section 13405(a) of the HITECH Act, we proposed a number of changes to the Privacy Rule's provisions regarding an individual's right to request restrictions of certain uses and disclosures. First, we proposed at § 164.522(a)(1)(vi) to require a covered entity to agree to a request by an individual to restrict the disclosure of protected health information about the individual to a health plan if: (A) the disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law; and (B) the protected health information pertains solely to a health care item or service for which the individual, or person on behalf of the individual other than the health plan, has paid the covered entity in full. In recognition that there are many situations in which family members or other persons may pay for the individual's treatment, we proposed to include language to the provision to ensure that this requirement not be limited to solely the individual paying for the health care item or service but would also include payment made by another person, other than the health plan, on behalf of the individual.

We proposed to modify § 164.522(a)(1)(ii), which states that a covered entity is not required to agree to a restriction, to refer to this exception to that general rule. We noted in the NPRM that in cases where an individual has exercised his or her right to restrict disclosure to a health plan under the above circumstances, the covered entity is also prohibited from making such disclosures to a business associate of the health plan, because a covered entity may only disclose protected health information to a business associate of another covered entity if the disclosure would be permitted directly to the other covered entity. We also proposed conforming modifications to § 164.522(a)(2) and (3) regarding terminating restrictions and documentation of restrictions to reflect these new requirements, and to make clear that, unlike other agreed to restrictions, a covered entity may not unilaterally terminate a required restriction to a health plan under § 164.522(a)(1)(ii).

We provided a number of clarifications, and solicited public comment on a number of issues, regarding these proposed provisions, as follows. We stated that we interpret section 13405(a) as giving the individual a right to determine for which health care items or services the individual wishes to pay out of pocket and restrict. Thus, section 13405(a) would not permit a covered entity to require individuals who wish to restrict disclosures about only certain health care items or services to a health plan to restrict disclosures of protected health information regarding all health care to the health plan. We requested comment on the types of treatment interactions between individuals and covered entities that would make implementing a restriction more difficult and ways to address such difficult situations, such as where an individual wishes to restrict a disclosure regarding a prescription to a health plan but because the provider electronically sends prescriptions to the pharmacy to be filled, the pharmacy may have already billed the health plan by the time the patient arrives at the pharmacy. We requested comment generally on whether covered health care providers that know of a restriction should inform other health care providers downstream of such restriction, including pharmacies, and whether technology could facilitate such notification. We requested comment on examples of the types of disclosures that may fall under this ''required by law'' exception. With respect to an individual, or someone on behalf of the individual, paying out of pocket for the health care item or service, we noted that the individual should not expect that this payment would count towards the individual's out of pocket threshold with respect to his or her health plan benefits. We requested comment on how this provision will function with respect to HMOs, given our understanding that under most current HMO contracts with providers an individual could not pay the provider in full for the treatment or service received. We clarified in the NPRM that if an individual's out of pocket payment for a health care item or service is not honored (e.g., the individual's check bounces), the covered entity is not obligated to continue to abide by the requested restriction because the individual has not fulfilled the requirements necessary to obtain the restriction. Additionally, we stated our expectation in such cases that covered entities make some attempt to resolve any payment issues with the individual prior to sending the protected health information to the health plan, such as by notifying the individual that his or her payment did not go through and giving the individual an opportunity to submit payment and requesting comment on the extent to which covered entities must make reasonable efforts to secure payment from the individual prior to billing the health plan. We requested comment on the scope of a restriction and in what circumstances it should apply to a subsequent, but related, treatment

encounter, such as follow-up care for treatment of a particular condition.

Overview of Public Comments

We received many comments on these proposed provisions and our questions as to how they should apply. A number of commenters generally supported the provisions as being an important right for health care consumers. However, many commenters expressed concerns with these new requirements. Many commenters raised concerns with, and requested guidance on, how to operationalize a restriction. Several commenters were concerned with having to create separate records to ensure that restricted data is not inadvertently sent to or accessible by the health plan or to manually redact information from the medical record prior to disclosure to a health plan. Commenters argued that having to segregate restricted and unrestricted information or redact restricted information prior to disclosure would be burdensome as such a process would generally have to occur manually, and may result in difficulties with ensuring that treating providers continue to have access to the entire medical record. Some commenters were concerned specifically with having to manually redact or create separate records prior to a health plan audit, or otherwise with withholding information from a plan during an audit, to ensure a health plan would not see restricted information.

With respect to the exception to a restriction for disclosures that are required by law, several commenters supported this exception but requested clarification on how such an exception would affect providers' existing legal obligations. Many commenters suggested that providers would be prohibited from receiving cash payment from individuals for items or services otherwise covered by State or Federally funded programs, such as Medicare and Medicaid, and thus, requested that disclosures to such State or Federally funded programs not be eligible for restriction. Similarly, some commenters sought clarification on the effect of this provision where certain State laws prohibit ''balance billing,'' making it illegal for the provider to bill the patient for any covered services over and above any permissible copayment, coinsurance or deductible amounts. Some commenters asked that we clarify that the ''required by law'' exception allows providers to disclose protected health information subject to a restriction for Medicare and Medicaid audits, because those insurers require complete, accurate records for audits.

Other commenters were concerned with applying a restriction to only certain health care items or services provided during a single patient encounter or visit. Commenters argued that split billing is not possible for most providers or that it may be obvious to a health plan if one item or service out of a bundle is restricted and that unbundling services may be costly. One commenter suggested that individuals should only be able to restrict certain types of services/treatment (e.g., cosmetic surgery and family planning services) as such services are more easily segregable from other health care services.

In response to our question regarding available electronic methods through which a prescribing provider could alert a pharmacy that an individual intends to pay out of pocket for a prescription and restrict disclosure to a health plan, commenters indicated they were generally unaware of any system that would alert a pharmacy of restrictions electronically, and many agreed that the cost and burden of flagging records manually would not be feasible for all covered entities. In general, commenters agreed that paper prescriptions would provide individuals with an opportunity to request a restriction when they arrive at the pharmacy. However, commenters also noted that returning to the use of paper prescriptions over electronic prescribing would be a step in the wrong direction, as there are many benefits to electronic prescribing, and it is important not to limit these benefits.

Almost all of the comments we received regarding the obligation generally of health care providers that know of a restriction to inform downstream health care providers of the restriction argued that it should be the individual's and not the provider's responsibility to inform downstream providers of any requested restriction. While a few commenters stated that the provider should bear this responsibility, the majority believed that this obligation would be difficult and burdensome for a provider. Some commenters acknowledged that in time, more advanced electronic and automated systems may allow providers to notify other providers downstream of a restriction, but these commenters stressed that such systems are not widely available at this time.

With respect to the requirement's application to health care providers providing care within an HMO context, many commenters expressed support for the suggestion that HMO patients would have to use an out-of-network provider for treatment to ensure that the restricted information would not be disclosed to the HMO. Some commenters indicated that State laws and/or provider contracts with an HMO may prohibit the provider from receiving a cash payment from an HMO patient above the patient's cost-sharing amount for the health care item or service. Conversely, some commenters stated that individuals should not have to go out-of-network when requesting a restriction and instead, providers could and should treat the services as non-covered services and accept payment directly from the patient. Several commenters also suggested that managed care contracts would have to be revised or renegotiated in order to comply with this provision and as such, ample time for renegotiation should be provided.

Commenters generally supported the language in the proposed rule making clear that a restriction would apply where an individual requests a restriction, but someone other than the individual (other than the health plan), such as a family member, pays for the individual's care on behalf of the individual. One commenter asked for clarification that payment by any health plan would not constitute payment out of pocket by the individual. The commenter stated that such clarification was necessary to avoid the situation where an individual has coverage under multiple plans, pays for care with a secondary plan, requests a restriction on disclosure to the primary plan, and then the secondary plan proceeds to obtain reimbursement from the primary plan disclosing the protected health information at issue. Another commenter asked that we clarify that a clinical research participant whose health care services are paid for by a research grant can still qualify for a restriction to the individual's health plan.

Most commenters supported not having to abide by a requested restriction in cases where the individual's method of payment is returned or otherwise does not go through. A few commenters suggested that a covered entity should include information to this effect in its notice of privacy practices. A number of commenters expressed concern with the ability of a provider to bill a health plan for services following an individual's inability to pay. For example, a provider may find it difficult to be reimbursed for services if the provider did not obtain the plan's required pre-certification for services because the individual initially agreed to pay out of pocket for the services.

Several commenters asked for guidance on what constitutes a

''reasonable effort'' to obtain payment from an individual prior to billing a health plan for health care services where an individual's original form of payment fails, and argued that the effort required should not be too burdensome on providers. A number of commenters suggested various alternatives. A few commenters suggested that providers should be able to set a deadline for payment and then bill the plan if the patient fails to pay; others requested that the regulation set a specific timeframe in which providers must be paid or the requested restriction is terminated. Some commenters suggested that a ''reasonable effort'' should be based upon a covered entity making one or two attempts to contact the patient and obtain payment. Another commenter recommended that reasonable efforts should require the provider to make a good faith effort to obtain payment based on their usual debt collection practices. Other commenters requested clarification that reasonable efforts would not require a provider sending a bill to a collection agency. Some commenters were generally concerned with requiring a provider to wait too long for payment, as the provider could risk the plan not paying for the treatment if it is billed too late. Certain commenters argued that providers should not have to engage in any attempts to resolve payment issues if an individual's payment fails prior to billing the health plan for the services. Finally, a number of commenters asked whether a provider could require payment in full at the time of the request for a restriction to avoid payment issues altogether.

Finally, many commenters responded to the NPRM's approach to follow-up care. The majority of commenters supported the idea that if an individual does not request a restriction and pay out of pocket for follow up care, then the covered entity may disclose the protected health information necessary to obtain payment from the health plan for such follow up care, recognizing that some of the protected health information may relate to and/or indicate that the individual received the underlying health care item or service to which a restriction applied. A few commenters asked whether individual authorization would be required to disclose previously restricted protected health information to a health plan if the individual does not want to restrict the follow up care. A number of commenters expressed support for providers counseling patients on the consequences of not restricting follow-up care. A few commenters were concerned as to how a provider would know when such counseling was needed and what it should include, and asked whether giving the individual a written statement explaining the consequences would suffice.

Final Rule

We adopt the modifications to § 164.522 as proposed in the NPRM to implement section 13405(a) of the HITECH Act. In response to questions and comments regarding how to operationalize these requirements, we provide the following clarifications. We clarify that these provisions do not require that covered health care providers create separate medical records or otherwise segregate protected health information subject to a restricted health care item or service. Covered health care providers will, however, need to employ some method to flag or make a notation in the record with respect to the protected health information that has been restricted to ensure that such information is not inadvertently sent to or made accessible to the health plan for payment or health care operations purposes, such as audits by the health plan. Covered entities should already have in place, and thus be familiar with applying, minimum necessary policies and procedures, which require limiting the protected health information disclosed to a health plan to the amount reasonably necessary to achieve the purpose of the disclosure. Thus, covered entities should already have mechanisms in place to appropriately limit the protected health information that is disclosed to a health plan.

With respect to commenters who were concerned about providers being able to continue to meet their legal obligations, such as disclosing protected health information to Medicare or Medicaid for required audits, we note that the statute and final rule continue to allow disclosures that are otherwise required by law, notwithstanding that an individual has requested a restriction on such disclosures. Thus, a covered entity may disclose the protected health information necessary to meet the requirements of the law. Under the Privacy Rule, ''required by law'' is defined at § 164.103 as a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. For purposes of this definition, ''required by law'' includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes and regulations that require the production of information if payment is sought under a government program providing public benefits. Therefore, if a covered entity is required by law to submit protected health information to a Federal health plan, it may continue to do so as necessary to comply with that legal mandate. With respect to commenters' concerns with prohibitions in State law and under Medicare and Medicaid that prevent providers from billing, and receiving cash payment from, an individual for covered services over and above any permissible cost sharing amounts, we provide the following guidance. If a provider is required by State or other law to submit a claim to a health plan for a covered service provided to the individual, and there is no exception or procedure for individuals wishing to pay out of pocket for the service, then the disclosure is required by law and is an exception to an individual's right to request a restriction to the health plan pursuant to § 154.522(a)(1)(vi)(A) of the Rule. With respect to Medicare, it is our understanding that when a physician or supplier furnishes a service that is covered by Medicare, then it is subject to the mandatory claim submission provisions of section 1848(g)(4) of the Social Security Act (the Act), which requires that if a physician or supplier charges or attempts to charge a beneficiary any remuneration for a service that is covered by Medicare, then the physician or supplier must submit a claim to Medicare. However, there is an exception to this rule where a beneficiary (or the beneficiary's legal representative) refuses, of his/her own free will, to authorize the submission of a bill to Medicare. In such cases, a Medicare provider is not required to submit a claim to Medicare for the covered service and may accept an out of pocket payment for the service from the beneficiary. The limits on what the provider may collect from the beneficiary continue to apply to charges for the covered service, notwithstanding the absence of a claim to Medicare. See the Medicare Benefit Policy Manual, Internet only Manual pub. 100–2, ch. 15, sect. 40, available at *http://www.cms.gov/manuals/Downloads/bp102c15.pdf*. Thus, if a Medicare beneficiary requests a restriction on the disclosure of protected health information to Medicare for a covered service and pays out of pocket for the service (i.e., refuses to authorize the submission of a bill to Medicare for the service), the provider must restrict the disclosure of protected health information regarding the service to Medicare in accordance with § 164.522(a)(1)(vi).

Certain commenters raised concerns with an individual requesting a restriction with respect to only one of several health care items or services provided in a single patient encounter, and a provider being prohibited from unbundling, or it being more costly to unbundle, the services for purposes of billing a health plan. In such cases, we expect providers to counsel patients on the ability of the provider to unbundle the items or services and the impact of doing so (e.g., the health plan still may be able to determine that the restricted item or service was performed based on the context). If a provider is able to unbundle the items or services and accommodate the individual's wishes after counseling the individual on the impact of unbundling, it should do so. If a provider is not able to unbundle a group of items or services, the provider should inform the individual and give the individual the opportunity to restrict and pay out of pocket for the entire bundle of items or services. Where a provider is not able to unbundle a group of bundled items or services, we view such group of bundled items or services as one item or service for the purpose of applying § 164.522(a)(1)(v). However, we would expect a provider to accommodate an individual's request for a restriction for separable and unbundled health care items or services, even if part of the same treatment encounter, such as in the prior example with respect to the patient receiving both treatment for asthma and diabetes. Thus, we decline to provide as a general rule that an individual may only restrict either all or none of the health care items or services that are part of one treatment encounter.

In response to the question we posed in the NPRM regarding methods through which a provider could electronically (such as through an e-prescribing tool) notify a pharmacist of an individual's restriction request, the majority of commenters indicated that there currently is not a widely available method for electronically notifying a pharmacy that a patient has requested a restriction. Further, commenters generally argued that it would be costly, burdensome, and unworkable for a provider to attempt to notify all subsequent providers of an individual's restriction request, particularly given the lack of automated tools to make such notifications, and thus, it should remain the obligation of the individual to notify downstream providers if the individual wants to restrict protected health information to a health plan. We agree that it would be unworkable at this point, given the lack of automated technologies to support such a requirement, to require health care providers to notify downstream providers of the fact that an individual has requested a restriction to a health plan. However, we do encourage providers to counsel patients that they would need to request a restriction and pay out of pocket with other providers for the restriction to apply to the disclosures by such providers. In the case of an individual who wants to restrict disclosures to a health plan concerning a prescribed medication, the prescribing provider can provide the patient with a paper prescription to allow the individual an opportunity to request a restriction and pay for the prescription with the pharmacy before the pharmacy has submitted a bill to the health plan. However, while we do not require it, providers are permitted and encouraged to assist individuals as feasible in alerting downstream providers of the individual's desire to request a restriction and pay out of pocket for a particular health care item or service.

For example, consider an individual who is meeting with her primary physician and requests a restriction on tests that are being administered to determine if she has a heart condition. If, after conducting the tests, the patient's primary physician refers the patient to a cardiologist, it is the patient's obligation to request a restriction from the subsequent provider, the cardiologist, if she wishes to pay out of pocket rather than have her health plan billed for the visit. Although the primary physician in this example would not be required to alert the cardiologist of the patient's potential desire to request a restriction, we encourage providers to do so if feasible or in the very least, to engage in a dialogue with the patient to ensure that he or she is aware that it is the patient's obligation to request restrictions from subsequent providers. In response to commenters who were confused about whether the individual or the provider would have the obligation of notifying subsequent providers when a Health Information Exchange is involved, we clarify that the responsibility to notify downstream providers of a restriction request in this situation also remains with the individual, and not the provider.

With respect to HMOs, we clarify that a provider providing care in such a setting should abide by an individual's requested restriction unless doing so would be inconsistent with State or other law. Thus, if a provider within an HMO is prohibited by law from accepting payment from an individual above the individual's cost-sharing amount (i.e., the provider cannot accept an out of pocket payment from the individual for the service), then the provider may counsel the individual that he or she will have to use an out-of-network provider for the health care item or service in order to restrict the disclosure of protected health information to the HMO for the health care. Providers operating within an HMO context and who are able under law to treat the health care services to which the restriction would apply as out-of-network services should do so in order to abide by the requested restriction. We would not consider a contractual requirement to submit a claim or otherwise disclose protected health information to an HMO to exempt the provider from his or her obligations under this provision. Further, the final rule provides a 180-day compliance period beyond the effective date of these revisions to the Privacy Rule, during which provider contracts with HMOs can be updated as needed to be consistent with these new requirements.

As proposed in the NPRM, under the final rule, a covered entity must apply a restriction not only where an individual pays in full for the healthcare item or service, but also where a family member or other person pays for the item or service on behalf of the individual. We decline to modify the regulation, as suggested by one commenter, to provide that payment from ''any'' health plan, rather than the one to which the disclosure is restricted, should not constitute payment on behalf of the individual. In response to the commenter's concern about difficulties in coordination of benefits for individuals with coverage under multiple plans, we note that this provision does not impede a health plan's ability to disclose protected health information as necessary to another health plan for coordination of benefits. Thus, health plans may continue to make such disclosures.

Many commenters supported the discussion in the NPRM regarding not abiding by a restriction if an individual's payment is dishonored. In such cases, we continue to expect that providers will make a reasonable effort to contact the individual and obtain payment prior to billing a health plan. We do not prescribe the efforts a health care provider must make but leave that up to the provider's policies and individual circumstances. While we require the provider to make a reasonable effort to secure payment from the individual, this requirement is not intended to place an additional

burden on the provider but is instead intended to align with its current policies for contacting individuals to obtain an alternative form of payment to one that was dishonored. We do not require that the individual's debt be placed in collection before a provider is permitted to bill a health plan for the health care services. Further, a provider may choose to require payment in full at the time of the request for a restriction to avoid payment issues altogether. Similarly, where precertification is required for a health plan to pay for services, a provider may require the individual to settle payments for the care prior to providing the service and implementing a restriction to avoid the situation where the provider is unable to be reimbursed by either the individual or the health plan.

We also recognize that a provider may not be able to implement a restriction where an individual waits until care has been initiated to make such a request, such as in the case of a hospital stay, in which case the individual's protected health information may have already been disclosed to the health plan.

With respect to restrictions and follow-up care, we continue to maintain the approach discussed in the NPRM. If an individual has a restriction in place with respect to a health care service but does not pay out of pocket and request a restriction with regard to follow-up treatment, and the provider needs to include information that was previously restricted in the bill to the health plan in order to have the service deemed medically necessary or appropriate, then the provider is permitted to disclose such information so long as doing so is consistent with the provider's minimum necessary policies and procedures. We also clarify that such a disclosure would continue to be permitted for payment purposes and thus, would not require the individual's written authorization. However, as we did in the NPRM, we highly encourage covered entities to engage in open dialogue with individuals to ensure that they are aware that previously restricted protected health information may be disclosed to the health plan unless they request an additional restriction and pay out of pocket for the follow-up care.

Response to Other Public Comments

Comment: Several commenters asked that the provision be limited to just providers and not to covered entities in general. Commenters also asked for clarification on whether the restriction prohibits providers from giving protected health information to health plans solely for payment or health care operations purposes in such cases or all entities that may receive protected health information for payment or health care operations.

Response: We clarify that this provision, in effect, will apply only to covered health care providers. However, the provisions of § 164.522(a) apply to covered entities generally and thus, we decline to alter the regulatory text. In response to commenters' concerns regarding disclosure for payment or health care operations purposes to entities other than the health plan, we clarify that this provision does not affect disclosures to these other entities as permitted by the Privacy Rule.

Comment: Commenters asked what the liability is for a provider who discloses restricted protected health information to a plan.

Response: A provider who discloses restricted protected health information to the health plan is making a disclosure in violation of the Privacy Rule and the HITECH Act, which, as with other impermissible disclosures is subject to the imposition of possible criminal penalties, civil money penalties, or corrective action.

Comment: Several commenters asked that we clarify that the ''required by law'' exception allows providers to respond to subpoenas, court orders, and judicial proceedings.

Response: The ''required by law'' exception in § 164.522(a)(1)(vi) does allow health care providers to respond to court orders and subpoenas issued by a court requiring disclosure of protected health information to a health plan. See the definition of ''required by law'' at § 164.103. Further, § 164.522(a)(1)(vi) does not affect the disclosure of protected health information to entities that are not health plans and thus, disclosures to these other entities made as required by law, for judicial and administrative proceedings, or for law enforcement activities in accordance with §§ 164.512(a), 164.512(e), and 164.512(f), respectively, continue to be permitted.

Comment: Several commenters suggested that the final rule be written to ensure that there are no conflicts with the Fair Debt Collection Practices Act and similar State laws regarding the legal obligation to validate a debt that is disputed by a debtor. Commenters sought clarification on whether the provider can still disclose protected health information for the recovery of debts.

Response: The final rule does not impact a provider's ability to disclose protected health information for payment purposes to a collection agency or otherwise for collection activities related to an individual's debt to the provider. Section 164.522(a) restricts disclosures to a health plan for payment purposes where the individual has paid out of pocket for the health care item or service that is the subject of the disclosure and requests such a restriction.

Comment: Commenters asked that we clarify whether payment with a Flexible Spending Account (FSA) or Health Savings Account (HSA) is considered a payment by a person on behalf of the individual.

Response: An individual may use an FSA or HSA to pay for the health care items or services that the individual wishes to have restricted from another plan; however, in doing so the individual may not restrict a disclosure to the FSA or HSA necessary to effectuate that payment.

Comment: When a restriction is requested, the provider is also prohibited from making disclosures of the restricted protected health information to the business associate of the health plan. One commenter suggested that the final rule make it the priority of the business associate to inform the provider that they are acting as the business associate of the health plan to ensure provider compliance with the rule. Other comments misconstrued the preamble statements on this issue and commented that a provider should be allowed to provide restricted protected health information to its own business associates.

Response: A provider that is prohibited from disclosing protected health information to a health plan may not disclose such information to the health plan's business associate. We do not include a requirement that the business associate inform the provider that they are acting as a business associate of the health plan as it is the provider's responsibility to know to whom and for what purposes it is making a disclosure. We also clarify that a provider is not prohibited from disclosing protected health information restricted from a health plan to its own business associates for the provider's own purposes.

Comment: One commenter expressed concern about the number of workforce members who must know about the restriction and indicated that this may create a risk for potential error with regard to the information.

Response: Covered entities must identify those workforce members or class of persons who need access to particular protected health information, and appropriately train their workforce members as necessary to comply with these new requirements.

10. Section 164.524—Access of Individuals to Protected Health Information

Proposed Rule

Section 164.524 of the Privacy Rule currently establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their protected health information to the extent such information is maintained in the designated record set(s) of a covered entity. An individual's right of access exists regardless of the format of the protected health information, and the standards and implementation specifications that address individuals' requests for access and timely action by the covered entity (i.e., provision of access, denial of access, and documentation) apply to an electronic environment in a similar manner as they do to a paper-based environment. See The HIPAA Privacy Rule's Right of Access and Health Information Technology (providing guidance with respect to how § 164.524 applies in an electronic environment and how health information technology can facilitate providing individuals with this important privacy right), available at: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/eaccess.pdf*.

Section 13405(e) of the HITECH Act strengthens the Privacy Rule's right of access with respect to covered entities that use or maintain an electronic health record (EHR) on an individual. Section 13405(e) provides that when a covered entity uses or maintains an EHR with respect to protected health information of an individual, the individual shall have a right to obtain from the covered entity a copy of such information in an electronic format and the individual may direct the covered entity to transmit such copy directly to the individual's designee, provided that any such choice is clear, conspicuous, and specific. Section 13405(e) also provides that any fee imposed by the covered entity for providing such an electronic copy shall not be greater than the entity's labor costs in responding to the request for the copy.

Section 13405(e) applies by its terms only to protected health information in EHRs. However, incorporating these new provisions in such a limited manner in the Privacy Rule could result in a complex set of disparate requirements for access to protected health information in EHR systems versus other types of electronic records systems. As such, the Department proposed to use its authority under section 264(c) of HIPAA to prescribe the rights individuals should have with respect to their individually identifiable health information to strengthen the right of access as provided under section 13405(e) of the HITECH Act more uniformly to all protected health information maintained in one or more designated record sets electronically, regardless of whether the designated record set is an EHR. The public comments and final regulation on the scope are discussed here. The proposed amendments to each provision implicated by section 13405(e), together with the public comments and final regulation, are discussed more specifically in separate sections below.

Overview of Public Comments

Most commenters were opposed to the proposal to expand the scope of the individual access provision to include all electronic designated record sets and favored limiting the requirement to EHRs. These commenters felt that limiting the access provision to EHRs was consistent with congressional intent and questioned the authority of the Department to expand the scope. Commenters also argued that having disparate requirements for different systems would not be confusing, and requiring electronic access to electronic designated record sets that are not EHRs would be highly burdensome for covered entities. Specifically, commenters stated that the proposed requirement for electronic access would include numerous types of legacy systems, many of which are incapable of producing reports in easily readable formats that can be transmitted electronically. These commenters indicated that a significant amount of information technology development and investment would be needed to comply with this requirement if it applies to all electronic designated record sets.

A number of consumer advocates supported the expanded scope to include all electronic designated records sets in addition to EHRs. These commenters felt that this would provide complete transparency for consumers, help individuals gain access to their medical records and make better-informed decisions about their health care, and promote consistent and uniform practices.

Final Rule

The final rule adopts the proposal to amend the Privacy Rule at § 164.524(c)(2)(ii) to require that if an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. In such cases, to the extent possible, we expect covered entities to provide the individual with a machine readable copy of the individual's protected health information. The Department considers machine readable data to mean digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the protected health information in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats.

We disagree with commenters that questioned the Department's authority to extend the strengthened electronic access right to all protected health information maintained electronically in designated record sets, and believe that this extended electronic right of access is important for individuals as covered entities increasingly transition from paper to electronic records. With regard to the additional burdens on covered entities, we note that providing access to protected health information held in electronic designated record sets was already required under the Privacy Rule at § 164.524, which applies to protected health information in both paper and electronic designated record sets, and which requires providing the copy in the form and format requested by the individual, including electronically, if it is readily producible in such form and format. We anticipate the additional burden to be small due to the flexibility permitted in satisfying this new requirement, as discussed in the section on Form and Format.

Response to Other Public Comments

Comment: Some commenters worried that giving individuals access to administrative systems (in contrast to clinical systems) would present a security concern to covered entities.

Response: Covered entities are not required by this provision to provide individuals with direct access to their systems. They must only provide individuals with an electronic copy of their protected health information.

Comment: Commenters requested clarification on what constitutes an EHR.

Response: Under this final rule, the requirement to provide individuals with access to an electronic copy includes all

protected health information maintained in an electronic designated record set held by a covered entity. Because we are not limiting the right of electronic access to EHRs, we do not believe there is a need to define or further clarify the term at this time.

Comment: One commenter requested clarification that this electronic access requirement preempts State laws that diminish, block, or limit individual access to their records.

Response: We clarify that this HIPAA electronic right of access requirement does preempt contrary State law unless such law is more stringent. In the case of right of access, more stringent means that such State law permits greater rights of access to the individual.

Comment: Several commenters sought clarification of how the new e-access provisions would apply to business associates. One commenter asked whether business associates could continue to provide patients access to records when permitted and acting on behalf of a covered entity. Another commenter asked whether business associates are required to provide information to covered entities and not to individuals directly. One commenter was opposed to direct access from a business associate because of security concerns and increased burden on business associates if corrections are needed.

Response: How and to what extent a business associate is to support or fulfill a covered entity's obligation to provide individuals with electronic access to their records will be governed by the business associate agreement between the covered entity and the business associate. For example, the business associate agreement may provide for the business associate to give copies of the requested information directly to the individual, or to the covered entity for the covered entity to provide the copies to the individual. There is no separate requirement on business associates to provide individuals with direct access to their health records, if that is not what has been agreed to between the covered entity and the business associate in the business associate agreement.

a. Form and Format

Proposed Rule

Section 164.524(c)(2) of the Privacy Rule currently requires a covered entity to provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format, or, if not, in a readable hard copy form or such other form or format as agreed to by the covered entity and the individual. Section 13405(e) of the HITECH Act expands this requirement by explicitly requiring a covered entity that uses or maintains an EHR with respect to protected health information to provide the individual with a copy of such information in an electronic format.

We proposed to implement this statutory provision, in conjunction with our broader authority under section 264(c) of HIPAA, by requiring, in proposed § 164.524(c)(2)(ii), that if the protected health information requested is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. This provision would require any covered entity that electronically maintains the protected health information about an individual, in one or more designated record sets, to provide the individual with an electronic copy of such information (or summary or explanation if agreed to by the individual in accordance with proposed § 164.524(c)(2)(iii)) in the electronic form and format requested or in an otherwise agreed upon electronic form and format. While an individual's right of access to an electronic copy of protected health information is currently limited under the Privacy Rule by whether the form or format requested is readily producible, covered entities that maintain such information electronically in a designated record set would be required under these proposed modifications to provide some type of electronic copy, if requested by an individual.

Because we did not want to bind covered entities to standards that may not yet be technologically mature, we proposed to permit covered entities to make some other agreement with individuals as to an alternative means by which they may provide a readable electronic copy to the extent the requested means is not readily producible. If, for example, a covered entity received a request to provide electronic access via a secure web-based portal, but the only readily producible version of the protected health information was in portable document format (PDF), proposed § 164.524(c)(2)(ii) would require the covered entity to provide the individual with a PDF copy of the protected health information, if agreed to by the covered entity and the individual. We noted that while a covered entity may provide individuals with limited access rights to their EHR, such as through a secure web-based portal, nothing under the current Rule or proposed modifications would require a covered entity to have this capability.

We noted that the option of arriving at an alternative agreement that satisfies both parties is already part of the requirement to provide access under § 164.524(c)(2)(i), so extension of such a requirement to electronic access should present few implementation difficulties. Further, as with other disclosures of protected health information, in providing the individual with an electronic copy of protected health information through a web-based portal, email, on portable electronic media, or other means, covered entities should ensure that reasonable safeguards are in place to protect the information. We also noted that the proposed modification presumes that covered entities have the capability of providing an electronic copy of protected health information maintained in their designated record set(s) electronically through a secure web-based portal, via email, on portable electronic media, or other manner. We invited public comment on this presumption.

Overview of Public Comments

We received many comments and requests for clarification and guidance regarding the permitted methods for offering protected health information on electronic media, and the acceptable form and format of the electronic copy. Several commenters suggested that covered entities be permitted flexibility in determining available electronic formats and requested clarification on what is considered ''readily producible.'' These commenters expressed concerns that a limited number of permissible electronic formats may result in a situation where protected health information could not be converted from a particular electronic system. Other commenters indicated that there should be minimum standards and clearly defined media that are permissible to meet this requirement. One commenter felt that this requirement is important but should be deferred until covered entities have improved their technological capabilities.

Many commenters requested guidance on how to proceed if a covered entity and an individual are unable to come to an agreement on the medium of choice and what is expected in terms of accommodating the individual's medium of choice. Some commenters suggested various alternate solutions if

an agreement cannot be reached, including any readily producible format, PDF, or hard copy protected health information. Some covered entities felt that individuals should not have an unlimited choice in terms of the electronic media they are willing to accept, and should only be permitted to confine their choices of electronic media to a couple of options that the covered entity has available.

Final Rule

The final rule adopts the proposal to require covered entities to provide electronic information to an individual in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. We recognize that what is available in a readable electronic form and format will vary by system and that covered entities will continue to improve their technological capabilities over time. We therefore allow covered entities the flexibility to provide readily producible electronic copies of protected health information that are currently available on their various systems. A covered entity is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific form that is not readily producible by the covered entity at the time of the request, provided that the covered entity is able to provide some form of electronic copy. We note that some legacy or other systems may not be capable of providing any form of electronic copy at present and anticipate that some covered entities may need to make some investment in order to meet the basic requirement to provide some form of electronic copy.

We agree with covered entities that individuals should not have an unlimited choice in the form of electronic copy requested. However, covered entities must still provide individuals with some kind of readable electronic copy. If an individual requests a form of electronic copy that the covered entity is unable to produce, the covered entity must offer other electronic formats that are available on their systems. If the individual declines to accept any of the electronic formats that are readily producible by the covered entity, the covered entity must provide a hard copy as an option to fulfill the access request. While we remain neutral on the type of technology that covered entities may adopt, a PDF is a widely recognized format that would satisfy the electronic access requirement if it is the individual's requested format or if the individual agrees to accept a PDF instead of the individual's requested format. Alternatively, there may be circumstances where an individual prefers a simple text or rich text file and the covered entity is able to accommodate this preference. A hard copy of the individual's protected health information would not satisfy the electronic access requirement. However, a hard copy may be provided if the individual decides not to accept any of the electronic formats offered by the covered entity.

Response to Other Public Comments

Comment: Several covered entities commented on the form of a request for access to electronic protected health information. Some expressed appreciation for permitting an electronic request process, including e-signatures and authentication. Some expressed opposition to the requirement for a signed request in writing, as it would be highly burdensome and cause delays. Covered entities sought guidance on elements that would be required or permitted in a request form for individuals.

Response: We clarify that the requirement at § 164.524(b)(1), which states that the covered entity may require individuals to make requests for access in writing, provided that it informs individuals of such a requirement, remains unchanged. Therefore, covered entities may at their option require individuals to make requests for electronic copies of their protected health information in writing. We note that the Privacy Rule allows for electronic documents to qualify as written documents, as well as electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law. If the covered entity chooses to require a written request, it has flexibility in determining what information to put into the request form. However, the request form may not be in any way designed to discourage an individual from exercising his or her right. A covered entity may also choose to accept an individual's oral request for an electronic copy of their protected health information without written signature or documentation.

Comment: We received several comments on the content that covered entities are required to provide in response to an electronic access request. Some commenters felt that there should be a defined minimum set of data elements to satisfy this requirement, particularly for non-EHR data. Covered entities also requested clarification on how to handle links to images or other data.

Response: We clarify that just as is currently required for hard copy protected health information access requests, covered entities must provide an electronic copy of all protected health information about the individual in an electronically maintained designated record set, except as otherwise provided at § 164.524(a). If the designated record set includes electronic links to images or other data, the images or other data that is linked to the designated record set must also be included in the electronic copy provided to the individual. The electronic copy must contain all protected health information electronically maintained in the designated record set at the time the request is fulfilled. The individual may request, however, only a portion of the protected health information electronically maintained in the designated record set, in which case the covered entity is only required to provide the requested information.

Comment: One commenter asserted that the request for protected health information should only apply to protected health information the covered entity has at the time of the request, not any additional protected health information that it obtains while processing the request.

Response: We clarify that the electronic copy must reflect all electronic protected health information held by the covered entity in a designated record set, or the subset of electronic protected health information specifically requested by the individual, at the time the request is fulfilled.

Comment: One commenter asked for confirmation that the new electronic requirement does not include a requirement to scan paper and provide electronic copies of records held in paper form.

Response: We clarify that covered entities are not required to scan paper documents to provide electronic copies of records maintained in hard copy. We note that for covered entities that have mixed media, it may in some cases be easier to scan and provide all records in electronic form rather than provide a combination of electronic and hard copies, however this is in no way required.

Comment: Many commenters expressed security concerns related to this new requirement. Covered entities felt that they should not have to use portable devices brought by individuals (particularly flash drives), due to the security risks that this would introduce to their systems. Some covered entities

additionally asserted that requiring the use of individually-supplied media is prohibited by the Security Rule, based on the risk analysis determination of an unacceptable risk to the confidentiality, integrity and availability of the covered entity's electronic protected health information.

Response: We acknowledge these security concerns and agree with commenters that it may not be appropriate for covered entities to accept the use of external portable media on their systems. Covered entities are required by the Security Rule to perform a risk analysis related to the potential use of external portable media, and are not required to accept the external media if they determine there is an unacceptable level of risk. However, covered entities are not then permitted to require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so. The individual may in such cases opt to receive an alternative form of the electronic copy of the protected health information, such as through email.

Comment: Several commenters specifically commented on the option to provide electronic protected health information via unencrypted email. Covered entities requested clarification that they are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. Some felt that the ''duty to warn'' individuals of risks associated with unencrypted email would be unduly burdensome on covered entities. Covered entities also requested clarification that they would not be responsible for breach notification in the event that unauthorized access of protected health information occurred as a result of sending an unencrypted email based on an individual's request. Finally, one commenter emphasized the importance that individuals are allowed to decide if they want to receive unencrypted emails.

Response: We clarify that covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email. We disagree that the ''duty to warn'' individuals of risks associated with unencrypted email would be unduly burdensome on covered entities and believe this is a necessary step in protecting the protected health information. We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual.

b. Third Parties

Proposed Rule

Section 164.524(c)(3) of the Privacy Rule currently requires the covered entity to provide the access requested by the individual in a timely manner, which includes arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of protected health information at the individual's request. The Department had previously interpreted this provision as requiring a covered entity to mail the copy of protected health information to an alternative address requested by the individual, provided the request was clearly made by the individual and not a third party. Section 13405(e)(1) of the HITECH Act provides that if the individual chooses, he or she has a right to direct the covered entity to transmit an electronic copy of protected health information in an EHR directly to an entity or person designated by the individual, provided that such choice is clear, conspicuous, and specific.

Based on section 13405(e)(1) of the HITECH Act and our authority under section 264(c) of HIPAA, we proposed to expand § 164.524(c)(3) to expressly provide that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. This proposed amendment is consistent with the Department's prior interpretation on this issue and would apply without regard to whether the protected health information is in electronic or paper form. We proposed to implement the requirement of section 13405(e)(1) that the individual's ''choice [be] clear, conspicuous, and specific'' by requiring that the individual's request be ''in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.'' We noted that the Privacy Rule allows for electronic documents to qualify as written documents for purposes of meeting the Rule's requirements, as well as electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law. Thus, a covered entity could employ an electronic process for receiving an individual's request to transmit a copy of protected health information to his or her designee under this proposed provision. Whether the process is electronic or paper-based, a covered entity must implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests protected health information, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed.

Overview of Public Comments

Commenters requested clarification regarding the proposal to transmit an electronic copy of protected health information to another person designated by the individual. In particular, covered entities sought clarification on whether or not an authorization is required prior to transmitting the requested electronic protected health information to a third party designated by the individual. Some commenters supported the ability to provide electronic protected health information access to third parties without individual authorization, while others felt that authorization should be required. Covered entities requested clarification that they are not liable when making reasonable efforts to verify the identity of a third party recipient identified by the individual.

Final Rule

The final rule adopts the proposed amendment § 164.524(c)(3) to expressly provide that, if requested by an individual, a covered entity must transmit the copy of protected health information directly to another person designated by the individual. In contrast to other requests under § 164.524, when an individual directs the covered entity to send the copy of protected health information to another designated person, the request must be made in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the protected health information. If a covered entity has decided to require all access requests in writing, the third party recipient information and signature by the individual can be included in the same written request; no additional or separate written request is

required. This written request for protected health information to be sent to a designated person is distinct from an authorization form, which contains many additional required statements and elements (see § 164.508(c)). Covered entities may rely on the information provided in writing by the individual when providing protected health information to a third party recipient identified by the individual, but must also implement reasonable policies and procedures under § 164.514(h) to verify the identity of any person who requests protected health information, as well as implement reasonable safeguards under § 164.530(c) to protect the information that is used or disclosed. For example, reasonable safeguards would not require the covered entity to confirm that the individual provided the correct email address of the third party, but would require reasonable procedures to ensure that the covered entity correctly enters the email address into its system.

c. Fees

Proposed Rule

Section 164.524(c)(4) of the Privacy Rule currently permits a covered entity to impose a reasonable, cost-based fee for a copy of protected health information (or a summary or explanation of such information). However, such a fee may only include the cost of: (1) The supplies for, and labor of, copying the protected health information; (2) the postage associated with mailing the protected health information, if applicable; and (3) the preparation of an explanation or summary of the protected health information, if agreed to by the individual. With respect to providing a copy (or summary or explanation) of protected health information from an EHR in electronic form, however, section 13405(e)(2) of the HITECH Act provides that a covered entity may not charge more than its labor costs in responding to the request for the copy.

In response to section 13405(e)(2) of the HITECH Act, we proposed to amend § 164.524(c)(4)(i) to identify separately the labor for copying protected health information, whether in paper or electronic form, as one factor that may be included in a reasonable cost-based fee. While we did not propose more detailed considerations for this factor within the regulatory text, we retained all prior interpretations of labor with respect to paper copies—that is, that the labor cost of copying may not include the costs associated with searching for and retrieving the requested information. With respect to electronic copies, we asserted that a reasonable cost-based fee includes costs attributable to the labor involved to review the access request and to produce the electronic copy, which we expected would be negligible. However, we did not consider a reasonable cost-based fee to include a standard ''retrieval fee'' that does not reflect the actual labor costs associated with the retrieval of the electronic information or that reflects charges that are unrelated to the individual's request (e.g., the additional labor resulting from technical problems or a workforce member's lack of adequate training). We invited public comment on this aspect of our rulemaking, specifically with respect to what types of activities related to managing electronic access requests should be compensable aspects of labor.

We also proposed to amend § 164.524(c)(4)(ii) to provide separately for the cost of supplies for creating the paper copy or electronic media (i.e., physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. This reorganization and the addition of the phrase ''electronic media'' reflected our understanding that since section 13405(e)(2) of the HITECH Act permits only the inclusion of labor costs in the charge for electronic copies, it by implication excludes charging for the supplies that are used to create an electronic copy of the individual's protected health information, such as the hardware (computers, scanners, etc.) or software that is used to generate an electronic copy of an individual's protected health information in response to an access request. We noted that this limitation is in contrast to a covered entity's ability to charge for supplies for hard copies of protected health information (e.g., the cost of paper, the prorated cost of toner and wear and tear on the printer). See 65 FR 82462, 82735, Dec. 28, 2000 (responding to a comment seeking clarification on ''capital cost for copying'' and other supply costs by indicating that a covered entity was free to recoup all of their reasonable costs for copying). We asserted that this interpretation was consistent with the fact that, unlike a hard copy, which generally exists on paper, an electronic copy exists independent of media, and can be transmitted securely via multiple methods (e.g., email, a secure web-based portal, or an individual's own electronic media) without accruing any ancillary supply costs. We also noted, however, that our interpretation of the statute would permit a covered entity to charge a reasonable and cost-based fee for any electronic media it provided, as requested or agreed to by an individual.

While we proposed to renumber the remaining factors at § 164.524(c)(4), we did not propose to amend their substance. With respect to § 164.524(c)(4)(iii), however, we noted that our interpretation of the statute would permit a covered entity to charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier (e.g., if the individual requests that the covered entity save protected health information to a CD and then mail the CD to a designee).

Overview of Public Comments

Commenters generally supported and appreciated the inclusion of a reasonable, cost-based fee that includes both labor and, in some cases, supply costs to support the new electronic access requirement. Several commenters disagreed that the cost related to reviewing and responding to requests would be negligible, particularly if the scope includes information in designated record sets and not only EHRs, since more technically trained staff would be necessary to perform this function.

Commenters provided many suggestions of costs that should be permitted in the fees, including those associated with labor, materials, systems, retrieval (particularly for old data maintained in archives, backup media or legacy systems), copying, transmission, and capital to recoup the significant investments made for data access, storage and infrastructure. Commenters offered additional suggestions on labor-related costs, including: skilled technical staff time; time spent recovering, compiling, extracting, scanning and burning protected health information to media, and distributing the media; and preparation of an explanation or summary if appropriate. Suggestions of materials-related costs included: CDs, flash drives, tapes or other portable media; new types of technology needed to comply with individual requests; office supplies; and mail copies. Systems-related costs included: software necessary to conduct protected health information searches; and implementation and maintenance of security systems and secure connectivity.

Final Rule

The final rule adopts the proposed amendment at § 164.524(c)(4)(i) to identify separately the labor for copying protected health information, whether

in paper or electronic form, as one factor that may be included in a reasonable cost-based fee. We acknowledge commenters' assertions that the cost related to searching for and retrieving electronic protected health information in response to requests would be not be negligible, as opposed to what we had anticipated, particularly in regards to designated record set access that will require more technically trained staff to perform this function. We clarify that labor costs included in a reasonable cost-based fee could include skilled technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning protected health information to media, and distributing the media. This could also include the time spent preparing an explanation or summary of the protected health information, if appropriate.

The final rule also adopts the proposed amendment at § 164.524(c)(4)(ii) to provide separately for the cost of supplies for creating the paper copy or electronic media (i.e., physical media such as a compact disc (CD) or universal serial bus (USB) flash drive), if the individual requests that the electronic copy be provided on portable media. We do not require that covered entities obtain new types of technology needed to comply with specific individual requests, and therefore the cost of obtaining such new technologies is not a permissible fee to include in the supply costs.

With respect to § 164.524(c)(4)(iii), we clarify that a covered entity is permitted to charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier (e.g., if the individual requests that the covered entity save protected health information to a CD and then mail the CD to a designee).

Fees associated with maintaining systems and recouping capital for data access, storage and infrastructure are not considered reasonable, cost-based fees, and are not permissible to include under this provision. Covered entities are not required to adopt or purchase new systems under this provision, and thus any costs associated with maintaining them are present regardless of the new electronic access right. Additionally, although the proposed rule indicated that a covered entity could charge for the actual labor costs associated with the retrieval of electronic information, in this final rule we clarify that a covered entity may not charge a retrieval fee (whether it be a standard retrieval fee or one based on actual retrieval costs). This interpretation will ensure that the fee requirements for electronic access are consistent with the requirements for hard copies, which do not allow retrieval fees for locating the data.

Response to Other Public Comments

Comment: Commenters requested clarification on how to proceed when State laws designate fees.

Response: When a State law provides a limit on the fee that a covered entity may charge for a copy of protected health information, this is relevant in determining whether a covered entity's fee is ''reasonable'' under § 164.524(c)(4). A covered entity's fee must be both reasonable and cost-based. For example, if a State permits a charge of 25 cents per page, but a covered entity is able to provide an electronic copy at a cost of five cents per page, then the covered entity may not charge more than five cents per page (since that is the reasonable and cost-based amount). Similarly, if a covered entity's cost is 30 cents per page but the State law limits the covered entity's charge to 25 cents per page, then the covered entity may not charge more than 25 cents per page (since charging 30 cents per page would be the cost-based amount, but would not be reasonable in light of the State law).

Comment: One commenter suggested that labor-related costs should include preparation of an affidavit certifying that the information is a true and correct copy of the records.

Response: We do not consider the cost to prepare an affidavit to be a copying cost. Thus, where an individual requests that an affidavit accompany the copy of protected health information requested by the individual for litigation purposes or otherwise, a covered entity may charge the individual for the preparation of such affidavit and is not subject to the reasonable, cost-based fee limitations of § 164.524(c)(4). However, a covered entity may not withhold an individual's copy of his or her protected health information for failure by the individual to pay any fees for services above and beyond the copying, such as for preparing an affidavit.

Comment: Some commenters recommended defining the following terms: ''preparing,'' ''producing,'' and ''transmitting.''

Response: We decline to define the terms ''preparing,'' ''producing,'' and ''transmitting,'' as we believe the terms have been adequately understood and utilized in the context of hard copy access to protected health information.

d. Timeliness

Proposed Rule

We requested comment on one aspect of the right to access and obtain a copy of protected health information which the HITECH Act did not amend. In particular, the HITECH Act did not change the timeliness requirements for provision of access at § 164.524(b). Under the current requirements, a request for access must be approved or denied, and if approved, access or a copy of the information provided, within 30 days of the request. In cases where the records requested are only accessible from an off-site location, the covered entity has an additional 30 days to respond to the request. In extenuating circumstances where access cannot be provided within these timeframes, the covered entity may have a one-time 30-day extension if the individual is notified of the need for the extension within the original timeframes.

With regard to the timeliness of the provision of access, we recognized that with the advance of EHRs, there is an increasing expectation and capacity to provide individuals with almost instantaneous electronic access to the protected health information in those records through personal health records or similar electronic means. On the other hand, we did not propose to limit the right to electronic access of protected health information to certified EHRs, and the variety of electronic systems that are subject to this proposed requirement would not all be able to comply with a timeliness standard based on personal health record capabilities. It was our assumption that a single timeliness standard that would address a variety of electronic systems, rather than having a multitude of standards based on system capacity, would be the preferred approach to avoid workability issues for covered entities. Even under a single standard, nothing would prevent users of EHR systems from exceeding the Privacy Rule's timeliness requirements for providing access to individuals. Additionally, the Medicare and Medicaid EHR Incentive Programs (the ''meaningful use'' programs) require users of Certified EHR Technology to provide individuals with expedited access to information. Based on the assumption that a single standard would be the preferred approach under the Privacy Rule, we requested public comment on an appropriate, common timeliness standard for the provision of access by covered entities with electronic designated record sets generally. We specifically requested comment on aspects of existing systems

that would create efficiencies in processing of requests for electronic information, as well as those aspects of electronic systems that would provide little change from the time required for processing a paper record. Alternatively, we requested comment on whether the current standard could be altered for all systems, paper and electronic, such that all requests for access should be responded to without unreasonable delay and not later than 30 days.

We also requested public comment on whether, contrary to our assumption, a variety of timeliness standards based on the type of electronic designated record set is the preferred approach and if so, how such an approach should be implemented.

Finally, we requested comment on the time necessary for covered entities to review access requests and make necessary determinations, such as whether the granting of access would endanger the individual or other persons so as to better understand how the time needed for these reviews relates to the overall time needed to provide the individual with access. Further, we requested comment generally on whether the provision which allows a covered entity an additional 30 days to provide access to the individual if the protected health information is maintained off-site should be eliminated altogether for both paper and electronic records, or at least for protected health information maintained or archived electronically because the physical location of electronic data storage is not relevant to its accessibility.

Overview of Public Comments

Commenters generally supported maintaining the same timeframe for response for both paper and electronic records and not modifying the existing timeframes for response. Commenters espoused many rationales for maintaining a single standard and the existing response standards, including that off-site electronic storage with back-up tapes will require time to obtain the electronic media, multiple electronic systems may need to be accessed, some systems may not have data stored in useable formats requiring time to convert data, and time may be required to obtain data from business associates and subcontractors.

Some commenters acknowledged that electronic records may be easier to access, but review of records and verification processes would still require time that cannot be shortcut because a record is electronic. One commenter acknowledged that shorter times may be achievable when specific data set standards are established and covered entities have electronic records in place. One commenter believed that electronic records could be furnished in a much shorter timeframe, such as two business days.

Several commenters suggested responses be done in much shorter timeframes, such as instantly, within one day or three days. One commenter noted that meaningful use standards required access within three days for 50 percent of patients. These commenters suggested alternative timeframes for adoption, such as allowing 60 days for response due to off-site storage issues and potential for multiple requests. One commenter suggested 30 and 60 day times were unworkable and another commenter suggested eliminating the 30 day extension for off-site record storage. One commenter suggested 30 days may be longer than is necessary, but cautioned against mandates that would unreasonably divert provider resources (e.g., five days would be unreasonable when a provider must take time to include explanatory notes).

Final Rule

The final rule modifies the timeliness requirements for right to access and to obtain a copy of protected health information at § 164.524(b). We remove the provision at § 164.524(b)(2)(ii) that permits 60 days for timely action when protected health information for access is not maintained or accessible to the covered entity on-site. We retain and renumber as necessary the provision at § 164.524(b)(2)(iii) that permits a covered entity a one-time extension of 30 days to respond to the individual's request (with written notice to the individual of the reasons for delay and the expected date by which the entity will complete action on the request).

We believe the 30 day timeframe for access is appropriate and achievable by covered entities given the increasing expectation and capacity to provide individuals with almost instantaneous electronic access to the protected health information in those records through personal health records or similar electronic means. While a covered entity is permitted 30 days to provide access (with a 30-day extension when necessary), we encourage covered entities to provide individuals with access to their information sooner, and to take advantage of technologies that provide individuals with immediate access to their health information. Nevertheless, for covered entities that continue to make use of off-site storage or have additional time constraints to providing access, the 30 day extension remains available for a covered entity to exercise. This means, for example, that a covered entity must provide an individual with access to off-site records within 30 days of the individual's request when possible, with a 30-day extension available (for a total of 60 days, in contrast to the current law that permits up to 90 days to provide the individual with access to such records).

We decline to establish separate timeframes for timely access based upon whether the protected health information to be accessed is paper or electronic. Commenters generally supported adoption of a single standard rather than differing standards based upon whether a record is paper or electronic and no comments provided compelling reasons to establish differing standards.

Response to Other Public Comments

Comment: One commenter asked for clarification as to when the time period for responding to a response begins if the parties spend significant time attempting to reach agreement on the format of the electronic copy.

Response: We confirm that the time period for responding to a request for access begins on the date of the request. Covered entities that spend significant time before reaching agreement on the electronic format for a response are using part of the 30 days permitted for response.

Comment: One commenter suggested there should be a transition period for those covered entities that do not currently have the capability to meet the electronic access requirement.

Response: We decline to implement a transition period for access to electronic copies of protected health information. Covered entities are already subject to the hard copy access requirement for all information held in designated record sets, including electronic designated record sets, and the new requirement for electronic copies gives covered entities the flexibility to provide an electronic copy in a form that is readily producible. We do not believe additional time is needed to provide electronic copies of protected health information that are readily producible.

11. Other Technical Changes and Conforming Changes

Proposed Rule

We proposed to make a number of technical and conforming changes to the Privacy Rule to fix minor problems, such as incorrect cross-references, mistakes of grammar, and typographical errors. These changes are shown in Table 3 below.

TABLE 3—TECHNICAL AND CONFORMING CHANGES

Regulation section	Current language	Proposed change	Reason for change
164.510(b)(2)(iii)	''based the exercise of professional Judgment''.	Insert ''on'' after ''based''	Correct typographical error.
164.512(b)(1)	''Permitted disclosures'' and ''may disclose''.	Insert ''uses and'' and ''use or'' before ''disclosures'' and ''disclose,'' respectively.	Correct inadvertent omission.
164.512(e)(1)(iii)	''seeking protecting health information''.	Change ''protecting'' to ''protected''	Correct typographical error.
164.512(e)(1)(vi)	''paragraph (e)(1)(iv) of this section''	Change ''(e)(1)(iv)'' to ''(e)(1)(v)''	Correct cross-reference.
164.512(k)(3)	''authorized by 18 U.S.C. 3056, or to foreign heads of state, or to for the conduct of investigations''.	Remove the comma after ''U.S.C. 3056'' and the ''to'' before ''for''.	Correct typographical errors.

In addition to the above technical changes, we proposed to make a few clarifications to existing text in various provisions of the regulation not otherwise addressed in the above preamble. These are as follows.

1. Section 164.506(c)(5) permits a covered entity to disclose protected health information ''to another covered entity that participates in the organized health care arrangement.'' We proposed to change the words ''another covered entity that participates'' to ''other participants'' because not all participants in an organized health care arrangement may be covered entities; for example, some physicians with staff privileges at a hospital may not be covered entities.

2. Section 164.510(a)(1)(ii) permits the disclosure of directory information to members of the clergy and other persons who ask for the individual by name. We proposed to add the words ''use or'' to this permission, to cover the provision of such information to clergy who are part of a facility's workforce.

3. Section 164.510(b)(3) covers uses and disclosures of protected health information when the individual is not present to agree or object to the use or disclosure, and, as pertinent here, permits disclosure to persons only of ''the protected health information that is directly relevant to the person's involvement with the individual's health care.'' We proposed to delete the last two quoted words and substitute the following: ''care or payment related to the individual's health care or needed for notification purposes.'' This change aligns the text of paragraph (b)(3) with the permissions provided for at paragraph (b)(1) of this section.

4. Where an employer needs protected health information to comply with workplace medical surveillance laws, such as the Occupational Safety and Health Administration or Mine Safety and Health Administration requirements, § 164.512(b)(1)(v)(A) permits a covered entity to disclose, subject to certain conditions, protected health information of an individual to the individual's employer if the covered entity is a covered health care provider ''who is a member of the workforce of such employer or who provides health care to the individual at the request of the employer.'' We proposed to amend the quoted language by removing the words ''who is a member of the workforce of such employer or,'' as the language is unnecessary.

5. At § 164.512(k)(1)(ii), we proposed to replace the word ''Transportation'' with ''Homeland Security.'' The language regarding a component of the Department of Transportation was included to refer to the Coast Guard; however, the Coast Guard was transferred to the Department of Homeland Security in 2003.

6. At § 164.512(k)(5), which permits a covered entity to disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual protected health information about the inmate or individual in certain necessary situations, we proposed to replace the word ''and'' after the semicolon in paragraph (i)(E) with the word ''or.'' The intent of § 164.512(k)(5)(i) is not that the existence of all of the conditions is necessary to permit the disclosure, but rather that the existence of any would permit the disclosure.

Overview of Public Comments

One commenter requested clarification about whether business associates may participate in an organized health care arrangement (OHCA) under § 164.506(c)(5). Another commenter recommended against changing the language of § 164.506(c)(5), arguing that such a change could bring entities like employers and pharmaceutical companies into OHCAs that should not otherwise have access to protected health information, and suggested that the Department change the language to make clear that an OHCA may include only professional staff members.

Final Rule

The final rule implements the technical, conforming, and clarifying changes as proposed. In response to the comments regarding which entities may participate in an OHCA, we clarify that a covered entity participating in an OHCA or the OHCA itself may contract with a business associate to provide certain functions, activities, or services on its behalf that involve access to protected health information, provided the applicable requirements of §§ 164.502(e), 164.504(e), 164.308(b) and 164.314(a) are met. Further, the definition of an organized health care arrangement (OHCA) at § 160.103 includes a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. We modified § 164.506(c)(5) as discussed above in recognition of the fact that not all participants in a clinically integrated care setting may be covered entities (e.g., hospital with physicians with staff privileges that are not workforce members). Such change does not permit employers and pharmaceutical representatives to receive access to protected health information from or through an OHCA in a manner they would otherwise be prohibited from now.

V. Modifications to the Breach Notification Rule Under the HITECH Act

A. Background

Section 13402 of the HITECH Act requires HIPAA covered entities to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information. In some cases, the Act requires covered entities also to provide notification to the media of breaches. In the case of a breach of unsecured protected health

information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach. Finally, the Act requires the Secretary to post on an HHS Web site a list of covered entities that experience breaches of unsecured protected health information involving more than 500 individuals.

Section 13400(1) of the Act defines ''breach'' to mean, generally, the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information. The Act includes three exceptions to this definition to encompass situations Congress clearly intended not to constitute breaches: (1) Unintentional acquisition, access, or use of protected health information by an employee or other person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such person with the covered entity or business associate and such information is not further acquired, accessed, used, or disclosed by any person (section 13400(1)(B)(i)); (2) inadvertent disclosure of protected health information from one person authorized to access protected health information at a facility operated by a covered entity or business associate to another person similarly situated at the same facility and the information received is not further acquired, accessed, used or disclosed without authorization by any person (section 13400(1)(B)(ii) and (iii)); and (3) unauthorized disclosures in which an unauthorized person to whom protected health information is disclosed would not reasonably have been able to retain the information (section 13400(1)(A)).

Further, section 13402(h) of the Act defines ''unsecured protected health information'' as ''protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance'' and provides that the guidance specify the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that implement the specified technologies and methodologies with respect to protected health information are not required to provide notifications in the event of a breach of such information—that is, the information is not considered ''unsecured'' in such cases. As required by the Act, the Secretary initially issued this guidance on April 17, 2009 (it was subsequently published at 74 FR 19006 on April 27, 2009). The guidance listed and described encryption and destruction as the two technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

In cases in which notification is required, the Act at section 13402 prescribes the timeliness, content, and methods of providing the breach notifications.

Section 13402 required HHS to issue within 180 days of enactment interim final regulations to implement these breach notification requirements. The Department issued an interim final rule on August 24, 2009, with a 60-day public comment period (74 FR 42740). The interim final rule became effective on September 23, 2009. In the preamble to the interim final rule, the Department also re-issued without substantive change its Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals that was initially issued on April 17, 2009. The Guidance continues to specify encryption and destruction as the two methods for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals—or ''secured''—and thus, exempt from the breach notification obligations. See 74 FR 42741–43.

B. Overview of the Interim Final Rule

The interim final rule added a new subpart D to part 164 of title 45 of the Code of Federal Regulations (CFR) to implement the breach notification provisions of section 13402 of the HITECH Act. In developing the interim final rule, the Department consulted closely with the Federal Trade Commission (FTC), which administers similar breach notification requirements on vendors of personal health records (PHRs) and their third party service providers under section 13407 of the HITECH Act. The interim final rule and FTC's Health Breach Notification Rule (74 FR 42962, published August 25, 2009) made clear that entities operating as HIPAA covered entities and business associates are subject to HHS', and not the FTC's, breach notification rule. Second, to address those limited cases where an entity may be subject to both HHS' and the FTC's rules, such as a vendor that offers PHRs to customers of a HIPAA covered entity as a business associate and also offers PHRs directly to the public, both sets of regulations were harmonized by including the same or similar language, within the constraints of the statutory language.

The 60-day public comment period on the interim final rule closed on October 23, 2009. The Department received approximately 120 comments during the comment period from a variety of entities, including health care providers, hospital and medical associations, health plans, educational institutions, information technology companies, privacy and security advocates, consumer groups, state agencies, and several members of Congress. The provisions of the interim final rule are discussed in more detail below, along with the public comments received, and the provisions of this final rule.

C. Section-by-Section Description of Final Rule and Response to Comments

1. Section 164.402—Definitions

a. Definition of ''Breach''

Interim Final Rule

Section 13400(1)(A) of the Act defines ''breach'' as the ''unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.'' Section 13400(1)(B) of the Act provides two additional exceptions to the definition of ''breach.'' The interim final rule at 45 CFR 164.402 defined a ''breach'' to mean generally ''the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information.'' The definition included the statutory exceptions to the definition (discussed below) and clarified that ''unauthorized'' for purposes of the statute meant in a manner not permitted by the Privacy Rule.

In addition, for purposes of this definition, the rule provided that ''compromises the security or privacy of the protected health information'' means poses a significant risk of financial, reputational, or other harm to the individual. The Department included this standard regarding a significant risk of harm to the individual (i.e., harm standard) after considering public comment received in response to the Department's request for information on the HITECH Act's breach notification provisions. See 74 FR 19006. The inclusion of the harm standard was intended to align the Department's rule with many State

breach notification laws, as well as existing obligations on Federal agencies pursuant to OMB Memorandum M–07–16, that have similar standards for triggering breach notification. In addition, the standard was intended to ensure that consumers were not flooded with breach notifications for inconsequential events, which could cause unnecessary anxiety and eventual apathy among consumers.

To determine whether an impermissible use or disclosure of protected health information constitutes a breach under this standard, covered entities and business associates were required to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In conducting the risk assessment, covered entities and business associates were to consider a number or combination of factors, including who impermissibly used the information or to whom the information was impermissibly disclosed; whether the covered entity or business associate had taken steps to mitigate or eliminate the risk of harm; whether the protected health information was actually accessed; and what type or amount of protected health information was impermissibly used or disclosed.

The rule provided further that an impermissible use or disclosure of protected health information that qualifies as a limited data set but also excludes dates of birth and zip codes (both identifiers that may otherwise be included in a limited data set) does not compromise the security or privacy of the protected health information. The Department included this narrow exception in the belief that it would be very difficult to re-identify a limited data set that excludes dates of birth and zip codes. Thus, a breach of such information would pose a low level of risk of harm to an individual.

The interim final rule also included the three statutory exceptions to the definition of breach. To implement section 13400(1)(B)(i) of the Act, the first regulatory exception provided that a breach excludes any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule. We substituted the term ''workforce members'' for the statutory term ''employees'' because ''workforce member'' is a defined term for purposes of the HIPAA Rules and means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate.

In addition to unintentional, good faith access to protected health information by workforce members, this exception covers similar access by a business associate of a covered entity or subcontractor with respect to a business associate or other person acting on behalf of a covered entity or business associate. The exception does not, however, cover situations involving snooping employees, because access as a result of such snooping would be neither unintentional nor done in good faith.

To implement section 13400(1)(B)(ii) and (iii) of the Act, the second regulatory exception provided that a breach excludes inadvertent disclosures of protected health information from a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates. The regulatory exception includes reference to an ''organized health care arrangement'' to capture, among other things, clinically integrated care settings in which individuals typically receive health care from more than one health care provider, such as a hospital, and the health care providers who have staff privileges at the hospital.

In this regulatory exception, we also interpreted the statutory limitations that the disclosure be to ''another person similarly situated at the same facility'' to mean that the disclosure be to another person authorized to access protected health information (even if the two persons may not be authorized to access the same types of protected health information) at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates (even if the covered entity, business associate, or organized health care arrangement has multiple facilities or locations across the country).

Finally, to implement section 13400(1)(A) of the Act, the interim final rule exempted disclosures of protected health information where a covered entity or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information. For example, if a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals and a few of the EOBs are returned by the post office, unopened, as undeliverable, the covered entity can conclude that the improper addressees could not reasonably have retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches. As another example, if a nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the protected health information from the patient, this would not constitute a breach if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information.

With respect to any of the three exceptions discussed above, a covered entity or business associate has the burden of proof, pursuant to § 164.414(b) (discussed below), for showing why breach notification was not required. Accordingly, the covered entity or business associate must document why the impermissible use or disclosure falls under one of the above exceptions.

Overview of Public Comments

Of the approximately 85 public comments received on the interim final rule addressing the definition of breach, approximately 70 of those comments addressed the harm standard and risk assessment approach in the interim final rule. We received approximately 60 comments in support of the harm standard and the risk assessment approach. The commenters in support of this approach included providers, health plans, professional associations, and certain members of Congress. These commenters argued that the inclusion of the harm standard and accompanying risk assessment was consistent with the statutory language, aligned the interim final rule with many State breach notification laws and Federal policies, and appropriately placed the obligation to determine if a breach had occurred on covered entities and business associates since they had the requisite knowledge of the incident to best assess the likely impact of the impermissible use or disclosure.

The proponents of the harm standard and risk assessment approach also argued that its removal would increase the cost and burden of implementing the rule for covered entities, business associates, as well as HHS, and may cause unnecessary anxiety and eventual

apathy among consumers if notifications are sent when there is no risk of harm to the individual.

We also received approximately 10 comments opposed to the harm standard. Generally, the commenters opposed to this approach were members of Congress and consumer advocacy groups. Some opponents of the harm standard argued that its addition to the interim final rule set too high a bar for triggering breach notification, which was contrary to statutory intent. These commenters argued that the final rule should adopt a bright line standard for breach notification to ensure that individuals are aware of all impermissible uses and disclosures of their health information regardless of the potential risk and to make implementation and enforcement of the rule more uniform by removing the discretion and judgment given to covered entities in the interim final rule. These commenters argued that such transparency would better breed consumer trust and would allow individuals to assess the risk of harm themselves and take necessary measures to mitigate an impermissible use or disclosure of their health information.

Other commenters, while opposed to a harm standard to trigger breach notification, nonetheless agreed that breach notification should not be required following every impermissible use or disclosure of unsecured protected health information no matter how inconsequential the breach. These commenters argued that, rather than a subjective standard measuring the risk of harm to an individual, the final rule should include a more objective standard against which entities would be required to assess risk. These commenters suggested that the risk assessment should focus on the risk that the protected health information was compromised instead of on the risk of harm to the individual. Additionally, these commenters proposed four factors that should be considered to determine whether the information was compromised: (1) To whom the information was impermissibly disclosed; (2) whether the information was actually accessed or viewed; (3) the potential ability of the recipient to identify the subjects of the data; and (4) in cases where the recipient is the disclosing covered entity's business associate or is another covered entity, whether the recipient took appropriate mitigating action.

Some commenters stated that the default function of the rule was unclear. In particular, these commenters questioned whether the rule required notification of a breach unless it is determined that a significant risk of harm does not exist, or alternatively, required notification only in cases where significant risk of harm can be demonstrated. Other commenters suggested that we include in the definition an express presumption of a breach unless an entity can show otherwise.

Additionally, many commenters responded to the treatment of limited data sets in the interim final rule. Although many commenters expressed support for the assertion that limited data sets that do not contain dates of birth and zip codes do not compromise the security or privacy of protected health information, most of these commenters expressed concern that the interim final rule did not go far enough and should exempt even those limited data sets that contain dates of birth and/or zip codes from the breach notification requirements. These commenters argued that no impermissible use or disclosure of a limited data set should trigger breach notification obligations because without the 16 direct identifiers that the Privacy Rule requires to be stripped from the information, there is minimal risk of harm to the individual. Additionally, commenters indicated it would be costly and burdensome for entities to have to re-identify the information in a limited data set to provide notification and that re-identifying the information could also pose an additional risk of harm to the affected individuals. Finally, other commenters noted that because researchers commonly rely on limited data sets that contain dates of birth and zip codes, researchers would not be able to take advantage of the exception for certain limited data sets in the interim final rule, which may have the effect of deterring research.

In contrast, some commenters expressed concern regarding the inclusion of even the limited exception to the definition of breach for limited data sets that do not include dates of birth and zip codes. These commenters supported requiring entities to perform a risk assessment to determine whether an impermissible use or disclosure of such information compromised the security or privacy of the information, as there may be a risk of re-identification of this information depending on who received the information.

Final Rule

After considering the public comments on the definition, the Department in this final rule amends the definition of ''breach'' at 45 CFR 164.402. Based on the comments, we recognize that the language used in the interim final rule and its preamble could be construed and implemented in manners we had not intended. Accordingly, this final rule modifies and clarifies the definition of breach and the risk assessment approach outlined in the interim final rule.

First, we have added language to the definition of breach to clarify that an impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised. We recognize that some persons may have interpreted the risk of harm standard in the interim final rule as setting a much higher threshold for breach notification than we intended to set. As a result, we have clarified our position that breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised (or one of the other exceptions to the definition of breach applies). We believe that the express statement of this presumption in the final rule will help ensure that all covered entities and business associates interpret and apply the regulation in a uniform manner and also responds to commenters that indicated the default function of the rule was unclear. This new language is also consistent with § 164.414, which provides that covered entities and business associates have the burden of proof to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach (such as by demonstrating through a risk assessment that there was a low probability that the protected health information had been compromised) and must maintain documentation sufficient to meet that burden of proof.

Second, to further ensure that this provision is applied uniformly and objectively by covered entities and business associates, we have removed the harm standard and modified the risk assessment to focus more objectively on the risk that the protected health information has been compromised. Thus, breach notification is not required under the final rule if a covered entity or business associate, as applicable, demonstrates through a risk assessment that there is a low probability that the protected health information has been compromised, rather than demonstrate that there is no significant risk of harm to the individual as was provided under

the interim final rule. The final rule also identifies the more objective factors covered entities and business associates must consider when performing a risk assessment to determine if the protected health information has been compromised and breach notification is necessary.

Although some commenters urged us to implement a bright line standard, requiring notification for all impermissible uses and disclosures without any assessment of risk, we believe that a risk assessment is necessary. The statute acknowledges, by including a specific definition of breach and identifying exceptions to this definition, as well as by providing that an unauthorized acquisition, access, use, or disclosure of protected health information must compromise the security or privacy of such information to be a breach, that there are several situations in which unauthorized acquisition, access, use, or disclosure of protected health information is so inconsequential that it does not warrant notification. In addition to the statutory exceptions that have been included in both the interim final rule and this final rule, there may be other similar situations that do not warrant breach notification. We agree with commenters that providing notification in such cases may cause the individual unnecessary anxiety or even eventual apathy if notifications of these types of incidents are sent routinely. For example, if a covered entity misdirects a fax containing protected health information to the wrong physician practice, and upon receipt, the receiving physician calls the covered entity to say he has received the fax in error and has destroyed it, the covered entity may be able to demonstrate after performing a risk assessment that there is a low risk that the protected health information has been compromised. Although this scenario does not fit into any of the statutory or regulatory exceptions, we believe that, like the exceptions to breach, notification should not be required if the covered entity demonstrates a low probability that the data has been compromised.

Commenters argued that a rule containing a bright line standard for notification would be easier for both the regulated entities to implement and for HHS to enforce. We disagree. Although a rule that required notification following every impermissible use or disclosure may appear easier for covered entities and business associates to implement—as no determination of the risk that the protected health information has been compromised would be required—in effect, a bright line standard would be extremely burdensome and costly for entities to implement. With no risk assessment following an impermissible use or disclosure, entities may be required to provide many notices each year for incidents that did not compromise the security or privacy of an individual's protected health information.

Although we do not believe a bright line approach to breach notification is appropriate, we do agree with the commenters who expressed concern that the risk assessment focus on ''harm to an individual'' in the interim final rule was too subjective and would lead to inconsistent interpretations and results across covered entities and business associates. As a result, instead of assessing the risk of harm to the individual, covered entities and business associates must assess the probability that the protected health information has been compromised based on a risk assessment that considers at least the following factors: (1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the protected health information or to whom the disclosure was made; (3) whether the protected health information was actually acquired or viewed; and (4) the extent to which the risk to the protected health information has been mitigated. We believe that the use of these factors, which are derived from the factors listed in the interim final rule as well as many of the factors suggested by commenters, will result in a more objective evaluation of the risk to the protected health information and a more uniform application of the rule.

As we have modified and incorporated the factors that must be considered when performing a risk assessment into the regulatory text, covered entities and business associates should examine their policies to ensure that when evaluating the risk of an impermissible use or disclosure they consider all of the required factors. In addition, given the circumstances of the impermissible use or disclosure, additional factors may need to be considered to appropriately assess the risk that the protected health information has been compromised. We note that, although we have included this risk assessment in the final rule, this type of assessment of risk should not be a new or different exercise for covered entities and business associates. Similar assessments of risk that data have been compromised must be performed routinely following security breaches and to comply with certain State breach notification laws.

The first factor requires covered entities and business associates to evaluate the nature and the extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification of the information. To assess this factor, entities should consider the type of protected health information involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature. For example, with respect to financial information, this includes credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. With respect to clinical information, this may involve considering not only the nature of the services or other information [11] but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results). Considering the type of protected health information involved in the impermissible use or disclosure will help entities determine the probability that the protected health information could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests. Additionally, in situations where there are few, if any, direct identifiers in the information impermissibly used or disclosed, entities should determine whether there is a likelihood that the protected health information released could be re-identified based on the context and the ability to link the information with other available information.[12] For example, if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers, the protected health information is obviously identifiable, and a risk assessment likely would determine that there is more than a low probability that the information has been compromised, dependent on an assessment of the other factors discussed below. Alternatively, if the covered entity disclosed a list of patient discharge dates and diagnoses, the

[11] We caution that many forms of health information, not just information about sexually transmitted diseases or mental health or substance abuse, are sensitive.

[12] Information that has been de-identified in accordance with 45 CFR 164.514(a)–(c) is not protected health information, and thus, any inadvertent or unauthorized use or disclosure of such information is not considered a breach for purposes of this rule.

entity would need to consider whether any of the individuals could be identified based on the specificity of the diagnosis, the size of the community served by the covered entity, or whether the unauthorized recipient of the information may have the ability to combine the information with other available information to re-identify the affected individuals (considering this factor in combination with the second factor discussed below). We emphasize, however, that the entity must evaluate all the factors, including those discussed below, before making a determination about the probability of risk that the protected health information has been compromised.

The second factor requires covered entities and business associates to consider the unauthorized person who impermissibly used the protected health information or to whom the impermissible disclosure was made. Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information. For example, as discussed in the interim final rule, if protected health information is impermissibly disclosed to another entity obligated to abide by the HIPAA Privacy and Security Rules or to a Federal agency obligated to comply with the Privacy Act of 1974 and the Federal Information Security Management Act of 2002, there may be a lower probability that the protected health information has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity. We also emphasize that this factor should be considered in combination with the factor discussed above regarding the risk of re-identification. If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the protected health information has the ability to re-identify the information. For example, if information containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the protected health information has been compromised.

Several commenters suggested that a risk assessment need be completed following only impermissible disclosures of protected health information, since information impermissibly ''used'' remains within the covered entity or business associate. We disagree. The final rule requires a risk assessment to be performed following both impermissible uses and disclosures (that do not otherwise fall within the other enumerated exceptions to breach). However, the fact that information only is impermissibly used within a covered entity or business associate and the impermissible use does not result in further impermissible disclosure outside the entity, is something that may be taken into account in conducting the risk assessment and may reduce the probability that the protected health information has been compromised.

The third factor requires covered entities and business associates to investigate an impermissible use or disclosure to determine if the protected health information was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed. For example, as we discussed in the interim final rule, if a laptop computer was stolen and later recovered and a forensic analysis shows that the protected health information on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed. In contrast, however, if a covered entity mailed information to the wrong individual who opened the envelope and called the entity to say that she received the information in error, then, in this case, the unauthorized recipient viewed and acquired the information because she opened and read the information to the extent that she recognized it was mailed to her in error.

The final factor included in the final rule requires covered entities and business associates to consider the extent to which the risk to the protected health information has been mitigated. Covered entities and business associates should attempt to mitigate the risks to the protected health information following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the protected health information has been compromised. We note that this factor, when considered in combination with the factor regarding the unauthorized recipient of the information discussed above, may lead to different results in terms of the risk to the protected health information. For example, a covered entity may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the entity or person destroyed information it received in error, while such assurances from certain third parties may not be sufficient. As described above, certain commenters suggested that mitigation should only be considered where the recipient of the information is a business associate of the covered entity or another covered entity. We do not in this rule limit this factor to those circumstances but, as discussed above, acknowledge that the recipient of the information will have an impact on whether the covered entity can conclude that an impermissible use or disclosure has been appropriately mitigated.

A covered entity's or business associate's analysis of the probability that protected health information has been compromised following an impermissible use or disclosure must address each factor discussed above. Other factors may also be considered where necessary. Covered entities and business associates must then evaluate the overall probability that the protected health information has been compromised by considering all the factors in combination, and we expect these risk assessments to be thorough, completed in good faith, and for the conclusions reached to be reasonable. If an evaluation of the factors discussed above fails to demonstrate that there is a low probability that the protected health information has been compromised, breach notification is required. We do note, however, that a covered entity or business associate has the discretion to provide the required notifications following an impermissible use or disclosure of protected health information without performing a risk assessment. Because the final rule clarifies the presumption that a breach has occurred following every impermissible use or disclosure of protected health information, entities may decide to notify without evaluation of the probability that the protected health information has been compromised. In the future, we will issue additional guidance to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios.

In addition to the removal of the harm standard and the creation of more objective factors to evaluate the probability that protected health information has been compromised, we have removed the exception for limited data sets that do not contain any dates of birth and zip codes. In the final rule, following the impermissible use or disclosure of any limited data set, a covered entity or business associate must perform a risk assessment that evaluates the factors discussed above to determine if breach notification is not required.

The vast majority of commenters were not supportive of the exception for certain limited data sets outlined in the interim final rule, either because they believed the exception did not go far enough and would chill research that needed access to birth dates and zip codes in limited data sets, or because of concerns regarding the re-identifiability of the limited information to which the exception applied. Based on the comments, we believe it is appropriate to require the impermissible use or disclosure of a limited data set, even those that do not contain dates of birth and zip codes, to be subject to a risk assessment to demonstrate that breach notification is not required. The final rule expressly includes a factor that would require consideration of the re-identifiability of the information, as well a factor that requires an assessment of the unauthorized person who used the protected health information or to whom the disclosure was made (i.e., whether this person has the ability to re-identify the affected individuals). Thus, the factors are particularly suited to address the probability that a data set without direct identifiers has been compromised following an impermissible use or disclosure. Further, we believe in most cases that the result would be the same under this final rule as under the interim final rule with respect to whether an impermissible use or disclosure of a limited data set that also excludes dates of birth and zip codes constitutes a breach for which notification is required. Due to the lack of identifiers present in the protected health information, entities may reasonably determine that there is a low probability of risk that the information has been compromised; however, we stress that this is a fact specific determination to be made based on the circumstances of the impermissible use or disclosure.

We encourage covered entities and business associates to take advantage of the safe harbor provision of the breach notification rule by encrypting limited data sets and other protected health information pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (74 FR 42740, 42742). If protected health information is encrypted pursuant to this guidance, then no breach notification is required following an impermissible use or disclosure of the information.

In addition to the comments discussed above, it was suggested that covered entities be required to include in their notice of privacy practices information about how a risk assessment will be conducted or their internal policies for determining whether a breach has occurred and notification is warranted. It was also suggested that the breach notice to the individual following discovery of a breach of unsecured protected health information contain information about the covered entity or business associate's risk assessment to help the individual better assess the level of threat posed by the breach and to better determine the appropriate steps, if any, to take.

We decline to require that the covered entity's notice of privacy practices include a description of how a risk assessment will be conducted, although covered entities may include such information in their notice of privacy practices if they choose. While each risk assessment will differ depending on the specific facts and circumstances surrounding the impermissible use or disclosure, we believe that the modifications in this final rule will help ensure that covered entities and business associates perform risk assessments more uniformly and objectively. We also note that the content requirements for the notice to the individual outlined in § 164.404(c) already require that the individual be notified of the circumstances of a breach, as well as what steps individuals should take to protect themselves from potential harm resulting from the breach.

One commenter suggested that we require a covered entity to hire an independent organization to assess the risk of an impermissible use or disclosure to determine if breach notification is required. We do not believe such a requirement is necessary, although covered entities are free to engage independent organizations to assist in making such determinations provided that, if access to protected health information is required, business associate agreements are entered into to protect the information. Further, we believe the modifications in this final rule are conducive to more uniform risk assessments across covered entities and business associates. Additionally, as with the interim final rule, we note that covered entities and business associates have the burden of proof, pursuant to § 164.414, to demonstrate that all notifications were provided or that an impermissible use or disclosure did not constitute a breach and to maintain documentation (e.g., of the risk assessment demonstrating that there was a low probability that the protected health information had been compromised or of the assessment that the impermissible use or disclosure falls within one of the other exceptions to breach), pursuant to 45 CFR 164.530(j)(1)(iv), as necessary to meet this burden of proof. Thus, covered entities and business associates have adequate incentive to conduct reasonable and diligent risk assessments.

Finally, after reviewing and considering the comments received regarding the exceptions to the definition of breach in the interim final rule, the Department adopts these exceptions without modification in this final rule. Although the substance of these exceptions has not changed, these exceptions are now located at paragraph (1) of the definition of breach instead of paragraph (2) to accommodate the modifications discussed above. We respond to the public comments addressing these exceptions, as well as other comments received on the definition of ''breach,'' below.

Response to Other Public Comments

Comment: Many commenters expressed concern that violations of the minimum necessary standard may trigger breach notification obligations.

Response: We do not believe it would be appropriate to exempt minimum necessary violations from the breach notification obligations as we do not believe that all minimum necessary violations present a low probability that the protected health information has been compromised. Thus, uses or disclosures that impermissibly involve more than the minimum necessary information, in violation of §§ 164.502(b) and 164.514(d), may qualify as breaches. Such incidents must be evaluated as any other impermissible uses or disclosures to determine whether breach notification is not required.

As explained above, there are several factors to be considered when determining the probability that the protected health information involved in an impermissible use or disclosure has been compromised, including the

unauthorized person who used the information or to whom the disclosure was made. Thus, where a minimum necessary violation occurs in a disclosure to a business associate or as an internal use within a covered entity or business associate, the fact that the information was not acquired by a third party would be considered as part of the risk assessment and may help lead to the conclusion that there is a low probability that the protected health information has been compromised. Alternatively, covered entities and business associates may determine that certain minimum necessary violations fall within the exceptions to the definition of breach at § 164.402(1)(i) or (1)(ii).

We note that the Privacy Rule's minimum necessary standard requires a covered entity to make reasonable efforts to limit access to protected health information to those persons or classes of persons who need access to protected health information to carry out their duties and to disclose an amount of protected health information reasonably necessary to achieve the purpose of a disclosure. The Privacy Rule requires covered entities to determine and define in their policies and procedures how the minimum necessary standard applies to their own uses and disclosures. Thus, covered entities are in a good position to know when such policies and procedures have been violated and to assess the probability that the incident has compromised the security or privacy of the information. Finally, we will consider including further guidance regarding the interaction between the minimum necessary standard and the breach notification requirements in the guidance required by section 13405(b)(1)(B) of the HITECH Act.

Comment: Several commenters asked that we clarify the differences between ''acquisition,'' ''access,'' ''use,'' and ''disclosure'' in the exceptions in the final rule. These commenters expressed confusion regarding the use of these terms in the first two exceptions to the definition of breach, stating that the term ''acquisition'' connotes a disclosure of information, and thus, the exception regarding unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate implicitly includes disclosures of protected health information.

Response: While the Privacy Rule uses the terms ''use'' and ''disclosure,'' we included both ''acquisition'' and ''access'' in the regulatory text for consistency with the statutory language. We interpret ''acquisition'' and ''access'' to information based on their plain meanings and believe that both terms are encompassed within the current definitions of ''use'' and ''disclosure'' in the HIPAA Rules. For example, an acquisition may be a ''use'' or ''disclosure'' depending on who acquired the information—i.e., a workforce member or someone outside the covered entity, such as a business associate.

Comment: Several commenters supported our interpretations of the statutory terms ''employee,'' ''same facility,'' and ''similarly situated individual'' with respect to the exceptions to the definition of breach.

Response: We retain these clarifications in this final rule.

Comment: Some commenters asked that we use the term ''use'' instead of ''disclosure'' to describe the type of information exchange contemplated by the exception for certain inadvertent disclosures among persons similarly authorized to access protected health information at a covered entity or business associate since the information must be shared within a covered entity or business associate for the exception to apply.

Response: We clarify that the exception at paragraph (1)(ii) of the definition of ''breach'' is intended to apply to certain ''disclosures'' that may occur ''at'' a covered entity, business associate, or organized health care arrangement in which the covered entity participates—e.g., to persons onsite at a covered entity's facility that are not workforce members, such as physicians with staff privileges at a hospital. For impermissible ''uses'' of protected health information among workforce members of a covered entity or a business associate, a covered entity or business associate should determine whether the exception to breach at paragraph (1)(i) regarding certain unintentional acquisition, access, or use by a workforce member or person acting under the authority of a covered entity or business associate applies.

Comment: One commenter asked if breach notification is required in cases where an impermissible use or disclosure originally qualifies for either of the exceptions to breach at § 164.402(1)(i) or (1)(ii) at the time the incident occurs but later no longer fits within the exception because the protected health information is further used or disclosed in an impermissible manner.

Response: The applicability of an exception to breach must be judged at the time the incident is discovered and evaluated. If an exception to breach is determined to apply such that notification is not warranted, the inquiry into that breach ends; however, the covered entity or business associate should take appropriate steps to ensure that the information is not further used or disclosed impermissibly. If, sometime after making the determination that the exception applied, the information is impermissibly used or disclosed, the covered entity or business associate should treat that incident as a separate impermissible use or disclosure that warrants evaluation as a breach on its own. As explained more fully below, we treat a breach as having occurred at the time of the impermissible use or disclosure, which in the case of the first two exceptions to breach, is at the time of the ''further'' impermissible use or disclosure.

Comment: One commenter asked that we broaden the application of the inadvertent disclosure exception to apply to all routine disclosures between covered entities. Other commenters asked that the rule exempt from the breach notification obligations situations in which a covered entity discloses information to a business associate or another covered entity. Commenters noted that because covered entities and business associates are required to protect the privacy of protected health information, there is little risk that even an impermissible disclosure between such entities would compromise the security or privacy of the information.

Response: We do not agree that such situations warrant a blanket exception from the breach notification rules. In appropriate cases, some of these impermissible disclosures among covered entities and covered entities and business associates may fall within the existing exceptions to breach at paragraphs (1)(i) and (ii) of the definition. Otherwise, such disclosures must be evaluated as to the probability that the protected health information has been compromised based on a risk assessment of a number of factors. While the fact that the recipient of an impermissible disclosure is a covered entity or business associate with obligations to protect the privacy and security of protected health information is a consideration with respect to assessing the risk that the protected health information has been compromised, it is not the only factor. For example, a covered entity or business associate must also evaluate the extent to which the risk to the protected health information has been mitigated.

Comment: Several commenters suggested that the exceptions to breach should not apply to situations where

workforce members or employees further use or disclose information they unintentionally or inadvertently acquired, accessed, or used, even if such further use or disclosure is permitted under the Privacy Rule. Additionally, these commenters suggested that the breach exceptions should apply only in cases in which the workforce member or employee has taken appropriate steps to mitigate the unintentional acquisition, access, or use of protected health information, such as by alerting the sender of the misdirected information, if applicable, and returning or destroying it.

Response: We do not believe it is appropriate to prohibit the sharing of protected health information for permissible purposes following an unintentional or inadvertent error by a workforce member or an employee. Doing so would restrict access and disclosure of the protected health information for necessary treatment and other important purposes to the extent the workforce member or employee needed access to the information in the future for authorized purposes, which would adversely affect health care delivery. We believe that the rule strikes an appropriate balance by not allowing workforce member errors to be excepted from the definition of breach in cases where the workforce member takes the information he or she has mistakenly obtained and then misuses it.

With respect to requiring workforce members or employees to take appropriate steps to mitigate their unintentional access to protected health information, we note that the Privacy Rule already requires covered entities to ensure as part of their minimum necessary policies and procedures that workforce members have appropriate access to protected health information. Therefore, covered entities should ensure that workforce members who gain access in an unauthorized manner to protected health information do not continue to have such unauthorized access. This may require having policies which require workforce members to return or destroy the information to which they obtained unauthorized access. Further, covered entities must implement reasonable safeguards to protect against impermissible uses and disclosures, including further impermissible uses and disclosures by a workforce member who has gained unauthorized access to protected health information.

Comment: One commenter asked that we include an exception in the final rule for situations in which a laptop is lost and recovered and a forensic analysis shows that the protected health information on the computer was not accessed. The commenter stated that because the forensic analysis showed that the information was not compromised, a risk assessment should not be required.

Response: We do not include an explicit exception for this particular scenario. As we explained above, in cases where a lost laptop is recovered, the fact that a forensic analysis of the computer shows that its information was not accessed is a relevant consideration for the risk assessment, and entities in such situations may be able to demonstrate a low probability that the information has been compromised. However, covered entities and business associates still must document their risk assessments in these cases. We also note, as we did in the interim final rule, if a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered.

Comment: Some commenters asked that we create an exception to breach to cover certain routine impermissible disclosures of protected health information. For example, commenters asked that we except from notification disclosures made as a result of the covered entity mailing information to a patient's old address, faxing information to the wrong number, disclosures made as a result of leaving a voice message at the wrong number reminding a patient of an upcoming appointment, or, in situations where patients have identical or similar names, contacting the wrong patient to inform him or her that lab results were ready.

Response: We decline to create such an exception. The ability of a covered entity or business associate to demonstrate that a particular situation poses a low probability that the protected health information was compromised is very fact specific and will depend on an assessment of all of the factors discussed above, such as to whom the information was disclosed, what information was disclosed, and what mitigation has taken place. We also note that, in some cases, some of the situations contemplated by the commenters may fall within an existing exception. For example, if a covered entity mails protected health information about an individual to a wrong address, the impermissible disclosure may fall into the exception at paragraph (1)(iii) of the definition of breach if the information is returned, undelivered and unopened, to the covered entity, such that an unauthorized recipient could not reasonably have retained the information. If, however, the information was not returned or if the covered entity was informed by the unauthorized recipient that he had received and opened the mail in error, the covered entity would need to complete a risk assessment to determine the probability that the protected health information had been compromised as a result of the impermissible disclosure.

Comment: Several commenters asked that we harmonize the final rule with the FTC's Health Breach Notification final rule.

Response: Although the FTC and HHS breach notification rules generally apply to different entities, HHS has worked closely with the FTC to ensure both sets of regulations were harmonized to the greatest extent possible by including the same or similar requirements within the constraints of the statutory language. In addition, in the few situations where an entity provides PHRs to customers of a HIPAA covered entity through a business associate arrangement but also provides PHRs directly to the public and a breach of its records occurs, in certain cases, the FTC will deem compliance with certain provisions of HHS' rule as compliance with FTC's rule. See 74 FR 42964. In particular, in such situations, it may be appropriate for the vendor to provide the same breach notice to all its PHR customers since it has a direct relationship with all the affected individuals. Thus, in those limited circumstances where a vendor of PHRs (1) provides notice to individuals on behalf of a HIPAA covered entity, (2) has dealt directly with these individuals in managing their PHR accounts, and (3) provides notice to its customers at the same time, the FTC will deem compliance with HHS requirements governing the timing, method, and content of notice to be compliance with the corresponding FTC rule provisions. Note, however, that the PHR vendor still must comply with all other FTC rule requirements, including the requirement to notify the FTC within ten business days after discovering the breach.

b. Definition of ''Unsecured Protected Health Information''

Interim Final Rule

Section 13402(h)(1)(A) of the Act defines ''unsecured protected health information'' as ''protected health information'' that is not secured through the use of a technology or methodology specified by the Secretary in guidance issued under [section 13402(h)(2)].'' The Act at section 13402(h)(2) requires that the Secretary specify in the guidance the technologies and methodologies that

render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Accordingly, the interim final rule defined ''unsecured protected health information'' as protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance. This guidance, which was published in updated form within the preamble to the interim final rule and made available on the HHS Web site, specifies that only encryption and destruction, consistent with National Institute of Standards and Technology (NIST) guidelines, renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals such that notification is not required in the event of a breach of such information.

Overview of Public Comments

While we received a number of technical and other comments on the guidance, we did not receive any comments on the language of the above definition itself. We intend to address the comments on the guidance in our next update to the guidance.

Final Rule

The final rule modifies the interim final rule's definition of ''unsecured protected health information'' to replace the term ''unauthorized individuals'' in the definition with ''unauthorized persons.'' The term ''individual'' is defined in § 160.103 to mean the person who is the subject of the protected health information, which is not what is intended with the reference to ''individual'' in the definition of ''unsecured protected health information.'' Accordingly, the final rule uses more appropriately the term ''unauthorized persons.'' The final rule also modifies the definition to remove the term ''on the HHS Web site'' as unnecessary language. While we remove the reference to the HHS Web site from the regulatory text, we do plan to continue to post updates to the guidance on the Web site as they are issued.

2. Section 164.404—Notification to Individuals

Interim Final Rule

Section 13402(a) of the Act provides that a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, in the case of a breach of such information that is discovered by the covered entity, notify each affected individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach. Accordingly, § 164.404(a)(1) of the interim final rule included the general rule that a covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of such breach.

Breaches Treated as Discovered

Section 13402(c) of the HITECH Act states that a breach shall be treated as discovered by a covered entity or business associate as of the first day on which such breach is known or should reasonably have been known to the covered entity or business associate. The Act also specifies that this discovery is triggered as soon as any person, other than the individual committing the breach, who is an employee, officer, or other agent of the covered entity or business associate knows or should reasonably have known of the breach.

Section 164.404(a)(2) of the interim final rule implemented the Act's discovery provision, with respect to covered entities by stating that a breach shall be treated as discovered by a covered entity on the first day the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity. The interim final rule incorporated the term ''by exercising reasonable diligence,'' which is used in the HIPAA Enforcement Rule and defined to mean the ''business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.''

Section 164.404(a)(2) of the interim final rule further provided, in accordance with the Act, that a covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person other than the person committing the breach, who is a workforce member or agent of the covered entity. Thus, the breach is treated as discovered by the covered entity at the time the workforce member or other agent has knowledge of the breach. The rule also clarified that the federal common law of agency controls in determining who is an agent of the covered entity, which is consistent with how agency liability is determined under the HIPAA Rules.

Overview of Public Comments

Several commenters argued that a breach should be treated as discovered by a covered entity only after management has been notified of the incident. Commenters stated that the Department should not hold an entity responsible for knowing of a breach if an appropriately trained employee fails to inform the proper persons within the entity of a breach. Other commenters asked for guidance and more clarification regarding what it means for a covered entity or business associate to be exercising reasonable diligence, such as what frequency of monitoring for breaches is expected or what types of systems must covered entities and business associates have in place to detect breaches.

Final Rule

We retain § 164.404(a)(2) in this final rule without modification. We decline to adopt the suggestion that a covered entity be deemed to have discovered a breach only when management is notified of the breach. The HITECH Act itself provides that a breach is to be treated as discovered by a covered entity or business associate if ''any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate'' knows or should reasonably have known of the breach. This concept is also consistent with the HIPAA Enforcement Rule and the Federal common law of agency. We encourage covered entities and business associates to ensure their workforce members and other agents are adequately trained on the importance of prompt reporting of privacy and security incidents.

With respect to those commenters asking for guidance on what it means for a covered entity to be exercising reasonable diligence, we note that the term reasonable diligence, as defined in § 160.401, means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances. The determination of whether a person acted with reasonable diligence is generally a factual one, since what is reasonable depends on the circumstances. Factors to be considered include whether a covered entity or business associate took reasonable steps to learn of breaches and whether there were indications of breaches that a person seeking to satisfy the Rule would have investigated under similar circumstances. Covered entities and business associates may wish to look to how other covered entities and business associates operating under

similar circumstances conduct themselves for a standard of practice.

Timeliness

Section 13402(d) of the Act and the implementing regulations at § 164.404(b) require covered entities to notify individuals of a breach without unreasonable delay but in no case later than 60 calendar days from the discovery of the breach, except in certain circumstances where law enforcement has requested a delay. Under this rule, the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule. A covered entity is expected to make the individual notifications as soon as reasonably possible after the covered entity takes a reasonable time to investigate the circumstances surrounding the breach in order to collect and develop the information required to be included in the notice to the individual. The 60 days is an outer limit and therefore, in some cases, it may be an ''unreasonable delay'' to wait until the 60th day to provide notification.

Overview of Public Comments

While some commenters generally were supportive of this provision in the interim final rule, others argued that the 60-day timeframe for notification to individuals is unreasonable and requested more time, such as 120 days, to provide the notifications. Some commenters argued that the clock on the 60-day timeframe should not begin to run until after a covered entity has completed its investigation and determined that a breach has occurred. Another commenter expressed the need for clarification about the types of delays in notifying individuals that would be considered reasonable and whether a covered entity's resources would be taken into account in determining whether any delay was reasonable.

Final Rule

We retain § 164.404(b) in this final rule without modification. This is the standard expressly provided for in the statute and we otherwise do not believe it necessary or prudent to extend the timeframe. Covered entities and business associates have been operating under this timeliness standard since the issuance of the interim final rule and we believe a longer time period to notify individuals of breaches of unsecured protected health information could adversely impact affected individuals and the ability to mitigate adverse consequences. For the same reasons, we continue to provide that the time period begins to run when the incident becomes known, not when it is determined that a breach as defined by the rule has occurred. There is sufficient time within this standard both to conduct a prompt investigation of the incident and to notify affected individuals.

With respect to what constitutes a reasonable versus unreasonable delay within the 60-day timeframe, such determinations are fact specific and there are many factors that may be relevant, including the nature of the breach, number of individuals affected, and resources of the covered entity.

Content of the Notification

Section 13402(f) of the HITECH Act set forth the content requirements for the breach notice to the individual. Section 164.404(c) of the interim final rule incorporated the statutory elements, requiring the following information be included in the notices, to the extent possible: (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (3) any steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity involved is doing to investigate the breach, mitigate the harm to individuals, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

The interim final rule added the term ''diagnosis,'' to the parenthetical listing of examples of types of protected health information, which was not in the statute, to make clear that, where appropriate, a covered entity may need to indicate in the notification to the individual whether and what types of treatment information were involved in a breach. In addition, with respect to a covered entity's mitigation, the interim final rule replaced the statutory term ''mitigate losses'' with ''mitigate harm to individuals'' to make clear that the notification should describe the steps the covered entity is taking to mitigate potential harm to individuals resulting from the breach and that such harm is not limited to economic loss.

To address the readability and accessibility of the notice, the interim final rule made a number of clarifications. First, the Department included in the interim final rule a requirement that the breach notices be written in plain language so that individuals will be able to understand them more easily, which means the notice should be written at an appropriate reading level, using clear language and syntax, and not include any extraneous material that might diminish the message it is trying to convey.

Second, the interim final rule explained that some covered entities may have obligations under other laws with respect to their communication with affected individuals. For example, to the extent a covered entity is obligated to comply with Title VI of the Civil Rights Act of 1964, the covered entity must take reasonable steps to ensure meaningful access for Limited English Proficient persons to the services of the covered entity, which could include translating the notice into frequently encountered languages. Similarly, to the extent that a covered entity is required to comply with Section 504 of the Rehabilitation Act of 1973 or the Americans with Disabilities Act of 1990, the covered entity has an obligation to take steps that may be necessary to ensure effective communication with individuals with disabilities, which could include making the notice available in alternate formats, such as Braille, large print, or audio.

Overview of Public Comments

Several commenters stated that the content requirements for breach notification were too vague. Some commenters asked that we provide templates or sample notices to be used by covered entities. Other commenters asked for more specific guidance about particular required content elements of the notice, such as what information should be provided to individuals about a covered entity's or business associate's mitigation efforts and regarding any employee sanctions, particularly if a company has policies that require certain employment actions be kept confidential. It was also suggested that we publish a list of actions to be included in the notices based on the type of breach with respect to the steps individuals should take to protect themselves from harm. Some commenters also asked that the Department clarify that the requirement

to include ''a brief description of what happened'' would not require the covered entity or business associate to describe how the breach occurred such that it would create a roadmap for future breaches.

Final Rule

We retain § 164.404(c) in this final rule without modification. The content requirements in the Rule generally mirror the content requirements in the statute and each element is an important component of the notice to ensure individuals receive the information they need to protect themselves to the extent possible from the consequences of a breach and to learn what is being done to mitigate the breach and prevent future breaches. At the same time, the content provisions are sufficiently flexible to allow covered entities and business associates to tailor the breach notices based on the circumstances surrounding the breach and of the entity. In our experience in administering the Rule since 2009, the Rule provides sufficient flexibility to describe to the individual the circumstances surrounding the breach in a more general manner that still provides the individual with pertinent information but that does not provide a roadmap to third parties for future breaches. For example, the notice need not explain the exact type of vulnerability in the security of a covered entity's electronic records system that led to unauthorized access and how that vulnerability was exploited. Similarly, a covered entity has flexibility in describing what the covered entity is doing in response to a breach. Where employee sanctions are relevant based on the circumstances of the breach, a covered entity may determine that it wants to describe the sanctions imposed more generally and nothing in the Rule would require that the notice include the names of the employees involved. For example, a covered entity may want to indicate generally that the employees involved have been appropriately disciplined, particularly if multiple employees received varying levels of sanctions based on their degrees of involvement in the breach. In other cases, it may benefit the covered entity to be more specific so as to better assure individuals that the entity is appropriately addressing the situation, such as indicating that an employee who improperly accessed and sold patient information was promptly terminated.

With respect to templates, examples, or other guidance, the Department anticipates providing additional guidance in the future.

Methods of Notification

Section 13402(e)(1) of the HITECH Act provides for both actual written notice to affected individuals, as well as substitute notice to affected individuals if contact information is insufficient or out-of-date. Specifically, the statute requires breach notifications to be sent by first-class mail at the last known address of the individual or next of kin if the individual is deceased, or by electronic mail if specified as the preferred method by the individual. The Act also provides that the notification may be provided in one or more mailings as the information becomes available. Where there is insufficient or out-of-date contact information that precludes direct written notice to the individual, the statute requires that a substitute form of notice be provided to the individual. If there is insufficient contact information for 10 or more individuals, the Act requires that the substitute notice be a conspicuous posting on the home page of the covered entity's Web site or notice in major print or broadcast media in the geographic areas where the affected individuals likely reside, and in either case, that a toll-free number be included where individuals can learn whether their information was possibly included in the breach. Finally, the Act provides that a covered entity may provide notice by telephone or other means to individuals, in addition to direct written notice by first-class mail or email, in urgent situations involving possible imminent misuse of the individual's information.

Section 164.404(d) of the interim final rule set forth these methods for providing breach notification to affected individuals. Section 164.404(d)(1)(i) of the interim final rule required a covered entity to provide breach notice to an affected individual in written form by first-class mail at the individual's last known address. The interim final rule also permitted covered entities to provide this written notice in the form of electronic mail if the individual has agreed to receive electronic notice and that agreement has not been withdrawn.

The Department clarified that, consistent with § 164.502(g) of the Privacy Rule, where the individual affected by a breach is a minor or otherwise lacks legal capacity due to a physical or mental condition, notice to the parent or other person who is the personal representative of the individual would satisfy the requirements of § 164.404(d)(1). Additionally, with respect to deceased individuals, the interim final rule at § 164.404(d)(1)(ii) provided that notice of a breach be sent to either the individual's next of kin or personal representative, as such term is used for purposes of the Privacy Rule, recognizing that in some cases, a covered entity may have contact information for a personal representative of a deceased individual rather than the next of kin. To address administrative and privacy concerns with a covered entity being required to obtain contact information for the next of kin of a deceased patient in cases where the individual did not otherwise provide the information while alive, the interim final rule also clarified that a covered entity is only required to provide notice to the next of kin or personal representative if the covered entity both knows the individual is deceased and has the address of the next of kin or personal representative of the decedent.

If a covered entity does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, the interim final rule required a covered entity to provide substitute notice for the unreachable individuals in accordance with § 164.404(d)(2). The interim final rule required that substitute notice be provided as soon as reasonably possible after the covered entity is aware that it has insufficient or out-of-date contact information for one or more affected individuals and that the notice contain all the elements that § 164.404(c) requires be included in the direct written notice to individuals. With respect to decedents, however, the interim final rule provided that a covered entity is not required to provide substitute notice for the next of kin or personal representative in cases where the covered entity either does not have contact information or has out-of-date contact information for the next of kin or personal representative.

Section 164.404(d)(2) of the interim final rule required that, whatever method used, the substitute form of notice be reasonably calculated to reach the individuals for whom it is being provided. If there are fewer than 10 individuals for whom the covered entity has insufficient or out-of-date contact information to provide the written notice, § 164.404(d)(2)(i) of the interim final rule permitted the covered entity to provide substitute notice to such individuals through an alternative form of written notice, by telephone, or other means. For example, if a covered entity learned that the home address it has for one of its patients was out-of-date, but it had the patient's email address or telephone number, it could provide

substitute notice by email (even if the patient had not agreed to electronic notice) or by phone. Alternatively, posting a notice on the Web site of the covered entity or at another location may be appropriate if the covered entity lacks any current contact information for the patients, so long as the posting is done in a manner that is reasonably calculated to reach the individuals.

If a covered entity has insufficient or out-of-date contact information for 10 or more individuals, then § 164.404(d)(2)(ii) of the interim final rule required the covered entity to provide substitute notice through either a conspicuous posting for a period of 90 days on the home page of its Web site or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. For either method involving 10 or more individuals, the covered entity was also required to have a toll-free phone number, active for 90 days, where an individual can learn whether the individual's unsecured protected health information may be included in the breach and to include the number in the notice.

If a covered entity chooses to provide substitute notice on its Web site, the covered entity may provide all the information described at § 164.404(c) directly on its home page (''home page'' includes the home page for visitors to the covered entity's Web site and the landing page or login page for existing account holders) or may provide a prominent hyperlink on its home page to the notice containing such information.

If the covered entity does not have or does not wish to use a Web site for the substitute notice, the interim final rule required the covered entity to provide substitute notice of the breach in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside. What is considered major print or broadcast media for a metropolitan area may be very different from what is considered major print or broadcast media in a rural area, such that the use of local, city, or state-wide media may be appropriate depending on the circumstances. Further, multiple media outlets may need to be utilized to reasonably reach individuals in different regions or States. In any event, substitute media notice, as with substitute Web notice, must be conspicuous and thus, covered entities should consider the location and duration of the notice to ensure the notice is reasonably calculated to reach the affected individuals.

Finally, we clarified that covered entities with out-of-date or insufficient contact information for some individuals can attempt to update the contact information so that they can provide direct written notification, in order to limit the number of individuals for whom substitute notice is required and, thus, potentially avoid the obligation to provide substitute notice through a Web site or major print or broadcast media under § 164.404(d)(2)(ii).

In accordance with the statute, § 164.404(d)(3) makes clear that notice to the individual by telephone or other means may be provided, in addition to the direct written notice required by § 164.404(d)(1), in cases deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information.

Overview of Public Comments

Several commenters questioned which entity has the responsibility for providing notifications to individuals when a breach occurs at or by a business associate and whether a covered entity could delegate its breach notification obligations to a business associate. Some commenters asked about the notification obligations in cases where a covered entity's business associate that experiences a breach is also a covered entity itself. Others requested clarification regarding the obligations for providing breach notification where multiple covered entities and business associates are involved in health information exchange and it may be unclear where a breach occurred and/or which entity has responsibility for the breach.

Additionally, many commenters suggested that covered entities be permitted to provide notification to individuals via telephone or orally instead of via written communication, or at a work address instead of a home address, if the individual has specified one of these alternative methods or locations as preferred for receiving breach notification. Commenters raised potential privacy concerns with communicating with individuals via mail to their home, particularly where the individual has received highly confidential medical services, such as substance abuse or mental health services, and others who may have access to the mail may not otherwise be aware of such condition or treatment. Some commenters argued that because the Privacy Rule requires covered entities to accommodate reasonable requests by individuals to receive communications by alternative means or at alternative locations, the same standard should apply to the provision of breach notification.

Finally, several commenters expressed concern over the substitute notice required in cases in which the covered entity has insufficient or out-of-date contact information for affected individuals. Many of these commenters stated that providing notification via Web posting or media publication is an inappropriate method of providing substitute notice, except in cases in which the covered entity can reasonably define the universe of affected individuals. In other cases, such notice will not give individuals who view the notice enough information to determine if they are affected by a breach, and may cause unaffected individuals unnecessary alarm. Some commenters recommended that covered entities instead be required to use reasonable efforts to identify alternative means of providing direct notice to the affected individuals, such as by phone or email, or to only require substitute media or Web notice when a covered entity cannot reach 10 or more individuals directly by mail, phone, or email. Other commenters argued that the substitute notice requirements, particularly the requirement to establish a toll-free number, may be cost prohibitive to smaller covered entities. It was also suggested that smaller covered entities, particularly those in rural areas, should be allowed to provide substitute notice via handouts or postings at the covered entity's physical location even in cases where the entity has insufficient contact information for more than 10 individuals.

Final Rule

We retain § 164.404(d) in this final rule without modification. In response to questions raised with respect to a breach at or by a business associate, we note that the covered entity ultimately maintains the obligation to notify affected individuals of the breach under § 164.404, although a covered entity is free to delegate the responsibility to the business associate that suffered the breach or to another of its business associates. This is the case even if the breach of the covered entity's protected health information occurred at or by a business associate that is also a covered entity. For example, if a covered provider (Provider A) hires another covered provider's practice (Provider B) as a business associate to perform his billing and other back office functions, and a breach of Provider A's protected health information occurs at Provider B while performing these functions for Provider A, it remains Provider A's responsibility to provide breach notification to the affected individuals, although Provider A may delegate this

responsibility to Provider B as its business associate.

Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

Similarly, when multiple covered entities participate in electronic health information exchange and there is a breach of unsecured protected health information at a Health Information Organization (HIO), the obligation to notify individuals of the breach falls to the covered entities. We recognize that it may be difficult to determine what breached information is attributable to which covered entity's individuals. For example, an HIO may store centralized electronic health records (EHRs) for a community, with each EHR including information generated by multiple covered entities. In such circumstances, it may be necessary for the HIO to notify all potentially affected covered entities and for those covered entities to delegate to the HIO the responsibility of sending the required notifications to the affected individuals. This would avoid the confusion of individuals receiving more than one notification about the same breach.

In response to the commenters who suggested that covered entities be permitted to accommodate reasonable requests by individuals to receive breach notifications by alternative means or at alternative locations, we provide the following guidance. The HITECH Act requires a covered entity to provide breach notification to an affected individual in written form either at the last known address of the individual or email address, if the individual agrees to receive notice electronically, where the covered entity has sufficient contact information to do so. The Act and this rule do not prohibit a covered entity from sending a breach notice to an alternative address rather than a home address, such as a work address or post office box, or the individual's email address of choice, if the individual requests communications be sent to such an address. Further, a covered health care provider (and health plan, if potential endangerment is raised by the individual) is required by the Privacy Rule at § 164.522 to accommodate any such reasonable requests.

In response to those commenters who urged that we allow breach notices to be provided orally or via telephone to individuals receiving highly confidential treatment services where the individual has requested to receive communications in such a manner, we note that the HITECH Act specifically refers to ''written'' notice to be provided to individuals. However, we understand the privacy concerns raised. We, thus, clarify that in the limited circumstances in which an individual has agreed only to receive communications from a covered health care provider orally or by telephone, the provider is permitted under the Rule to telephone the individual to request and have the individual pick up their written breach notice from the provider directly. In cases in which the individual does not agree or wish to travel to the provider to pick up the written breach notice, the health care provider should provide all of the information in the breach notice over the phone to the individual, document that it has done so, and the Department will exercise enforcement discretion in such cases with respect to the ''written notice'' requirement. We stress that our enforcement discretion applies only to cases where the individual affirmatively chooses not to receive communications from a covered health care provider at any written addresses or email addresses, and not to situations where providing telephonic notice is simply less burdensome or easier on a provider and the entity has a valid address, or email address if applicable, on file for the affected individual.

Finally, with respect to commenters who expressed concerns with the substitute media and Web notice provisions of the interim final rule, we emphasize that these are statutory requirements that have been incorporated into the Rule. Section 13402(e)(1)(B) of the HITECH Act expressly requires that a covered entity that has insufficient or out-of-date contact information for 10 or more individuals provide substitute notification to such individuals via posting on their Web site or notification in major print or broadcast media in the areas in which the affected individuals likely reside. Additionally, the statute requires such ''notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.'' Thus, we retain these requirements in this final rule.

Response to Other Public Comments

Comment: One commenter expressed concern about providing breach notification to individuals by first-class mail because it could require some entities, such as those that have Web-based relationships with individuals, to collect more information about individuals (e.g., physical addresses) than they currently do.

Response: The Rule allows a covered entity to provide written breach notice to an affected individual by email if the individual agrees to electronic notice and such agreement has not been withdrawn. We would expect that covered entities that have primarily or solely an online relationship with individuals would ask and encourage individuals to receive breach notices by email and that generally individuals would agree. However, an individual that does not affirmatively agree to receive breach notices by email, or that withdraws a prior agreement, has a right to notice by first-class mail.

Comment: One commenter suggested that we excuse a covered entity from providing notification of a breach to an individual where a licensed health care professional has determined in the exercise of professional judgment that the provision of such notice is likely to cause substantial harm to the individual. The commenter appeared to be concerned due to the nature of the services it provides—mental health services—and the distress breach notification could cause for certain of its patients.

Response: The statute does not include such an exception to the provision of breach notification, and we do not include one in this Rule. An affected individual has a right to be informed of breaches of unsecured protected health information so the individual can take steps if appropriate to protect themselves from the consequences. In situations where a health care provider believes that the provision of written breach notification to an individual may cause extreme anguish or distress, based on the individual's mental state or other circumstances, the provider may telephone the individual prior to the time the breach notice is mailed or have them come into the provider's office to discuss the situation. However, we note that the breach notification must still be mailed without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Where a provider is aware that an individual has a personal representative due to incapacity or other health condition, the breach notification may be sent to the personal representative.

Comment: Many commenters expressed support for allowing covered entities to provide breach notification to a deceased individual's personal representative instead of to the next of

kin. One commenter suggested that we also allow covered entities to provide breach notification to the emergency contact provided by a deceased individual prior to death as this is the information they collect from individuals and yet this person may not be the next of kin or a personal representative of the deceased individual.

Response: We do not believe it appropriate to permit covered entities to send breach notifications to a deceased individual's emergency contact where such person is not a personal representative (such as an executor or administrator of the decedent's estate) or next of kin of the decedent, as such notices may convey information about the decedent's care the decedent never wished the emergency contact to have and/or may go to a person who has no authority to act on the notice.

Comment: To reduce the costs associated with sending breach notifications, one commenter asked that we adopt the Department of Labor's standard for providing COBRA Election Notices to allow a covered entity to: (1) Where a breach affects both a plan participant and the participant's spouse, send one breach notice addressed to both if both spouses reside at the same address; and (2) where a breach affects a dependent child (of any age) under a plan, send a breach notice to either the plan participant and/or the participant's spouse, provided the dependent child resides at the same address. The commenter stated the notice should clearly identify the individuals or classes of individuals to whom the notice applies.

Response: A covered entity is permitted to send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan who are affected by a breach, so long as they all reside at a single address and the covered entity clearly identifies on the notice the individuals to which the notice applies. Further, a covered entity may send a notice regarding the breach of a dependent child's protected health information addressed to the plan participant and/or participant's spouse living with the dependent child, so long as the participant and/or participant's spouse are the personal representatives of the dependent child and the notice clearly identifies to whom it applies. Such notices by first-class mail would meet the written notice requirements of § 164.404(d)(1)(i). However, one breach notice covering both the plan participant and the dependents under the plan mailed to the plan participant's address would not suffice if the address of one or more dependents affected by the breach was different than the participant's address. Further, where a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, a covered entity must address a breach notice to the dependent himself or herself.

Comment: Several commenters expressed support for the acknowledgment in the preamble to the interim final rule that some covered entities may have obligations under Civil Rights laws to ensure that breach notifications are provided to individuals in alternative languages, and in alternative formats, such as Braille, large print, or audio, where appropriate. Some commenters requested additional guidance regarding how to ensure compliance with these laws with respect to breach notifications.

Response: Additional guidance on how to comply with Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, and the Americans with Disabilities Act of 1990, is available on the OCR Web site at *http://www.hhs.gov/ocr/civilrights/*. Further, covered entities with questions on how to comply may contact one of OCR's ten regional offices. Contact information is available at *http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html*.

Comment: Some commenters suggested that the final rule adopt a substitute notification provision similar to that in many State laws that allows for substitute notification, rather than direct written notice, to the individual in the event of breaches affecting a very large number of individuals, such as over 250,000 or 500,000, where the costs of notification would be extremely high.

Response: The Act does not waive direct written notice to the individual when a breach has affected a threshold number of individuals and we do not do so in this rule.

Comment: One commenter requested confirmation that a covered entity could make multiple attempts to provide direct written notice to individuals within the 60-day timeframe before the individual counts towards the 10 or more threshold for providing substitute Web or media notice.

Response: We clarify that a covered entity can attempt to cure out-of-date contact information on individuals when notices are returned as undeliverable by the United States Postal Service to avoid substitute notice so long as a covered entity does so promptly upon receiving the returned notices and no later than 60 calendar days from discovery of the breach. However, at the time the covered entity is aware that it will be unable to reach 10 or more individuals with direct written notice, the covered entity should provide substitute Web or media notice as soon as reasonably possible thereafter, which may be prior to the end of the 60-day period depending on the circumstances.

Comment: One commenter stated that the required content of the breach notice itself, when made available to the public through the Web or media, could lead to the identification of individuals affected by the breach in some cases, undermining the intent of HIPAA's privacy and security protections.

Response: It is unclear the circumstances to which the commenter refers. For example, the notification must include the types of protected health information involved (e.g., social security numbers, dates of birth, full names). However, this is not a requirement to include in the notice the actual names or other identifiers of the affected individuals. We believe covered entities are able to post breach notices in a manner that does not identify particular individuals affected by a breach and thus, must do so.

Comment: One commenter asked that OCR engage in an educational campaign to ensure that covered entities and business associates understand their obligations under the breach notification rule.

Response: Published guidance is the primary method that the Department uses to educate and provide technical assistance to covered entities and business associates. We intend to issue guidance on these requirements in the future as questions are raised or clarifications sought.

3. Section 164.406—Notification to the Media

Section 13402(e)(2) of the HITECH Act, implemented at § 164.406 of the interim final rule, requires that a covered entity provide notice of a breach to prominent media outlets serving a State or jurisdiction, following the discovery of a breach if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach. This media notice is in addition to, not a substitute for, individual notice. In accordance with the Act, § 164.406(b) of the interim final rule required covered entities to notify prominent media outlets without unreasonable delay and in no case later than 60 calendar days after discovery of the breach. Section 164.406(c) of the interim final rule required that the

notification to the media include the same information required to be included in the notification to the individual under § 164.404(c).

The interim final rule did not define ''prominent media outlet'' because what constitutes a prominent media outlet will differ depending upon the State or jurisdiction affected. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole State.

With regard to the term ''State,'' the existing definition of ''State'' at § 160.103 of the HIPAA Rules applies. Section § 160.103 defines ''State'' to mean ''any one of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, and Guam.'' We also expressly provided in the regulation that ''State'' for purposes of notice to the media includes American Samoa and the Northern Mariana Islands, because they were included in the HITECH Act's definition of ''State'' in addition to what appears in the definition at § 160.103. With respect to what was meant by ''jurisdiction'' as opposed to a ''State,'' jurisdiction is a geographic area smaller than a state, such as a county, city, or town.

The interim final rule also clarified that some breaches involving more than 500 individuals who are residents in multiple States may not require notice to the media. For example, if a covered entity discovers a breach of 600 individuals, 200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, the breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media pursuant to § 164.406. However, individual notification under § 164.404 would be required, as would notification to the Secretary under § 164.408 because the breach involved 500 or more individuals.

The Department also recognized that in some cases a breach may occur at a business associate and involve the protected health information of multiple covered entities. In such cases, a covered entity involved would only be required to provide notification to the media if the information breached included the protected health information of more than 500 individuals located in any one State or jurisdiction. For example, if a business associate discovers a breach affecting 800 individuals in a State, the business associate must notify the appropriate covered entity (or covered entities) subject to § 164.410 (discussed below). If 450 of the affected individuals are patients of one covered entity and the remaining 350 are patients of another covered entity, because the breach has not affected more than 500 individuals at either covered entity, there is no obligation to provide notification to the media under this section.

Section 164.406(c) requires that the notice to the media include the same content as that required for notification to the individual under § 164.404(c), and we emphasized that this provision does not replace either direct written or substitute notice to the individual under § 164.404.

Overview of Public Comments

In general, we received few comments on this provision of the interim final rule. One commenter expressed general support for this provision because it does not require the covered entity to incur the cost of printing or running the media notice and asked for clarification that this policy places no requirement on the media to publically report the information provided by a covered entity. Another commenter asked whether a covered entity could fulfill the requirements for providing media notification by posting a press release on the covered entity's Web site.

Final Rule

We retain § 164.406 in this final rule with one minor change. As described in Section IV above, to align the definition of ''State'' in the HIPAA Rules with the definition of the same term used in the HITECH Act, the Department has modified the definition of ''State'' at § 160.103 to include reference to American Samoa and the Northern Mariana Islands. Given this change, it is not necessary to include specific reference to American Samoa and the Northern Mariana Islands at § 164.406 and we remove it in this final rule.

In response to public comments, we clarify that § 164.406 does not require a covered entity to incur any cost to print or run media notice about a breach of unsecured protected health information (unlike the obligations for providing substitute notice to individuals in § 164.404(d)(2) if there is insufficient or out-of-date contact information for 10 or more affected individuals) nor does it obligate prominent media outlets who receive notification of a breach from a covered entity to print or run information about the breach. We also emphasize that posting a press release regarding a breach of unsecured protected health information on the home page of the covered entity's Web site will not fulfill the obligation to provide notice to the media (although covered entities are free to post a press release regarding a breach on their Web site). To fulfill the obligation, notification, which may be in the form of a press release, must be provided directly to prominent media outlets serving the State or jurisdiction where the affected individuals reside.

4. Section 164.408—Notification to the Secretary

Section 13402(e)(3) of the HITECH Act requires covered entities to notify the Secretary of breaches of unsecured protected health information. The Act requires covered entities to report breaches affecting 500 or more individuals to the Secretary immediately. For breaches affecting fewer than 500 individuals, covered entities may maintain a log of all such breaches occurring during the year and annually submit such log to the Secretary.

To implement the statutory provisions, § 164.408(a) contains the general rule that requires a covered entity to notify the Secretary following the discovery of a breach of unsecured protected health information. With respect to breaches involving 500 or more individuals, we interpreted the term ''immediately'' in the statute to require notification be sent to the Secretary concurrently with the notification sent to the individual under § 164.404 (i.e., without unreasonable delay but in no case later than 60 calendar days following discovery of a breach). The rule provided that these notifications be provided in a manner to be specified on the HHS Web site. Further, as required by section 13402(e)(4) of the Act, the interim final rule stated that the Secretary would begin to post and maintain on the HHS Web site a list of covered entities that submit reports of breaches of unsecured protected health information involving more than 500 individuals.

Under these provisions, covered entities must notify the Secretary of all discovered breaches involving more than 500 individuals, without regard to

whether the breach involved more than 500 residents of a particular State or jurisdiction (the threshold for triggering notification to the media under § 164.406 of the interim final rule). Thus, where a covered entity has discovered a breach involving 600 individuals, 300 of which reside in Maryland and 300 of which reside in the District of Columbia, notification of the breach must be provided to the Secretary concurrently with notification to the affected individuals. However, in this example, the breach would not trigger the requirement to notify the media under § 164.406 because the breach did not involve more than 500 residents of any one State or jurisdiction.

For breaches involving less than 500 individuals, § 164.408(c) requires a covered entity to maintain a log or other documentation of such breaches and to submit information annually to the Secretary for breaches occurring during the preceding calendar year. The interim final rule required the submission of this information to the Secretary no later than 60 days after the end of each calendar year. As with notification of the larger breaches, the interim final rule required that information about breaches involving less than 500 individuals be provided to the Secretary in the manner specified on the HHS Web site.

Although covered entities need only provide notification to the Secretary of breaches involving less than 500 individuals annually, they must still provide notification of such breaches to affected individuals without unreasonable delay and not later than 60 days after discovery of the breach pursuant to § 164.404. In addition, pursuant to § 164.414(a), a covered entity must follow the documentation requirements that otherwise apply to the HIPAA Privacy Rule under § 164.530 with respect to the requirements of this rule. Thus, pursuant to § 164.530(j)(2), covered entities must maintain the internal log or other documentation for six years. Further, as with other required documentation, a covered entity must make such information available to the Secretary upon request for compliance and enforcement purposes in accordance with § 160.310.

Overview of Public Comments

Some commenters expressed concern regarding the timing of providing notification to the Secretary of breaches affecting fewer than 500 individuals. These commenters asked when notification should be provided if a covered entity discovers, after the reporting deadline, a breach that occurred in the previous year. Several others commented on the interim final rule's process for providing the Secretary with breach notification. Some commenters asked that this process be revised to allow covered entities to maintain a log of all breaches affecting fewer than 500 individuals and then submit that log, via attachment (such as an Excel spreadsheet), to the Secretary on an annual basis. These commenters stated that submitting reports of these smaller breaches in this manner would be much less burdensome than submitting the reports individually. Other commenters asked that we provide a template log for entities to use to document smaller breaches for annual submission to the Secretary. Additionally, several commenters suggested that there be access or authentication controls for submitting breach reports because of concerns of false breach reports being submitted to the Secretary without the covered entity's knowledge.

Final Rule

The final rule retains § 164.408(c) with one modification. The modification clarifies that covered entities are required to notify the Secretary of all breaches of unsecured protected health information affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were ''discovered,'' not in which the breaches ''occurred.'' We recognize that there may be situations where, despite having reasonable and appropriate breach detection systems in place, a breach may go undetected for some time. In these cases, if a breach of unsecured protected health information affecting fewer than 500 individuals that occurred in the previous year is discovered, the covered entity has until 60 days after the end of the calendar year in which the breach was discovered to provide notice to the Secretary. We emphasize, however, that this modification does not alter a covered entity's obligation to promptly report the breach to affected individuals without unreasonable delay but in no cases later than 60 calendar days after discovery of the breach.

In response to the comments suggesting that covered entities be permitted to submit a log of all smaller breaches to the Secretary instead of submitting each breach individually through the online form, we agree that the current process may be burdensome for some entities and are considering alternative ways to receive such reports.

With respect to the commenters who asked that access or authentication controls be added to the breach reporting form, we do not believe this is necessary at the present time. Since the Department began receiving and processing breach reports on September 23, 2009, we have not yet received a report that has been falsely submitted by an individual or entity not acting on behalf of the covered entity. Additionally, we emphasize that following receipt of a breach report that affects 500 or more individuals, we contact the covered entity identified in the breach report and verify the information in the report before we post any information about the breach on the HHS Web site. If circumstances change in the future, we will explore options for modifying the process.

Response to Other Public Comments

Comment: One commenter asked that the final rule should not interpret the term ''immediately'' in the statute to mean without unreasonable delay, but in no case later than 60 days, but rather to mean as soon as the breach is discovered. Another commenter asked that the final rule expand the timeframe for providing notification to the Secretary to no later than 120 days after discovery of a breach.

Response: We believe that our interpretation of ''immediately'' with respect to notification to the Secretary for breaches affecting 500 or more individuals is reasonable and appropriate and thus, retain the provision that requires such notice be provided contemporaneously with notice to the individual. Requiring contemporaneous notice allows the notice to the Secretary to include all of the information provided in the notice to the individual and better ensures that a covered entity does not report information to the Secretary that later turns out to be incorrect because the entity did not have sufficient time to conduct an investigation into the facts surrounding the breach. In addition, this interpretation satisfies the statutory requirement that notifications of larger breaches be provided to the Secretary immediately (as they occur) as compared to the reports of smaller breaches the statute allows be reported annually to the Secretary.

Comment: Some commenters asked for further guidance on submitting online breach notifications to the Secretary. Additionally, some commenters asked that HHS provide a confirmation to submitters that an initial breach report or an addendum to a breach report has been successfully submitted.

Response: Since the publication of the interim final rule, OCR has posted

instructions for filling out and submitting the breach form on its Web site: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.* We will continue to examine the instructions for submitting breach notification to the Secretary and will update this information, as necessary, to ensure that covered entities are able to navigate and submit the form easily. The Department has also made changes to the process to ensure that covered entities receive a confirmation following their submission of breach notification to the Secretary. Additionally, we note that the breach reporting form does include an option for indicating that a submission is an addendum to a previous submission. OCR updates the original breach report, as appropriate, with any additional or modified information submitted in an addendum.

Comment: With respect to the posting of breaches affecting 500 or more individuals on the HHS Web site, some commenters stated that these breach submissions must be verified with the covered entity before they are posted publicly. Other commenters asked for clarification of what information will be posted, while another commenter asked that we post only the name of the covered entity involved in the breach. Finally, one commenter suggested that we only post these breaches on our Web site for a six month period.

Response: To provide helpful information to the public, OCR currently posts the following information regarding breaches affecting 500 or more individuals: name of the covered entity (and if applicable, the business associate) involved; State where the covered entity is located; number of individuals affected by the breach; the date of the breach; type of breach (e.g., theft, loss, unauthorized access/disclosure); and location of the breached information (e.g., laptop, paper records, desktop computer). Prior to posting this information, OCR verifies the information in the breach notification report with the covered entity. We do not believe it would serve the public to only disclose the name of the covered entity involved in each of the breaches, because the additional information enables members of the public to understand the nature of the breach and to determine if the breach affects them directly. In terms of how long information about each of the breaches is to remain posted, we intend to maintain the information on our Web site for as long as there is public interest and the data can remain posted in a manner that gives the public access effectively and efficiently.

5. Section 164.410—Notification by a Business Associate

Interim Final Rule

Section 13402(b) of the HITECH Act requires a business associate of a covered entity that accesses, maintains, retains, modifies, records, destroys, or otherwise holds, uses, or discloses unsecured protected health information to notify the covered entity when it discovers a breach of such information. The Act requires business associates to provide such notification to covered entities without unreasonable delay and in no case later than 60 days from discovery of the breach. Additionally, the Act requires business associates to provide covered entities with the identity of each individual whose unsecured protected health information has, or is reasonably believed to have been, affected by the breach. Section 164.410(a) implements section 13402(b) of the Act.

A business associate is required to notify the covered entity of the breach of unsecured protected health information so that the covered entity can notify affected individuals. In the interim final rule, we clarified that a business associate that maintains the protected health information of multiple covered entities need notify only the covered entity(s) to which the breached information relates. However, in cases in which a breach involves the unsecured protected health information of multiple covered entities and it is unclear to whom the breached information relates, it may be necessary to notify all potentially affected covered entities.

Section 164.410(a)(2) provides that a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. As with a covered entity, a business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency). Similarly, as with knowledge imputed to covered entities, the Federal common law of agency controls in determining who is an agent of the business associate.

Section 164.410(b) requires that a business associate provide notice of a breach of unsecured protected health information to a covered entity without unreasonable delay and in no case later than 60 days following the discovery of a breach. With respect to timing, if a business associate is acting as an agent of a covered entity, then, pursuant to § 164.404(a)(2), the business associate's discovery of the breach will be imputed to the covered entity. In such circumstances, the covered entity must provide notifications under § 164.404(a) based on the time the business associate discovers the breach, not from the time the business associate notifies the covered entity. In contrast, if the business associate is not an agent of the covered entity, then the covered entity is required to provide notification based on the time the business associate notifies the covered entity of the breach. We encouraged covered entities and business associates to address the timing of this notification in their business associate contracts.

Section 164.410(c)(1) requires business associates, to the extent possible, to provide covered entities with the identity of each individual whose unsecured protected health information has been, or is reasonably believed to have been, breached. Depending on the circumstances, business associates could provide the covered entity with immediate notification of the breach and then follow up with the required information in § 164.410(c) when available but without unreasonable delay and within 60 days.

Section 164.410(c)(1) requires business associates to provide this information ''to the extent possible,'' recognizing that there may be situations in which a business associate may be unaware of the identification of the individuals whose unsecured protected health information was breached. For example, a business associate that is a record storage company that holds hundreds of boxes of paper medical records on behalf of a covered entity may be unaware of the names of the individuals whose records are stored. Thus, if the business associate discovers that several boxes are missing, it may be unable to provide the covered entity with a list of the individuals whose information has been breached. In such circumstances, it is not our intent that the business associate delay notification of the breach to the covered entity, when the covered entity may be better able to identify the individuals affected.

Depending on the circumstances surrounding a breach of unsecured protected health information, a business

associate may be in the best position to gather the information the covered entity is required by § 164.404(c) to include in the notification to the individual about the breach. Therefore, in addition to the identification of affected individuals, § 164.410(c)(2) requires a business associate to provide the covered entity with any other available information that the covered entity is required to include in the notification to the individual under § 164.404(c), either at the time it provides notice to the covered entity of the breach or promptly thereafter as information becomes available. Because we allow this information to be provided to a covered entity after the initial notification of the breach as it becomes available, a business associate should not delay the initial notification to the covered entity of the breach in order to collect information needed for the notification to the individual. To ensure the covered entity is aware of all the available facts surrounding a breach, the Rule also requires that a business associate provide this information even if it becomes available after notifications have been sent to affected individuals or after the 60-day period specified in § 164.410(b) has elapsed.

We clarified that business associates and covered entities would continue to have the flexibility to set forth specific obligations for each party, such as who will provide notice to individuals and when the notification from the business associate to the covered entity will be required, following a breach of unsecured protected health information, so long as all required notifications are provided and the other requirements of the interim final rule were met. We encouraged the parties to consider which entity is in the best position to provide notice to the individual, which may depend on circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual. We also encouraged the parties to ensure the individual does not receive notifications from both the covered entity and the business associate about the same breach, which may be confusing to the individual.

Overview of Public Comments

Many commenters expressed concern over the interim final rule's treatment of a covered entity's knowledge of a breach that occurs at or by a business associate. Some commenters stated that a covered entity's knowledge of a breach should begin when the business associate notifies them of the breach, regardless of whether the business associate is an agent of the covered entity or a non-agent independent contractor. If knowledge is imputed when the business associate discovers the breach, one commenter argued that a covered entity would not have sufficient time to provide the required notifications to individuals in a timely manner. Other commenters argued that all business associates should be treated as agents of the covered entity, such that the business associate's knowledge of a breach is imputed to the covered entity. Finally, some commenters asked for more guidance on when a business associate is acting as an agent versus as an independent contractor and how to determine this status under the Federal common law of agency.

Final Rule

The final rule modifies § 164.410 only to make the following technical and non-substantive correction: in paragraph (a)(2) of § 164.410, the first sentence is revised to refer to paragraph (a)(1) rather than paragraph (1).

With respect to the commenters who expressed concern that a covered entity's knowledge of a breach depends not only on a business associate's discovery of the breach but also on the covered entity's relationship with the business associate, we acknowledge that there are many different types of relationships that can develop between covered entities and business associates based upon the function the business associate performs on behalf of the covered entity. In some situations, a business associate will be acting as an agent of the covered entity, and as such, it makes sense to treat the business associate's knowledge of a breach analogous to the knowledge of one of the covered entity's own employees. However, in other situations, because a business associate may not be an agent of the covered entity, it would not be reasonable to impute the business associate's knowledge directly to the covered entity, and therefore, the covered entity's knowledge depends on notification from the business associate.

Furthermore, the use of the Federal common law of agency to determine the business associate's status with respect to the covered entity is consistent with the approach taken in the Enforcement Rule for determining agency liability under the HIPAA Rules. Thus, we believe the use of the standard is appropriate here and should be familiar to most entities. We provide additional guidance regarding who is an agent above in our response to comments on the HITECH modifications to the HIPAA Enforcement Rule. Because of the agency implications on the timing of breach notifications, we encourage covered entities to discuss and define in their business associate agreements the requirements regarding how, when, and to whom a business associate should notify the covered entity of a potential breach.

Response to Other Public Comments

Comment: Several commenters asked OCR to provide sample business associate agreement language to outline the covered entity's and business associate's obligations following a breach of unsecured protected health information.

Response: A covered entity's and business associate's obligations following a breach of unsecured protected health information will vary depending on the relationship. For example, whether a business associate will send the breach notices to affected individuals and/or to notify the Secretary (and media, if applicable) on behalf of a covered entity is a business decision of the parties and how quickly a business associate is to notify a covered entity of a breach within the required timeframe may be based on a number of factors, such as whether the business associate is an agent of the covered entity. However, to help covered entities and business associates implement the new business associate agreement requirements generally under the HITECH modifications to the HIPAA Rules, the Department has published sample business associate agreement provisions on its web site.

Comment: Some commenters asked what happens if a covered entity and a business associate disagree about whether an impermissible use or disclosure is a breach that requires notification. These commenters asked if both parties must be in agreement before breach notification obligations are triggered.

Response: The covered entity is ultimately responsible for providing individuals with notification of breaches and, as indicated above, the clock for notifying individuals of breaches begins upon knowledge of the incident, even if it is not yet clear whether the incident qualifies as a breach for purposes of this rule. Further, this final rule clarifies that the default presumption is that an impermissible use or disclosure is a breach unless it can be determined through a risk assessment that there is a low probability that the data may be compromised. This standard should allow for more uniform application of the risk assessment approach across covered entities and business associates.

Comment: One commenter stated that the requirement that a business

associate notify a covered entity of a breach of unsecured protected health information is duplicative of a business associate's other obligations to notify the covered entity of privacy violations and security incidents.

Response: Business associates are required to report to covered entities any security incidents or uses or disclosures of protected health information not provided for by their business associate agreements, which include but are broader than breaches of unsecured protected health information under this Rule. For example, a security incident need not lead to unauthorized access to protected health information (and thus, is not a breach) but is still an event that should be reported to the covered entity. Further, when a security incident occurs that does rise to the level of a breach, the breach notice to the covered entity suffices to meet the requirement to report the security incident to the covered entity (however, a covered entity may require through the business associate agreement that additional information be reported). Therefore, these requirements are not duplicative.

6. Law Enforcement Delay

Interim Final Rule

Section 13402(g) of the HITECH Act provides that if a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under 45 CFR 164.528(a)(2) of the Privacy Rule in the case of a disclosure covered under such section. Section 164.412 implements section 13402(g) of the Act, requiring a covered entity or business associate to temporarily delay notification to the individual, the media (if applicable), to a covered entity by a business associate, and to the Secretary if instructed to do so by a law enforcement official.

Section 164.412(a), based on the requirements of 45 CFR 164.528(a)(2)(i) of the Privacy Rule, provides for a temporary delay of notification in situations in which a law enforcement official provides a statement in writing that the delay is necessary because notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required. In such instances, the covered entity is required to delay the notification, notice, or posting for the time period specified by the official.

Similarly, § 164.412(b), based on 45 CFR 164.528(a)(2)(ii) of the Privacy Rule, requires a covered entity or business associate to temporarily delay a notification, notice, or posting if a law enforcement official states orally that a notification would impede a criminal investigation or cause damage to national security. However, in this case, the covered entity or business associate must document the statement and the identity of the official and delay notification for no longer than 30 days, unless a written statement meeting the above requirements is provided during that time. We interpreted these provisions as tolling the time within which notification is required under §§ 164.404, 164.406, 164.408, and 164.410, as applicable.

Final Rule

The Department did not receive public comments on this provision of the interim final rule. We retain § 164.412 in this final rule without modification.

7. Section 164.414—Administrative Requirements and Burden of Proof

Interim Final Rule

Section 164.414(a) requires covered entities to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) of the Privacy Rule with respect to the breach notification provisions of this subpart. These Privacy Rule provisions, for example, require covered entities and business associates to develop and document policies and procedures, train workforce members on and have sanctions for failure to comply with these policies and procedures, permit individuals to file complaints regarding these policies and procedures or a failure to comply with them, and require covered entities to refrain from intimidating or retaliatory acts. Thus, a covered entity is required to consider and incorporate the breach notification requirements with respect to its administrative compliance and other obligations.

Section 164.414(b) provides that, following an impermissible use or disclosure under the Privacy Rule, covered entities and business associates have the burden of demonstrating that all notifications were made as required by this subpart. Additionally, as part of demonstrating that all required notifications were made, a covered entity or business associate, as applicable, also must be able to demonstrate that an impermissible use or disclosure did not constitute a breach, as such term is defined at § 164.402, in cases where the covered entity or business associate determined that notifications were not required. To conform to these provisions, § 160.534 of the HIPAA Enforcement Rule makes clear that, during any administrative hearing, the covered entity has the burden of going forward and the burden of persuasion with respect to these issues.

Thus, when a covered entity or business associate knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively, to demonstrate that notification was not required: (1) Its risk assessment (discussed above in § 164.402) demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure or (2) the application of any other exceptions to the definition of ''breach.''

Overview of Public Comments

One commenter stated that it is critical that all employees are trained and knowledgeable about what constitutes a breach, so that the covered entity or business associate can provide the required notifications within the required timeframe. The commenter also maintained that OCR should emphasize the necessity of this training.

With respect to the burden of proof placed upon covered entities and business associates, one commenter agreed that covered entities and business associates should have the burden to demonstrate that all notifications were provided following a breach of unsecured protected health information. However, the commenter asked that we include a presumption that an impermissible use or disclosure of protected health information did not constitute a breach if a covered entity or business associate has implemented a breach notification policy, completed a risk assessment, and documented that it followed its policy in reaching a conclusion that breach notification was not required.

Final Rule

We retain § 164.414 in this final rule without modification. We emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured protected health information. We note that because this final rule modifies the definition of breach as stated in the interim final rule, covered

entities will need to update their policies and procedures and retrain workforce members as necessary to reflect such modifications.

With respect to this burden of proof, section 13402 of the statute places the burden of proof on a covered entity or business associate, if applicable, to demonstrate that all notifications were made as required. Therefore, section 164.530(j)(1)(iv) requires covered entities to maintain documentation to meet this burden of proof. This includes documentation that all required notifications have been provided or that no breach occurred and notification was not necessary. If a covered entity's determination with respect to whether a breach occurred is called into question, the covered entity should produce the documentation that demonstrates the reasonableness of its conclusions based on the findings of its risk assessment.

8. Technical Corrections

The interim final rule made several technical changes to align the HIPAA Rules in light of the new breach notification requirements of subpart D. See 74 FR 42755–56. We did not receive comments on these changes. We retain the technical corrections made in the interim final rule and also make an additional technical correction by adding ''and'' to the end of § 160.534(b)(1)(iii) to make clear the relationship between § 160.534(b)(1)(iii) and the new § 160.534(b)(1)(iv).

9. Preemption

Interim Final Rule

The interim final rule clarified that contrary State law will be preempted by these breach notification regulations. Section 1178 of the Social Security Act, 42 U.S.C. 1320d–7, which was added by HIPAA, provides that HIPAA administrative simplification provisions generally preempt conflicting State law. Section 160.203 states that a standard, requirement, or implementation specification that is adopted as regulation at 45 CFR parts 160, 162, or 164 and that is ''contrary to a provision of State law preempts the provision of State law.'' Thus, whether a State law is contrary to these breach notification regulations is to be determined based on the definition of ''contrary'' at § 160.202, which states that a State law is contrary if ''[a] covered entity would find it impossible to comply with both the State and Federal requirements'' or if the State law ''stands as an obstacle to the accomplishment and execution of the full purposes and objectives'' of the breach notification provisions in the Act. Covered entities must analyze relevant State laws with respect to the breach requirements to understand the interaction and apply this preemption standard appropriately.

In the interim final rule, we stated our belief that, in general, covered entities can comply with both the applicable State laws and this regulation and that in most cases, a single notification can satisfy the notification requirements under State laws and this regulation. For example, if a State breach notification law requires notification be sent to the individual in a shorter time frame than is required by this regulation, a covered entity that sends the notice within the time frame required by the State law will also be in compliance with this regulation's timeliness requirements.

Additionally, since the Act and rule are flexible in terms of how the elements are to be described, and do not prohibit additional elements from being included in the notice, in general, Federal requirements contain flexibility for covered entities to develop a notice that satisfies both laws.

Overview of Public Comments

While some commenters were pleased that the breach notification rule preempts conflicting State law, other commenters expressed confusion or concern with this preemption standard. Many commenters stated that despite the fact that in most cases a covered entity may only need to provide one notification to satisfy both State and Federal law, there will be some cases in which a covered entity will have to provide multiple notices to the same individual to ensure compliance with all relevant laws. This will result in confusion for the individual and increased costs for the covered entity. Some of these commenters suggested that this Federal breach notification law should preempt all State breach notification laws, or alternatively, that HHS should work with Congress and the States to harmonize the breach notification laws such that only one notice is required following a breach.

Final Rule

We maintain the preemption standard discussed in the interim final rule, which is based on section 1128 of the Social Security Act and applies to the HITECH Act's breach notification provisions by virtue of section 13421 of the HITECH Act. We continue to believe that, generally, covered entities are able to comply with both State and Federal requirements for providing breach notification with one breach notice based on the flexibility provided to entities in this Rule. However, even in the exceptional case, we do not have authority to preempt a State breach notification law that is not contrary to this Rule.

10. Responses to Other Public Comments

Comment: One commenter asked whether penalties are automatically assessed following a violation of the breach notification rule or if this is done at OCR's discretion and whether civil money penalties can be assessed for the underlying cause of a breach of unsecured protected health information where a covered entity has provided all required breach notifications.

Response: OCR's enforcement of the breach notification rule will be carried out pursuant to the Enforcement Rule. Pursuant to the Enforcement Rule, OCR may impose a civil money penalty for a failure to comply with the breach notification rule. OCR also has the discretion to work with the covered entity to achieve voluntary compliance through informal resolution, except in cases in which it has found a violation due to willful neglect. Because every breach of unsecured protected health information must have an underlying impermissible use or disclosure under the Privacy Rule, OCR also has the authority to impose a civil money penalty for the underlying Privacy Rule violation, even in cases where all required breach notifications were provided.

VI. Modifications to the HIPAA Privacy Rule Under GINA

A. Background

The Genetic Information Nondiscrimination Act of 2008 (''GINA''), Public Law 110–233, 122 Stat. 881, prohibits discrimination based on an individual's genetic information in both the health coverage and employment contexts. With respect to health coverage, Title I of GINA generally prohibits discrimination in premiums or contributions for group coverage based on genetic information, proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental (Medigap) insurance markets, and limits the ability of group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing. Title II of GINA generally prohibits use of genetic information in the employment context, restricts employers and other entities covered by Title II from requesting, requiring, or purchasing genetic

information, and strictly limits such entities from disclosing genetic information. The Departments of Labor, Treasury, and Health and Human Services (HHS) are responsible for administering and enforcing the GINA Title I nondiscrimination provisions, and the Equal Employment Opportunity Commission (EEOC) is responsible for administering and enforcing the GINA Title II nondiscrimination provisions.[13]

In addition to these nondiscrimination provisions, section 105 of Title I of GINA contains new privacy protections for genetic information, which require the Secretary of HHS to revise the Privacy Rule to clarify that genetic information is health information and to prohibit group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.[14]

B. Overview of the Proposed Rule

On October 7, 2009, the Department published a notice of proposed rulemaking (NPRM or ''proposed rule'') to strengthen the privacy protections for genetic information under the HIPAA Privacy Rule by implementing the protections for genetic information required by GINA [15] and making related changes to the Rule. In particular, in accordance with section 105 of GINA and the Department's general authority under sections 262 and 264 of HIPAA, the Department proposed to: (1) Explicitly provide that genetic information is health information for purposes of the Privacy Rule; (2) prohibit all health plans covered by the HIPAA Privacy Rule from using or disclosing protected health information that is genetic information for underwriting purposes; (3) revise the provisions relating to the Notice of Privacy Practices for health plans that perform underwriting; (4) make a number of conforming changes to definitions and other provisions of the Rule; and (5) make technical corrections to update the definition of ''health plan.''

The 60-day public comment period for the proposed rule closed on December 7, 2009, and the Department received approximately twenty-five comments in response to its proposal.[16] After considering the public comments, the Department is issuing this final rule to strengthen the privacy protections for genetic information in accordance with GINA and the Department's general authority under sections 262 and 264 of HIPAA. In developing this rule, the Department consulted with the Departments of Labor and Treasury, as required by section 105(b)(1) of GINA, to ensure, to the extent practicable, consistency across the regulations. In addition, the Department coordinated with the EEOC in the development of these regulations.

The provisions of the proposed rule and the public comments received that were within the scope of the proposed rule are described in more detail below in the section-by-section description of the final rule.

C. Section-by-Section Description of Final Rule and Response to Public Comments

1. Scope: Extension of Required Protections to All Health Plans Subject to the HIPAA Privacy Rule

Proposed Rule

Section 105 of GINA requires HHS to modify the Privacy Rule to prohibit ''a covered entity that is a group health plan, health insurance issuer that issues health insurance coverage, or issuer of a medicare [sic] supplemental policy'' from using or disclosing genetic information for underwriting purposes. Section 105 of GINA provides that the terms ''group health plan'' and ''health insurance coverage'' have the meanings given such terms under section 2791 of the Public Health Service Act (PHSA) (42 U.S.C. 300gg–91), and that the term ''medicare [sic] supplemental policy'' has the meaning given such term in section 1882(g) of the Social Security Act. In addition, the term ''health insurance issuer,'' as defined at 42 U.S.C. 300gg–91, includes a health maintenance organization (HMO). These four types of entities (i.e., group health plans, health insurance issuers, and health maintenance organizations, as defined in the PHSA, as well as issuers of Medicare supplemental policies), correspond to the types of covered entities listed at subparagraphs (i) through (iii) and (vi) of paragraph (1) of the definition of ''health plan'' at § 160.103 in the HIPAA Privacy Rule, issued under HIPAA's Administrative Simplification provisions. These also are the entities to which HIPAA's nondiscrimination provisions apply and to which the nondiscrimination provisions of GINA Title I were directed.

However, in addition to these four types of entities, the HIPAA Privacy Rule also includes a number of other entities within the definition of ''health plan'': (1) Long-term care policies (excluding nursing home fixed-indemnity policies); (2) employee welfare benefit plans or other arrangements that are established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers (to the extent that they are not group health plans or health insurance issuers); (3) high risk pools that are mechanisms established under State law to provide health insurance coverage or comparable coverage to eligible individuals; (4) certain public benefit programs, such as Medicare Part A and B, Medicaid, the military and veterans' health care programs, the Indian Health Service program, and others; as well as (5) any other individual or group plan, or combination of individual or group plans that provides or pays for the cost of medical care (as the term ''medical care'' is defined in section 2791(a)(2) of the PHSA, 42 U.S.C. 300gg–91(a)(2)). This last category includes, for example, certain ''excepted benefits'' plans described at 42 U.S.C. 300gg–91(c)(2), such as limited scope dental or vision benefits plans. See the definition of ''health plan'' at § 160.103.

In the NPRM, the Department, using both its authority under GINA as well as its broad authority under HIPAA, proposed to apply the prohibition on using and disclosing protected health information that is genetic information for underwriting to all health plans that are subject to the Privacy Rule, rather than solely to the plans GINA explicitly requires be subject to the prohibition. As explained in the proposed rule, the HIPAA Administrative Simplification provisions provide the Secretary with

[13] The Departments of Labor (Employee Benefits Security Administration), Treasury (Internal Revenue Service), and HHS (Centers for Medicare & Medicaid Services (CMS)) have issued regulations in a separate rulemaking (at 74 FR 51664) to implement sections 101–103 of GINA, which amended: section 702 of the Employee Retirement Income Security Act of 1974 (29 U.S.C. 1182); section 2702 of the Public Health Service Act (42 U.S.C. 300gg–1) (renumbered as section 2705 by the Affordable Care Act); and section 9802 of the Internal Revenue Code of 1986. Section 104 of GINA applies to Medigap issuers, which are subject to the provisions of section 1882 of the Social Security Act that are implemented by CMS, and which incorporate by reference certain provisions in a model regulation of the National Association of Insurance Commissioners (NAIC). The NAIC amended its model regulation on September 24, 2008, to conform to section 104 of GINA, and the amended regulation was published by CMS in the **Federal Register** on April 24, 2009, at 74 FR 18808. With respect to Title II of GINA, the EEOC issued final regulations on November 9, 2010, at 75 FR 68912.

[14] Section 105 of GINA, entitled ''Privacy and Confidentiality,'' amends Part C of Title XI of the Social Security Act by adding section 1180 to address the application of the HIPAA Privacy Rule to genetic information.

[15] Any reference in this preamble to GINA is a reference to Title I of GINA, except as otherwise indicated.

[16] The public comments are available at *http://www.regulations.gov*.

broad authority to craft privacy standards that uniformly apply to all health plans, regardless of whether such health plans are governed by other portions of the HIPAA statute. In addition, the Department indicated in the proposed rule that nothing in GINA explicitly or implicitly curtails this broad authority of the Secretary to promulgate privacy standards for any and all health plans that are governed by the HIPAA Administrative Simplification provisions.

Under the Privacy Rule, and consistent with HIPAA, an individual's privacy interests and rights with respect to the use and disclosure of protected health information are protected uniformly without regard to the type of health plan that holds the information. Thus, under the Privacy Rule, individuals can expect and benefit from privacy protections that do not diminish based on the type of health plan from which they obtain health coverage. In developing the proposed rule, the Department believed that individuals' interests in uniform protection under the Privacy Rule against the use or disclosure of their genetic information for underwriting purposes would outweigh any adverse impact on health plans that are not covered by GINA, particularly since it was not expected that all of the health plans subject to the Privacy Rule use or disclose protected health information that is genetic information for underwriting (or even perform underwriting generally, in the case of some of the public benefit plans). For these reasons, the Department proposed to apply the prohibition on using or disclosing protected health information that is genetic information for underwriting purposes to all health plans that are HIPAA covered entities.

Overview of Public Comments

The Department received comments both in support of and against the proposed application of the prohibition on using or disclosing genetic information for underwriting purposes to all health plans covered by the Privacy Rule. Several commenters agreed that the extension of the proposed requirements to all health plans is an appropriate exercise of the Secretary's discretion under HIPAA and is necessary to protect the privacy interests of all individuals without regard to the type of health plan holding individuals' health information, and stated that such an extension would further encourage individuals to take advantage of genetic services. In addition, one commenter in support of the proposal indicated that sixteen States also regulate the use of genetic information in disability insurance, and ten States regulate its use in long-term care insurance, and it is expected that these numbers will continue to increase. The commenter stated that as States move forward in this area it was appropriate for the Federal government to do so as well. However, this and one other commenter, while generally in support of extending the prohibition on using or disclosing genetic information for underwriting to all health plans, also recommended that the Department monitor the impact of such a prohibition on long-term care insurers.

A few commenters did not support the Department's proposal and argued that the prohibition against using or disclosing genetic information for underwriting purposes in the Privacy Rule should apply only to those plans to which GINA expressly applies. Commenters argued that applying the prohibition beyond the health plans identified in GINA was contrary to GINA and its intent.

Certain commenters expressed particular disagreement and concern with applying the prohibition on the use of genetic information for underwriting to long-term care insurers. One commenter argued that there was clear Congressional intent in the legislative history of GINA to exempt ''excepted benefits,'' particularly long-term care insurance, from any prohibitions under GINA and thus, the Privacy Rule should not apply the prohibition on underwriting with genetic information to issuers of long term care policies. The commenter also argued that the GINA prohibition should not apply to long-term care insurers because long-term care plans have different characteristics from other health plans and applying the GINA prohibition to long-term care insurers would jeopardize the ability of long-term care insurers to adequately underwrite and thus, the viability of the long-term care insurance market. The commenter explained that this would be due to the fact that when underwriting, long term care insurers look to determine an individual's probability of needing long-term care in the future and diagnosis of a particular condition is not the only way this may be determined and in some cases may not even be relevant to such a determination. The Department also heard similar concerns about the potential negative impact of an underwriting prohibition on the economic viability of the long-term market, from certain members of Congress who wrote to the Secretary on this issue, as well as from certain outside parties during fact finding meetings held by the Department.

Final Rule

The final rule adopts the approach of the proposed rule to apply the prohibition on using or disclosing protected health information that is genetic information for underwriting purposes to all health plans that are covered entities under the HIPAA Privacy Rule, including those to which GINA does not expressly apply, except with regard to issuers of long term care policies. We continue to disagree with the commenters that stated such an extension would conflict with GINA and is outside the scope of our authority. As explained more fully in the proposed rule, the Department has broad authority under HIPAA to regulate a health plan's uses and disclosures of protected health information, including genetic information, to protect an individual's privacy interests. See 74 FR 51698, 51699–51700. It does not follow that by exempting ''excepted benefits'' from the prohibitions under GINA that Congress intended to restrict the Department's broad authority under HIPAA. Further, there is no conflict with GINA in extending the same privacy protections outlined in GINA to those health plans that are not covered by GINA but are otherwise covered by the HIPAA Privacy Rule. GINA and section 264 of HIPAA are not irreconcilably inconsistent but rather operate concurrently without conflict. Lastly, GINA did not override HIPAA, and did not displace the Department's authority to prohibit uses and disclosures of genetic information that GINA does not otherwise prohibit. Therefore, nothing in GINA explicitly or implicitly curtails the broad authority of the Secretary to promulgate privacy standards for any and all health plans that are governed by the HIPAA Administrative Simplification provisions.

We also continue to believe that individuals have a strong privacy interest in not having their genetic information used in an adverse manner for underwriting purposes and to believe that this privacy interest outweighs any adverse impact on most health plans covered by the Privacy Rule. With respect to most health plans not subject to GINA, the public comment did not indicate that a prohibition on using genetic information for underwriting would have significant adverse impacts on the viability of these plans. Nor did the public comment generally provide information showing that these health plans actually use or disclose protected health information that is genetic information for underwriting, or plan to

do so in the future (or even perform underwriting generally, in the case of some of the public benefit plans).

However, as indicated above, the Department did hear from a number of sources about the potential adverse impact a prohibition on using genetic information for underwriting would have on the ability of a long-term care insurer to effectively underwrite and thus, on the viability of the long-term care insurance market generally. The Department recognizes the importance of long-term care insurance coverage and the need to ensure its continued availability. The Department also acknowledges that, at this time, it does not have the information necessary to more precisely and carefully measure the extent of such an impact on the long-term market in order to appropriately balance an individual's privacy interests with such an impact. Thus, this final rule excludes long-term care plans from the underwriting prohibition.

While we exempt long-term care plans from the underwriting prohibition in this final rule, we continue to believe an individual has a strong privacy interest in the way his or her genetic information is used for the underwriting of long-term care insurance. At the current time, however, we do not have sufficient information to determine the proper balance between the individual's privacy interests and the industry's concerns about the cost effects of excluding genetic information. For that reason, we are looking into ways to obtain further information on this issue, such as through a study by the National Association of Insurance Commissioners (NAIC) on the tension between the use of genetic information for underwriting and the associated privacy concerns in the context of their model long-term care rules. Based on the information the Department may obtain, the Department will reassess how best to move forward in this area in the future.

Long-term care plans, while not subject to the underwriting prohibition, continue to be bound by the Privacy Rule, as are all other covered health plans, to protect genetic information from improper uses and disclosures, and to only use or disclose genetic information as required or expressly permitted by the Rule, or as otherwise authorized by the individual who is the subject of the genetic information.

2. Section 160.101—Statutory Basis and Purpose

We have revised § 160.101, which describes the statutory basis of the HIPAA Rules, to include a reference to section 1180 of the Social Security Act, as added by section 105 of GINA (Pub. L. 110–233).

3. Section 160.103—Definitions

The final rule modifies § 160.103 of the Privacy Rule to: (1) Revise the definition of ''health information'' to make clear that the term includes ''genetic information;'' (2) add definitions for the GINA-related terms of ''family member,'' ''genetic information,'' ''genetic services,'' ''genetic test,'' and ''manifestation or manifested;'' and (3) make technical corrections to the definition of ''health plan.'' With respect to the GINA-related terms, the final rule adopts definitions that are generally consistent with the definitions of such terms promulgated in the implementing regulations for sections 101–103 of GINA. This will facilitate compliance for those health plans subject to both the privacy as well as the nondiscrimination provisions of GINA.

a. Definition of ''Health information''

Proposed Rule

Prior to enactment of GINA, the Department issued guidance that genetic information is health information protected by the Privacy Rule to the extent that such information is individually identifiable and held by a covered entity (subject to the general exclusions from the definition of ''protected health information'').[17] Section 105 of GINA requires the Secretary to revise the Privacy Rule to make clear that genetic information is health information under the Rule. Thus, the Department proposed to modify the definition of ''health information'' at § 160.103 to explicitly provide that such term includes genetic information.

Overview of Public Comments

The Department received a few comments expressing specific support for and one comment against the proposed inclusion of the term ''genetic information'' in the definition of ''health information.'' The commenters supporting the revision to the definition of ''health information'' indicated that such an inclusion was necessary to clarify that genetic information is health information. The commenter against the proposed inclusion to the definition argued that although GINA directs the Department to treat genetic information as health information, the language of GINA does not require a change to the definition of ''health information,'' and this change would create costs for health plans, which would have to update all their policies and procedures to reflect the change.

Final Rule

The final rule adopts the proposed modification to the definition of ''health information'' at § 160.103. This modification to the definition is a necessary clarification to the Privacy Rule based on the statutory language. Given that revising the definition of ''health information'' to include genetic information does not substantively change the scope of the Privacy Rule, it is unclear why such a change alone would require revisions to a health plan's policies and procedures. Health plans that perform underwriting will otherwise need to revise their policies and procedures as necessary to comply with this final rule, as well as the modifications to the HIPAA Rules required by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Thus, to the extent the concern about this modification stems from the fact that a health plan's policies and procedures quote the prior regulatory definition of ''health information,'' the health plan can revise the definition at the time it is otherwise updating its policies and procedures to comply with these rules.

b. Definition of ''Genetic Information''

Proposed Rule

The term ''genetic information'' is defined in GINA and establishes what information is protected by the statute. Section 105 of GINA provides that the term ''genetic information'' in section 105 shall have the same meaning given the term in section 2791 of the PHSA (42 U.S.C. 300gg–91), as amended by section 102 of GINA. Section 102(a)(4) of GINA defines ''genetic information'' to mean, with respect to any individual, information about: (1) Such individual's genetic tests; (2) the genetic tests of family members of such individual; and (3) the manifestation of a disease or disorder in family members of such individual (i.e., family medical history). GINA also provides that the term ''genetic information'' includes, with respect to any individual, any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by such

[17] See, e.g., Frequently Asked Question number 354, available at *http://www.hhs.gov/ocr/privacy/hipaa/faq/protected_health_information/354.html*, which states: *Question:* Does the HIPAA Privacy Rule protect genetic information? *Answer:* Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse. See also 45 CFR 160.103.

individual or family member of such individual. GINA expressly provides that the term ''genetic information'' shall not include information about the sex or age of any individual. This basic definition of ''genetic information'' in section 102(a)(4) of GINA (and that is to apply for purposes of section 105) is also expanded by section 102(a)(3), which provides that any reference to genetic information concerning an individual or family member in the PHSA shall include: with respect to an individual or family member of an individual who is a pregnant woman, the genetic information of any fetus carried by such pregnant woman; and with respect to an individual or family member utilizing an assisted reproductive technology, the genetic information of any embryo legally held by the individual or family member. The Department proposed to include this statutory definition of ''genetic information'' in § 160.103.

Overview of Public Comments

Most commenters did not address the proposed definition of ''genetic information'' in their comments on the proposed rule. However, one commenter stated that it was unclear what information may fall within the scope of the term ''genetic information'' and whether such term may be construed to include traditional medical information or medical tests used in underwriting today.

Final Rule

The final rule adopts without modification the definition of ''genetic information'' proposed in the NPRM. This definition is consistent with the definition found in the implementing regulations for sections 101–103 of GINA and with which compliance is already required by most health plans. The term ''genetic information'' includes information about the genetic tests of the individual or of the individual's family members and about diseases or disorders manifested in an individual's family members (i.e., family health history). Thus, information about manifested diseases, disorders, or conditions of the individual or medical tests that do not meet the rule's definition of ''genetic test,'' such as HIV tests, complete blood counts, cholesterol or liver function tests, or tests to detect for the presence of alcohol or drugs, are not genetic information, and such information may be used or disclosed for underwriting purposes. Conversely, family health histories and information about genetic tests, such as tests to determine whether an individual or family member has a gene variant associated with breast cancer, are genetic information, and such information may not be used or disclosed for underwriting purposes. The definitions of ''manifestation or manifested'' and ''genetic test'' are discussed more fully below.

c. Definition of ''Genetic Test''

Proposed Rule

As explained above, GINA provides that the term ''genetic information'' includes information about an individual's genetic tests or the genetic tests of family members of the individual. Section 105 of GINA provides that the term ''genetic test'' shall have the same meaning as the term has in section 2791 of the PHSA (42 U.S.C. 300gg–91), as amended by section 102 of GINA. Section 102(a)(4) of GINA amends section 2791(d) of the PHSA to define ''genetic test'' to mean ''an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes.'' GINA further clarifies that the term ''genetic test'' does not include an analysis of proteins or metabolites that does not detect genotypes, mutations, or chromosomal changes, nor does it include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved.

Consistent with the statutory definition, the Department proposed to define ''genetic test'' at § 160.103 as an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes, and to provide in the definition that ''genetic test'' does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition. While the statute refers to a ''manifested'' disease as one that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved, the statute does not define ''manifested.'' Consequently, for clarity, the Department proposed a definition of ''manifested,'' as described below.

Overview of Public Comments

The Department received one comment requesting that the Department include examples within the regulatory text of the definition and another comment stated that it is not clear what constitutes a genetic test under the definition.

Final Rule

The final rule adopts without modification the definition of ''genetic test'' as proposed in the NPRM. This definition is consistent with the definition found in the implementing regulations for sections 101–103 of GINA and with which compliance is already required by most health plans. Under this definition, a test to determine whether an individual has a gene variant associated with breast cancer (such as the BRCA1 or BRCA2 variant) is a genetic test. Similarly, a test to determine whether an individual has a genetic variant associated with hereditary nonpolyposis colorectal cancer is a genetic test. Such tests are genetic in nature because they detect genotypes, mutations, or chromosomal changes. In contrast, medical tests that do not detect genotypes, mutations, or chromosomal changes, are not genetic tests. For example, HIV tests, complete blood counts, cholesterol tests, liver function tests, or tests for the presence of alcohol or drugs are not genetic tests. Consistent with the approach taken generally with the HIPAA Privacy Rule, the Department declines to include these examples in the regulatory text. The Department intends to issue future guidance on its web site about this issue.

d. Definition of ''Genetic Services''

Proposed Rule

GINA provides that the term ''genetic information'' includes, with respect to any individual, any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by such individual or any family member of such individual. Section 102(a)(4) of GINA defines ''genetic services'' to mean: (1) A genetic test; (2) genetic counseling (including obtaining, interpreting, or assessing genetic information); or (3) genetic education. Thus, the fact that an individual or a family member of the individual requested or received a genetic test, counseling, or education is information protected under GINA. Genetic counseling and education are means by which individuals can obtain information and support about potential risks for genetic diseases and disorders. The Department proposed to add the statutory definition of ''genetic services'' to the Privacy Rule.

Overview of Public Comments

The Department received one comment requesting that the

Department add language to the definition to make clear that the genetic tests, genetic counseling, or genetic education of a family member of an individual are specifically covered by the term.

Final Rule

The final rule adopts without modification the definition of ''genetic services'' proposed in the NPRM. This definition is consistent with the definition found in the implementing regulations for sections 101–103 of GINA and with which compliance is already required by most health plans. The Department does not believe it necessary to add the term ''family member'' to the definition of ''genetic services'' because the definition of ''genetic information'' makes clear that information about any request for, or receipt of, genetic services by a family member of an individual is protected information.

e. Definition of ''Family Member''

Proposed Rule

The term ''family member'' is used in the definition of ''genetic information'' in GINA to indicate that an individual's genetic information also includes information about the genetic tests of the individual's family members, as well as family medical history. Section 105 of GINA states that the term ''family member'' shall have the meaning given such term in section 2791 of the PHSA (42 U.S.C. 300gg–91), as amended by GINA section 102(a)(4), which defines ''family member'' to mean, with respect to any individual: (1) A dependent (as such term is used for purposes of section 2701(f)(2) of the PHSA, 42 U.S.C. 300gg(f)(2)) of such individual; or (2) any other individual who is a first-degree, second-degree, third-degree, or fourth-degree relative of such individual or of a dependent of the individual. Section 2701(f)(2) of the PHSA uses the term ''dependent'' to mean an individual who is or may become eligible for coverage under the terms of a group health plan because of a relationship to the plan participant.

The Department proposed to incorporate GINA's definition of ''family member'' into the Privacy Rule. The proposed rule also clarified within the definition that relatives by affinity (such as by marriage or adoption) are to be treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor) and that, in determining the degree of relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents). The NPRM explained that this broad interpretation of ''family member'' was consistent with GINA's legislative history, which suggests that the term ''family member'' is to be broadly construed to provide the maximum protection against discrimination.[18] In addition, the Department proposed to include in the definition of ''family member'' non-exhaustive lists of persons who are first-, second-, third-, or fourth-degree relatives. Finally, within the definition of ''family member,'' the Department proposed to refer to the definition of ''dependent'' contained in the implementing regulations at 45 CFR 144.103 rather to the PHSA directly.

Overview of Public Comments

One commenter expressed support for including relatives by affinity and by less than full consanguinity, agreeing that this interpretation is consistent with Congressional intent and provides the most privacy protection for individuals. This commenter also was supportive of including non-exhaustive lists of persons who are first-, second-, third-, and fourth-degree relatives to add clarity to the definition.

Final Rule

As we received only support with regard to the definition of ''family member,'' the final rule adopts without modification the definition of ''family member'' proposed in the NPRM. This definition also is consistent with the definition found in the implementing regulations for sections 101–103 of GINA and with which compliance is already required by most health plans.

f. Definition of ''Manifestation or Manifested''

Proposed Rule

Although not separately defined by GINA, the terms ''manifestation'' or ''manifested'' are used in GINA in three important contexts. First, GINA uses the term ''manifestation'' to incorporate ''family medical history'' into the definition of ''genetic information'' by stating that ''genetic information'' includes, with respect to an individual, the manifestation of a disease or disorder in family members of such individual. Second, GINA uses the term ''manifested'' to exclude from the definition of ''genetic test'' those tests that analyze a physical malady rather than genetic makeup by excluding from the definition analyses of proteins or metabolites that are directly related to a manifested disease, disorder, or pathological condition. Third, GINA uses the term ''manifestation'' to clarify that nothing in Title I of GINA should be construed to limit the ability of a health plan to adjust premiums or contribution amounts for a group health plan based on the manifestation of a disease or disorder of an individual enrolled in the plan.[19] However, GINA provides that, in such case, the manifestation of a disease or disorder in one individual cannot also be used as genetic information about other group members and to further increase the premium for the plan. Similarly, for the individual health insurance market, GINA clarifies that it does not prohibit a health plan from establishing rules for eligibility for an individual to enroll in coverage or from adjusting premium or contribution amounts for an individual based on the manifestation of a disease or disorder in that individual or in a family member of such individual where such family member is covered under the individual's policy. However, under GINA, the manifestation of a disease or disorder in one individual cannot also be used as genetic information about other individuals and to further increase premiums or contribution amounts.

Given the importance of the term ''manifested'' or ''manifestation,'' the Department proposed to define the term. Although GINA does not define the term, it is clear from the statutory definition of ''genetic test'' that a manifested disease or disorder is one ''that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved.'' Accordingly, the proposed rule defined the term ''manifestation or manifested'' to mean, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. The proposed definition also provided that a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information. This clarification was included due to the fact that variants of genes associated with diseases have varying degrees of predictive power for

[18] *See* House Report 110–28, Part 2 at 27.

[19] We note that the Affordable Care Act, enacted on March 23, 2010, includes a provision effective for plan years beginning on or after January 1, 2014, that prohibits insurers from discriminating against individuals or charging individuals higher rates based on pre-existing conditions. See Public Law 111–148.

later development of the disease. In some cases, an individual may have a genetic variant for a disease and yet never develop the disease. In other cases, the presence of a genetic variant indicates that the individual will eventually develop the disease, such as is the case with Huntington's disease. However, an individual may obtain a positive test that shows the genetic variant for Huntington's disease decades before any clinical symptoms appear. Under the proposed definition, the presence of a genetic variant alone would not constitute the diagnosis of a disease even in cases where it is certain the individual possessing the genetic variant will eventually develop the disease, such as with Huntington's disease.

Overview of Public Comments

A few commenters expressed support for adopting the proposed definition of ''manifestation or manifested'' because it would provide clarity to the rule and the scope of the underwriting prohibition. One commenter requested that the Department include the examples provided in the preamble to the proposed rule directly within the regulatory definition. A few commenters raised concerns about the inclusion in the proposed definition of the clarification that ''a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.'' It was argued that the proposed definition was too narrow because, for some diseases, disorders, or pathological conditions, a genetic test is the primary means of diagnosing the condition and further that genetic tests will more frequently be used to diagnose diseases or conditions in the future given the continuing evolution of genetics. It was also argued that the proposed definition went beyond GINA by indicating how a manifested disease or disorder is diagnosed.

Final Rule

The final rule adopts without modification the definition of ''manifestation or manifested'' proposed in the NPRM. The definition is consistent with the definition of ''manifestation or manifested'' found in the implementing regulations for the non-discrimination provisions of sections 101–103 of GINA and with which compliance is already required for most health plans. In developing this definition, the agencies consulted with technical experts at the National Human Genome Research Institute within the National Institutes of Health (NIH). In addition, for the reasons stated above regarding the varying degrees of predictive power genes provide in terms of ultimate development of a disease, as well as of the fact that a genetic test for a disease may precede clinical signs or symptoms by years or even decades, the Department does not believe that the definition is too narrow but rather that it is consistent with the provisions of GINA that protect genetic information from being used for health coverage determinations. Finally, the definition does not preclude a health care provider from performing one or more genetic tests to confirm a diagnosis so long as the diagnosis is not based solely or principally on the result of the genetic test.

To illustrate the definition, we provide the following examples, which were also included in the NPRM:

- An individual may have a family member that has been diagnosed with Huntington's disease and also have a genetic test result that indicates the presence of the Huntington's disease gene variant in the individual. However, when the individual is examined by a neurologist (a physician with appropriate training and expertise for diagnosing Huntington's disease) because the individual has begun to suffer from occasional moodiness and disorientation (symptoms which are associated with Huntington's disease), and the results of the examination do not support a diagnosis of Huntington's disease, then Huntington's disease is not manifested with respect to the individual. In contrast, if the individual exhibits additional neurological and behavioral symptoms, and the results of the examination support a diagnosis of Huntington's disease by the neurologist, then Huntington's disease is manifested with respect to the individual.
- An individual has had several family members with colon cancer, one of whom underwent genetic testing which detected a mutation in the MSH2 gene associated with hereditary nonpolyposis colorectal cancer (HNPCC). On the recommendation of his physician (a health care professional with appropriate training and expertise in the field of medicine involved), the individual undergoes a targeted genetic test to look for the specific mutation found in the family member of the individual to determine if the individual himself is at increased risk for cancer. The genetic test shows that the individual also carries the mutation but the individual's colonoscopy indicates no signs of disease and the individual has no symptoms. Because the individual has no signs or symptoms of colorectal cancer that could be used by the individual's physician to diagnose the cancer, HNPCC is not a manifested disease with respect to the individual. In contrast, if the individual undergoes a colonoscopy or other medical tests that indicate the presence of HNPCC, and the individual's physician makes a diagnosis of HNPCC, HNPCC is a manifested disease with respect to the individual.
- If a health care professional with appropriate expertise makes a diagnosis based on the symptoms of the patient, and uses genetic tests to confirm the diagnosis, the disease will be considered manifested, despite the use of genetic information. For example, if a neurologist sees a patient with uncontrolled movements, a loss of intellectual faculties, and emotional disturbances, and the neurologist suspects the presence of Huntington's disease, the neurologist may confirm the diagnosis with a genetic test. While genetic information is used as part of the diagnosis, the genetic information is not the sole or principal basis for the diagnosis, and, therefore, the Huntington's disease would be considered a manifested disease of the patient.

As with the definition of ''genetic test,'' the Department declines to include these examples in the regulatory text as this is inconsistent with the approach generally taken in the HIPAA Privacy Rule. The Department intends to issue future guidance on its web site with respect to the Rule's protections for genetic information.

g. Definition of ''Health Plan''

Proposed Rule

The Department proposed to make technical corrections to update the definition of ''health plan'' by revising and renumbering the definition to: Include specific reference to the Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Social Security Act, 42 U.S.C. 1395w–101 through 1395w–152; remove the specific reference to the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)), as this program is now part of the TRICARE health care program under title 10 of the United States Code, and revise the reference to the title 10 health care program accordingly to read more generally ''health care program for the uniformed services'' rather than ''health care program for active military personnel''; and reflect that Part C of title XVIII of the Social Security Act, 42 U.S.C. 1395w–21 through 1395w–28, is now called the Medicare Advantage program.

Overview of Public Comments

The Department did not receive any comments on the proposed technical corrections to the definition of ''health plan.''

Final Rule

The final rule incorporates the technical corrections to the definition.

4. Section 164.501—Definitions

The Department proposed to modify § 164.501 to add a definition of ''underwriting purposes'' and to make conforming changes to the definitions of ''payment'' and ''health care operations.''

a. Definition of ''Underwriting Purposes''

Proposed Rule

Section 105 of GINA provides that the term ''underwriting purposes'' means, with respect to a group health plan, health insurance coverage, or Medicare supplemental policy: (A) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy; (B) the computation of premium or contribution amounts under the plan, coverage, or policy; (C) the application of any pre-existing condition exclusion under the plan, coverage, or policy; and (D) other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

The Department proposed to adopt GINA's statutory definition of ''underwriting purposes'' in § 164.501 of the Privacy Rule, but also proposed to include certain clarifications for consistency with the regulations promulgated to implement the nondiscrimination provisions in sections 101 through 103 of GINA. In particular, the Department proposed to include a parenthetical to explain that the rules for, or determination of eligibility for, or determination of, benefits under the plan include changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program. The proposed rule also included a parenthetical to make clear that the computation of premium or contribution amounts under the plan, coverage, or policy includes discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program. Finally, we proposed a provision within the definition to clarify that ''underwriting purposes'' does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

Overview of Public Comments

About ten commenters addressed the proposed definition of ''underwriting purposes.'' Four commenters generally supported the proposed definition. Other commenters expressed concern with the definition's inclusion of discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment (HRA) or participating in a wellness program. These commenters were concerned that prohibiting the use of genetic information, particularly family health history, for such purposes would have a detrimental impact on wellness and disease management programs. One commenter was concerned that the definition would prohibit dental insurance plans from offering preventive prognostic features to enrollees as part of the plan that test for susceptibility to dental decay and periodontal diseases. Enrollees that test positive would be provided with additional plan benefits as a supplement to the standard benefits to cover more aggressive preventive services. Finally, a few commenters were concerned that the broad definition of ''underwriting purposes'' would preclude plans from using HRAs and offering wellness programs even if no genetic information is requested or used. For example, one commenter was concerned that the definition would prohibit the use of ''personal habit'' information, such as information about smoking, or alcohol or drug use.

Final Rule

The final rule adopts the proposed definition of ''underwriting purposes'' but moves the definition to within the underwriting prohibition at § 164.502(a)(5)(i). This makes clear that the definition applies only for purposes of the prohibition on a health plan's use or disclosure of genetic information for underwriting purposes. As discussed more fully below with respect to the definition of ''health care operations,'' we move the definition of ''underwriting purposes'' and retain the term ''underwriting'' within the definition of ''health care operations'' in response to several public comments expressing concern that the proposed rule would no longer allow health plans to use or disclose any protected health information (i.e., even non-genetic information) for underwriting.

The adopted definition is consistent with the definition promulgated in the interim final regulations to implement sections 101–103 of GINA and with which compliance is already required by most health plans. We decline to exclude wellness programs and the use of HRAs from the definition because, as discussed in the interim final regulations issued by DOL, Treasury, and HHS, GINA Title I does not include an exception for wellness programs.[20] However, we emphasize that health plans may continue to provide incentives for completing HRAs and participating in wellness programs in manners that do not involve the use or disclosure of genetic information. For example, ''personal habit'' information about an individual, such as smoking status and alcohol and drug use, is not genetic information and thus, may be used by health plans for underwriting purposes. Further, DOL has issued guidance which makes clear that health plans may continue to collect family health history through the use of HRAs that are not tied to any reward.[21]

In addition, the definition of ''underwriting purposes'' includes an exception for determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy. Thus, to the extent that an individual is seeking a particular benefit under the plan and the health plan needs genetic information to determine the medical appropriateness of providing the benefit to the individual, the plan may use or disclose the minimum necessary genetic information to determine the medical appropriateness of providing the benefit. For example, if a health plan covers yearly mammograms for individuals under age 40 only in cases where the individual can demonstrate she is at increased risk for breast cancer, the plan can ask an individual under age 40 to provide the results of a genetic test or family health history and use such information to determine medical appropriateness prior to paying a claim for the mammogram. The medical appropriateness exception would also cover situations where a dental plan requires the results of a genetic test prior to offering a supplemental benefit for more aggressive preventive services to the extent the individual seeks such a benefit. For example, a dental plan may provide information to all of its enrollees about how to take advantage of

[20] See 74 FR 51669, footnote 12.

[21] See Q14 at *http://www.dol.gov/ebsa/faqs/faq-GINA.html.*

such a benefit, and when an enrollee contacts the plan about obtaining the benefit, may require the individual to take and provide the results of a genetic test to determine the medical appropriateness of providing the supplemental benefit to the individual.

b. Definition of ''Health Care Operations''

Proposed Rule

The definition of ''health care operations'' at § 164.501 includes at paragraph (3) ''underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or benefits * * *.'' To avoid confusion with the use of both ''underwriting'' and ''underwriting purposes'' in the Privacy Rule, and in recognition of the fact that the proposed definition of ''underwriting purposes'' includes activities that fall within both the definitions of ''payment'' and ''health care operations'' in the Rule, the Department proposed to remove the term ''underwriting'' from the definition of ''health care operations.'' We also proposed to add the term ''enrollment'' to the express list of health care operations activities to make clear that the removal of the term ''underwriting'' would not impact the use or disclosure of protected health information that is not genetic information for enrollment purposes. These proposed revisions were not intended to be substantive changes to the definition and thus, health plans would be permitted to continue to use or disclose protected health information, except genetic information, for underwriting purposes.

Overview of Public Comments

The Department received a few comments on the proposed revisions to the definition of ''health care operations.'' One commenter supported the inclusion of the word ''enrollment.'' A few commenters, however, expressed concern and confusion that the removal of the term ''underwriting'' from the definition of ''health care operations'' would no longer permit uses or disclosures of even non-genetic protected health information for underwriting.

Final Rule

Due to the confusion and concern expressed by the commenters regarding the removal of the term ''underwriting'' from the definition, we retain the term ''underwriting'' within the definition of ''health care operations'' at § 164.501 However, to make clear that a health plan may continue to use or disclose only protected health information that is not genetic information for underwriting, we include a reference to the prohibition on using or disclosing genetic information for underwriting purposes within the definition. The final rule also retains the term ''enrollment'' within the definition because we believe it is helpful to clarify that this is a permitted health care operations activity.

c. Definition of ''Payment''

Proposed Rule

The definition of ''payment'' in the Privacy Rule at § 164.501 includes activities, such as ''determinations of eligibility or coverage'' by a health plan, some of which may fall within the definition of ''underwriting purposes.'' To avoid any implication that a health plan would be permitted to use or disclose protected health information for ''payment'' purposes that are otherwise prohibited by the underwriting prohibition, we proposed to include a cross-reference in the definition of ''payment'' to the prohibition. Further, we believed the inclusion of such a cross-reference to be necessary to properly align the definition of ''payment'' in the Privacy Rule with the nondiscrimination provisions of GINA Title I and their implementing regulations. GINA provides a rule of construction at section 102(a)(2), which adds paragraph 2702(c)(3) of the PHSA, to make clear that health plans are not prohibited from obtaining and using the results of a genetic test in making determinations regarding payment, as such term is defined by the HIPAA Privacy Rule. Thus, the proposed exception would make clear that GINA's rule of construction regarding payment does not allow a health plan to use the results of genetic tests for activities that would otherwise constitute ''underwriting purposes,'' such as for determinations of eligibility for benefits.

Overview of Public Comments

The Department received two comments on the proposed change to the definition of ''payment,'' one supporting the change and one indicating it is unnecessary.

Final Rule

For the reasons described above, the final rule adopts the proposed change to the definition of ''payment.''

5. Section 164.502(a)—Uses and Disclosures of Protected Health Information: General Rules

a. Prohibition

Proposed Rule

To implement section 105 of GINA, the Department proposed a new prohibition on health plans using or disclosing protected health information that is genetic information for underwriting purposes at § 164.502(a)(3). We made clear that such a provision would operate notwithstanding the other provisions in the Privacy Rule permitting uses and disclosures, and proposed a conforming change to § 164.502(a)(1)(iv) to clarify further that an authorization could not be used to permit a use or disclosure of genetic information for underwriting purposes.

Overview of Public Comments

Some commenters expressly supported the proposed modification to the Privacy Rule to include the prohibition, and the proposed clarification that an authorization cannot be used to otherwise permit a prohibited use or disclosure of genetic information. One commenter suggested adding the examples from the preamble to the regulatory text, as well as language to the regulatory text to clarify that the prohibition applies to genetic information obtained by a health plan prior to the passage of GINA.

Final Rule

The final rule adopts the proposed prohibition on a health plan's use or disclosure of genetic information for underwriting purposes, except with regard to health plans that are issuers of long term care policies, as explained above in section VI.C.1 regarding to which plans the final rule applies. This prohibition, located in this final rule at § 164.502(a)(5), applies to all genetic information from the compliance date of these modifications forward, regardless of when or where the genetic information originated. We do not believe a clarification of this fact in the regulatory text is necessary.

Consistent with Sec. 101(a) of the statute, this prohibition should not be construed to limit the ability of a health plan to adjust premiums or contribution amounts for a group health plan based on the manifestation of a disease or disorder of an individual enrolled in the plan, even though a health plan cannot use the manifestation of a disease or disorder in one individual as genetic information about other group members and to further increase the premium for the plan. Similarly, for the individual

health insurance market, a health plan is not prohibited from establishing rules for eligibility for an individual to enroll in coverage or from adjusting premium or contribution amounts for an individual based on the manifestation of a disease or disorder in that individual or in a family member of such individual where such family member is covered under the individual's policy, even though the health plan cannot use the manifestation of a disease or disorder in one individual as genetic information about other individuals to further increase premiums or contribution amounts for those other individuals.

To illustrate how the prohibition operates, we reiterate the following examples (but for the reasons explained above, decline to include them in the regulatory text). If a health insurance issuer, with respect to an employer-sponsored group health plan, uses an individual's family medical history or the results of genetic tests maintained in the group health plan's claims experience information to adjust the plan's blended, aggregate premium rate for the upcoming year, the issuer would be using protected health information that is genetic information for underwriting purposes in violation of § 164.502(a)(5)(i). Similarly, if a group health plan uses family medical history provided by an individual incidental to the collection of other information on a health risk assessment to grant a premium reduction to the individual, the group health plan would be using genetic information for underwriting purposes in violation of § 164.502(a)(5)(i).

The prohibition is limited to health plans. A health care provider may use or disclose genetic information as it sees fit for treatment of an individual. If a covered entity, such as an HMO, acts as both a health plan and health care provider, it may use genetic information for purposes of treatment, to determine the medical appropriateness of a benefit, and as otherwise permitted by the Privacy Rule, but may not use such genetic information for underwriting purposes. Such covered entities, in particular, should ensure that appropriate staff members are trained on the permissible and impermissible uses of genetic information.

6. Section 164.504(f)(1)(ii)—Requirements for Group Health Plans

Proposed Rule

Section 164.504(f)(1)(ii) permits a group health plan, or health insurance issuer or HMO with respect to the group health plan, to disclose summary health information to the plan sponsor if the plan sponsor requests the information for the purpose of obtaining premium bids from health plans for providing health insurance coverage under the group health plan, or for modifying, amending, or terminating the group health plan. As this provision permits activities that constitute ''underwriting purposes,'' as defined by GINA and the proposed rule, the Department proposed to modify § 164.504(f)(1)(ii) to clarify that § 164.504(f)(1)(ii) would not allow a disclosure of protected health information that is otherwise prohibited by the underwriting prohibition.

Overview of Public Comments

The Department received one comment in support of this modification.

Final Rule

The final rule adopts the modification to § 164.504(f)(1)(ii).

7. Section 164.506—Uses and Disclosures To Carry Out Treatment, Payment, or Health Care Operations

Proposed Rule

Section 164.506(a) of the Privacy Rule sets out the uses and disclosures a covered entity is permitted to make to carry out treatment, payment, or health care operations. In light of the fact that the proposed definition of ''underwriting purposes'' encompasses activities that fall both within the definitions of ''payment'' and ''health care operations'' under the Privacy Rule, the Department proposed to add a cross-reference in § 164.506(a) to the new underwriting prohibition to make clear that § 164.506 of the Privacy Rule would not permit health plans to use or disclose an individual's protected health information that is genetic information for underwriting, even though such a use or disclosure is considered payment or health care operations.

Overview of Public Comments

The Department received one comment in support of this modification.

Final Rule

The final rule adopts the modification to § 164.506(a).

8. Section 164.514(g)—Uses and Disclosures for Activities Relating to the Creation, Renewal, or Replacement of a Contract of Health Insurance or Health Benefits

Proposed Rule

Section 164.514(g) of the Privacy Rule prohibits a health plan that receives protected health information for underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract for health insurance or health benefits, from using or disclosing such protected health information for any other purpose (except as required by law) if the health insurance or health benefits are not placed with the health plan. The Department proposed conforming amendments to § 164.514(g) to: (1) Remove the term ''underwriting'' to avoid confusion given the new definition of ''underwriting purposes,'' which encompasses the activities described above; and (2) make clear that a health plan that receives protected health information that is genetic information for the above purposes is not permitted to use or disclose such information for underwriting purposes. The proposed removal of the term ''underwriting'' from § 164.514(g) was not intended as a substantive change to the scope of the provision.

Overview of Public Comments

One commenter suggested that the Department reconsider the removal of the term ''underwriting'' from this section as it could be viewed as a substantive change to the scope of the provision, and expressed concern that the modification would prohibit a health plan from using or disclosing genetic information as required by other law.

Final Rule

The final rule modifies § 164.514(g) to refer to the prohibition, now at § 164.502(a)(5). However, as with the definition of ''health care operations,'' we do not remove the term ''underwriting'' to avoid unnecessary confusion. We also clarify that a health plan may continue to use or disclose protected health information that is genetic information as required by other law, except to the extent doing so would be inconsistent with the prohibition in GINA and this final rule at § 164.502(a)(5)(i) against using or disclosing genetic information for underwriting purposes.

9. Section 164.520—Notice of Privacy Practices for Protected Health Information

Proposed Rule

As discussed above in Section IV with regard to the changes made to § 164.520 pursuant to the HITECH Act, § 164.520 of the Privacy Rule sets out the requirements for most covered entities to have and distribute a Notice of Privacy Practices (NPP). With respect to the NPP, the Department believes that

individuals should be informed of their new rights and protections under this rule with respect to genetic information in the health coverage context. Thus, the Department proposed in § 164.520(b)(1)(iii)(D) to require health plans that use or disclose protected health information for underwriting to include a statement in their NPP that they are prohibited from using or disclosing protected health information that is genetic information about an individual for such purposes. Without such a specific statement, individuals would not be aware of this restriction and the general statements regarding permitted uses and disclosures for treatment, payment, and health care operations in the NPP of a health plan that performs underwriting would not be accurate (i.e., the NPP would state that the health plan may use or disclose PHI for purposes of payment and health care operations, which would not be true with respect to genetic information when the use or disclosure is for underwriting purposes).

The preamble explained that the proposed prohibition on using or disclosing genetic information for underwriting and the proposed requirement to explicitly include a statement regarding the prohibition would represent a material change to the NPP of health plans that perform underwriting, and the Privacy Rule requires at § 164.520(c)(1)(i)(C) that plans provide notice to individuals covered by the plan within 60 days of any material revision to the NPP. As in the NPRM issued to implement HITECH Act provisions, the Department requested comment on ways to inform individuals of this change to privacy practices without unduly burdening health plans and provided several possible alternatives. The Department also explained that the obligation to revise the NPP for the reasons described above would fall only on health plans that intend to use or disclose protected health information for activities that constitute ''underwriting purposes.'' Thus, health care providers, as well as health plans that do not perform underwriting, would not be required to revise their NPPs.

Overview of Public Comments

One commenter supported informing individuals in the NPP that health plans are prohibited from using or disclosing genetic information for underwriting purposes. One commenter asked the Department to clarify that where a health plan has already made a change to the NPP to comply with a statute, such as with GINA, and has sent the revised NPP to members, the health plan would not be required to make another change to its NPP to comply with the regulation.

A number of comments addressed the issue of the timing and manner of distributing revised NPPs. In general, commenters recommended various alternatives, including: (1) Require health plans to provide a revised NPP to members in the next annual mailing; (2) require health plans to provide either a revised NPP or a supplement to members in the next annual mailing and to post the revised NPP or supplement on the health plan Web site immediately; (3) retain the existing 60-day deadline for providing a revised NPP to individuals or provide for a 30-day extension; and (4) allow for distribution via electronic processes for more efficient delivery of NPPs to members.

Final Rule

The final rule adopts the requirement for health plans that perform underwriting to include in their NPPs a statement that they are prohibited from using or disclosing genetic information for such purposes, except with regard to issuers of long term care policies, which are not subject to the underwriting prohibition. Health plans that have already modified and redistributed their NPPs to reflect the statutory prohibition are not required to do so again, provided the changes to the NPP are consistent with this rule. We also modify the NPP distribution requirements for health plans where there are material changes. These modifications are discussed above in Section IV with regard to material changes to the NPP resulting from changes pursuant to the HITECH Act.

10. Other Comments

Comment: One commenter requested clarification on preemption with regard to the new underwriting prohibition.

Response: Pursuant to subpart B of Part 160 of the HIPAA Administrative Simplification Rules, to the extent that a provision of State law requires a use or disclosure of genetic information for an activity that would otherwise constitute ''underwriting purposes,'' such State law would be preempted by the Privacy Rule unless an exception at § 160.203 applies. In contrast, State laws that provide greater privacy protection for genetic information than the Privacy Rule continue to remain in place.

Comment: One commenter asked how a health care provider should ensure that releasing an individual's information to a health plan will not result in an inappropriate disclosure to the health plan for underwriting purposes. This commenter also asked what the rules are for access to protected health information about an individual by the individual's extended family members seeking to determine if they are affected by a genetic trait.

Response: With respect to the first question, these rules do not apply to health care providers. A covered health provider may continue to disclose protected health information, including genetic information, where doing so meets the minimum necessary standard, to health plans for payment purposes. Under this Rule, the onus is on the health plan to not use or disclose protected health information it receives for such purposes for prohibited underwriting purposes. Further, health plans continue to be required by the Privacy Rule to limit requests of protected health information to the minimum necessary when requesting such information from other covered entities. The regulations implementing sections 101–103 of GINA also restrict the ability of health plans covered by those rules to request genetic information.

With respect to the second question, to the extent that an individual's genetic information is needed for the treatment purposes of a family member, a covered health care provider is permitted to disclose such information, subject to any agreed-upon restriction, to another provider for the treatment of the family member. See FAQ #512 at *http://www.hhs.gov/ocr/privacy/hipaa/faq/right_to_request_a_restriction/512.html*, which makes clear that a health care provider may share genetic information about an individual with providers treating family members of the individual who are seeking to identify their own genetic health risks, provided the individual has not requested and the health care provider has not agreed to a restriction on such disclosure.

Comment: One commenter requested that the rule require that health plans conducting or sponsoring research involving genetic information provide research participants with an explicit statement to ensure the individuals understand that such information may not and will not be used for underwriting purposes.

Response: We decline to require such a statement. The regulations implementing sections 101–103 of GINA already require a statement to that effect as a condition of the health plan requesting that a research participant undergo a genetic test as part of the research. See, e.g., 45 CFR 144.122(c)(5). Further, this rule requires that health plans that perform underwriting inform individuals through their NPPs that the

plans may not use or disclose genetic information for such purposes.

Comment: One commenter asked that the HIPAA de-identification standard be strengthened to provide better protection for health information, including genetic information.

Response: The Privacy Rule's de-identification standard is outside the scope of this rulemaking.

VII. Regulatory Analyses

A. Introduction

We have prepared a regulatory impact statement in compliance with Executive Order 12866 (September 1993, Regulatory Planning and Review), Executive Order 13563 (January 2011, Improving Regulation and Regulatory Review), the Regulatory Flexibility Act (RFA) (September 19, 1980, Pub. L. 96–354), the Unfunded Mandates Reform Act of 1995 (UMRA) (March 22, 1995, Pub. L. 104–4), and Executive Order 13132 on Federalism. We begin with a discussion of Executive Orders 12866 and 13563 and then present a more detailed analysis of costs and benefits. Finally, relying on information explained in the cost-benefit analysis, we discuss issues related to the RFA, UMRA, and Federalism considerations.

1. Executive Order 12866 and Executive Order 13563

Executive Orders 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. A regulatory impact analysis must be prepared for major rules that have economically significant effects ($100 million or more in any one year) or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or Tribal government or communities (58 FR 51741). Based on the following analysis, this rule has been designated as an economically significant regulatory action within the meaning of section 3(f)(4) of Executive Order 12866. Accordingly, the rule has been reviewed by the Office of Management and Budget.

To summarize, we estimate that the rule will result in new first-year costs of between $114 million and $225.4 million. Annualizing the midpoints of our cost estimates at three and seven percent over ten years produces costs of $35.2 million and $42.8 million, respectively.[22]

We estimate that the effects of the requirement for covered entities (including indirect costs incurred by third party administrators, which frequently send out notices on behalf of health plans) to issue new notices of privacy practices, as a result of the final changes to the HIPAA Privacy Rule under both the HITECH Act and GINA, will result in new costs of $55.9 million within 12 months of the effective date of the final rule. Annualizing the costs over 10 years at 3 percent and 7 percent results in annual NPP costs of approximately $6.6 million and $8 million, respectively. We have revised our cost estimate for NPP revisions since the proposed rule to reflect the increased flexibility provided in the final rule, which allows health plans to include their new NPPs in their usual, annual mailing rather than send them to individuals in a separate mailing. We also note that combining GINA and HITECH requirements into a single rule results in lower costs than would be incurred if covered entities were required to revise their NPPs multiple times to comply with separate rulemakings.

Additionally, we have revised the annual estimated cost to comply with the final breach notification provisions. As we discuss below, we acknowledge there may still be some underreporting of breaches, however we do anticipate that the overall number of breaches will decrease in the future. As such, Table 2 below shows the costs of complying with the provisions of the breach notification final rule, which have been revised based on our experience with the number of breach notifications we have received from covered entities during calendar years 2010 and 2011. We estimate the total annual cost for the breach notification rule to be approximately $14.5 million. Annualizing over 10 years at 3% and 7% produces annual breach implementation costs of approximately $17 million and $20.6 million.

With regard to the business associate provisions of the final rule, we assume that business associates currently comply with the HIPAA Privacy Rule use and disclosure provisions as required by their business associate contracts. However, with regard to the Security Rule, while we continue to believe that most business associates have implemented security protections that meet the Security Rule requirements as part of the assurances provided to covered entities through their contracts, we recognize that some smaller or less sophisticated business associates may not have engaged in the formal administrative safeguards required by the HIPAA Security Rule, and may not have written policies and procedures for compliance. For these business associates, we estimate that the costs to come into compliance with the Security Rule will be between approximately $22.6 million and $113 million. Annualizing the midpoint estimate ($67.8 million) at 3 percent and 7 percent produces costs of $7.9 million and $9.7 million, respectively.

Although we also continue to believe that most business associates have made a good faith attempt to conform their agreements with subcontractors to HIPAA requirements, we acknowledge the possibility that some business associates may make such efforts for the first time now that they and their subcontractors are subject to direct liability under the Rules. For this fraction of business associates, we estimate that the costs to bring subcontracts into compliance with the business associate agreement requirements will be between $21 million and $42 million. Annualizing the midpoint of those estimates ($31.5 million) at 3 percent and 7 percent results in costs of $3.7 million and $4.5 million, respectively.

There may be other costs we are not able to monetize because we lack data, and the rule may produce savings that may offset some or all of the added costs. We discuss these unquantified costs and benefits of the rule at the end of the Regulatory Impact Analysis.

As a result of the economic impact, and other costs that are described but not quantified in the regulatory analysis below, OMB has determined that this rule is an economically significant regulatory action within the meaning of section 3(f)(4) of Executive Order 12866. We present our analysis of the costs and benefits of the rule in sections C and D below.

2. Entities Subject to the Rule

This rule impacts covered health care providers, health insurance issuers, and third party administrators acting on behalf of health plans, which we estimate to total 698,238 entities. The rule also applies to approximately 1–2

[22] The breach notification provisions are the rule's only source of ongoing, annual costs. Therefore, with respect to breach, we annualize costs incurred on an annual basis. For the other provisions, we calculate annualized opportunity costs based on costs expended only in the first year of implementation.

million business associates and an unknown number of subcontractors.[23]

Table 1 below shows the number of covered entities by class of provider and insurer that will be affected by the Rule.

TABLE 1—NUMBER OF COVERED ENTITIES BY NAICS CODE[24]

NAICS	Providers/suppliers	Number of entities	Estimated number of small entities[25]
622	Hospitals (General Medical and Surgical, Psychiatric, Substance Abuse, Other Specialty).	4,060	4,060
623	Nursing Facilities (Nursing Care Facilities, Residential Mental Retardation Facilities, Residential Mental Health and Substance Abuse Facilities, Community Care Facilities for the Elderly, Continuing Care Retirement Communities).	34,400	34,400
6211–6213	Office of MDs, DOs, Mental Health Practitioners, Dentists, PT, OT, ST, Audiologists.	419,286	419,286
6214	Outpatient Care Centers (Family Planning Centers, Outpatient Mental Health and Drug Abuse Centers, Other Outpatient Health Centers, HMO Medical Centers, Kidney Dialysis Centers, Freestanding Ambulatory Surgical and Emergency Centers, All Other Outpatient Care Centers).	13,962	13,962
6215	Medical Diagnostic, and Imaging Service Covered Entities.	7,879	7,879
6216	Home Health Service Covered Entities	15,329	15,329
6219	Other Ambulatory Care Service Covered Entities (Ambulance and Other).	5,879	5,879
N/A	Durable Medical Equipment Suppliers[26]	107,567	107,567
4611	Pharmacies[27]	88,396	88,396
524114	Health Insurance Carriers[28]	730	276
524292	Third Party Administrators Working on Behalf of Covered Health Plans[29].	750	750
Total Entities		698,238	697,784

B. Why is this rule needed?

This final rule is needed to strengthen and expand the privacy and security protections for individuals' health information and privacy rights established under the HIPAA, as mandated by the HITECH Act and GINA. These enhancements are necessary to ensure continued adequate protections for health information, as well as trust in the health care system, particularly as the adoption and use of electronic health records increases. Importantly, among other changes, the rule makes business associates of covered entities directly liable for Federal penalties for failures to comply with certain provisions of the rule. This expansion in liability closes a large gap in protection that existed prior to these modifications with respect to business associates, which are the cause of many of the security breaches for which the Department receives breach reports.

The final rule also lays out standards for when individuals and the Secretary must be informed that a breach of protected health information has occurred so that individuals may take measures to protect themselves from risks associated with the breach. By establishing requirements for notifying individuals and making business associates directly liable for complying with certain provisions of the Privacy and Security rules, we expect the number of breaches of protected health information to decline over time.

This final rule also makes changes to the HIPAA rules, such as those that streamline the research authorization process, that are designed to increase flexibility for, and decrease burden on, the regulated entities, as well as to harmonize certain requirements with those under the Department's Human Subjects Protections regulations.

C. Costs

1. Breach Notification Costs

The preamble to the interim final rule published on August 24, 2009, contained a regulatory impact statement estimating the economic burden of implementing the rule. We are revising that impact statement in this final rule based upon our experience with collecting breach notifications from covered entities during calendar years 2010 and 2011.

The analysis that follows is very similar to the analysis set forth in the preamble to the interim final rule; however, instead of using information

[23] Although we do not have data on the numbers of business associates, our enforcement experience leads us to believe that each covered entity has, on average, two to three business associates, for a total of 1–2 million business associates. This number likely overestimates the number of business associates, as some entities may be business associates to multiple covered entities. We do not have a basis for estimating the number of subcontractors that will be subject to the rule.

[24] Office of Advocacy, SBA, *http://www.sba.gov/advo/research/data.html.*

[25] Because the vast majority of covered providers are small entities, we include all providers in our estimates of small providers.

[26] Centers for Medicare & Medicaid Services covered entities.

[27] The Chain Pharmacy Industry *http://www.nacds.org/wmspage.cfm?parm1=507.*

[28] Source: HHS ASPE analysis of 2010 NAIC Supplemental Health Care Exhibit data.

[29] We include third party administrators in our count of covered entities, although they are business associates, because the nature of their representation of the majority of ERISA plans makes them an appropriate ''surrogate'' for those plans.

from *http://www.datalossdb.org* to estimate the number of breaches that would occur each year, we have used the breach notifications provided to the Secretary during calendar years 2010 and 2011 to project the ongoing, annual costs to covered entities for implementing the breach notification provisions. Several commenters noted that significantly more breaches would occur each year than the interim final rule anticipated, and we acknowledge that the estimates provided in the interim final rule were significantly lower than our experience has been to date. As such, we believe that relying on our experience receiving notifications addresses the concerns of the commenters who thought we were underestimating the number of breaches that would occur each year. Based upon this information, we have revised the projected annual cost to implement these breach notification provisions.

We acknowledge that there may still be some underreporting of breaches as the obligations of the regulation may not yet have penetrated down to all covered entities and business associates. At the same time, we expect that some types of incidents being reported today may not in the future as covered entities and business associates become more familiar with the definition of breach and more adept at performing risk assessments and determining whether a breach has occurred. We have received breach notifications from covered entities in several situations in which notification was not necessary, such as where there was no underlying impermissible use or disclosure under the Privacy Rule or where one of the exceptions to breach clearly applied to the situation. This is the type of over-reporting that we expect to diminish in the future. Additionally, covered entities and business associates are beginning to recognize areas of potential weakness and to take systemic actions to prevent breaches from occurring in the future, such as encrypting portable devices to avoid having to provide breach notifications in the event the device is lost or stolen.

Table 2 shows the costs of the provisions of the final rule based on the breach notifications we have received from covered entities during calendar years 2010 and 2011. We also present the costs required for investigating breaches and the amount of time we anticipate individuals will spend calling the toll-free number for substitute notice. We estimate the total cost for the breach notification rule to be approximately $14.5 million. Discounting at 3 percent and 7 percent and annualizing over 10 years results in costs of $17 million and $20.6 million, respectively.

TABLE 2—SUMMARY OF ANNUAL COMPLIANCE COST FOR BREACH NOTIFICATION IN 2011 DOLLARS

Cost elements	Number of breaches	Number of affected individuals	Cost/breach	Cost/affected individuals	Cost
E-mail and 1st Class Mail	19,000	6,710,000	$182	$0.517	$3,467,122
Substitute Notices: Media Notice	1,190	6,605,500	480	0.086	571,200
Substitute Notices: Toll-Free Number	1,190	[30] 660,550	1,526	2.750	1,816,379
Imputed cost to affected individuals who call the toll-free line	1,190	660,550	1,725	3.108	2,052,665
Notice to Media of Breach: Over 500	250	6,600,000	62	0.002	15,420
Report to the Secretary: 500 or More	250	6,600,000	62	0.002	15,420
Investigation Costs: Under 500	18,750	324,050	281	16.29	5,277,456
Investigation Costs: 500 or More	250	6,600,000	3,350	0.127	837,500
Annual Report to the Secretary: Under 500	18,750	110,000	23	3.84	422,438
Total Cost					14,475,600

[30] As we explain below in the section on substitute notice, we project that 6,605,500 individuals will be affected by breaches that may require substitute notice, but we expect that at most 10% of affected individuals will call the toll-free line for information.

In this revised analysis, we rely entirely on our experience with breach notifications received by the Secretary during calendar years 2010 and 2011, for projecting the ongoing, annual costs of the breach notification rule. Based on our experience in those years, we project the likely number of breaches, number of affected individuals, and costs associated with this regulation. We have not attempted to predict future costs because, as discussed above, while we anticipate the overall number of breaches and the overall costs of implementing the breach notification provisions to fall over time, we do not currently have enough data to establish such a trend.

Affected Entities

The entities affected by the breach notification regulation are outlined in the impact statement of the interim final rule. HIPAA covered entities and their business associates must comply with these regulations. We estimate that approximately 700,000 HIPAA covered entities will be subject to the final rule, although many fewer will experience a breach requiring them to fulfill the breach notification requirements.

How many breaches will require notification?

Although this final rule modifies the definition of breach at § 164.402 to remove the harm standard, we do not believe that this will have a significant effect on the number of breaches reported to HHS or on the number of individuals affected. As discussed in Section V above, this final rule removes the harm standard and implements a more objective risk assessment for evaluating whether an impermissible use or disclosure is a breach. As a result, covered entities must still perform a risk assessment following an impermissible use or disclosure of protected health information to determine the probability that the protected health information has been compromised. Events such as hacking into an unencrypted database and theft of unsecured protected health information would in almost all cases constitute a breach in this final rule, just as they would under the interim final rule's definition of breach. However, given the further clarity in this rule as to the standard and factors to be considered, other incidents that may not have been considered a breach under the interim final rule may be considered a breach under this final rule (or in some cases, vice versa).

Instead of relying on data from *http://www.datalossdb.org* to estimate the number of breaches and the number of individuals affected by such breaches

each year, this final rule uses breach notification reports submitted to the Secretary by covered entities to revise our previous estimates. We believe these reports provide us with much more complete information from which to project the overall cost of implementing this regulation.

Beginning September 23, 2009, covered entities were obligated to notify the Secretary of all breaches of protected health information occurring on or after that date. As of September 23, 2009, covered entities must report breaches affecting 500 or more individuals to the Secretary without unreasonable delay and in no case later than 60 days from discovery of the breach, while breaches affecting fewer individuals must be reported to the Secretary within 60 days of the end of the calendar year in which the breach occurred.

Based on our experience receiving breach notifications during calendar years 2010 and 2011, we project that HHS will receive approximately 19,000 breach notifications from covered entities annually or, on average, approximately 1,583 breach notifications each month. Approximately 250 such notifications will report breaches affecting 500 or more individuals and the remaining 18,750 reported breaches will affect fewer than 500 individuals.

We project that approximately 6.71 million individuals will be affected by the 19,000 breaches reported to HHS each year, which is, on average, roughly 353 affected individuals per breach.

As in the interim final rule, we have assumed that no State has a notification requirement, despite the fact that this will overestimate the burden imposed on covered entities because covered entities have trained their staffs and have prepared procedures to follow when a breach occurs to comply with existing breach notification requirements of most of the States. To ameliorate the overstatement of our cost estimate somewhat, we have assumed the costs for training personnel and for developing procedures for the most part have already been expended and are therefore in the baseline. We did not include these costs in our analysis of the annual costs.

We have followed the same approach to estimating the costs as outlined in the interim final rule. We examined the cost of notifying affected individuals by first class mail, issuing substitute notice in major media or on a Web site along with a toll-free phone number, notifying prominent media in the event of a breach involving more than 500 individuals, and notifying the Secretary of a breach, as well as the costs of investigating and documenting breaches. Some commenters requested that we include the cost of modifying contracts with business associates to potentially define the breach notification obligations between the parties. We note that costs to modify business associate agreements generally to comply with the new HITECH provisions are discussed elsewhere in this impact analysis.

Cost of Notifying Affected Individuals by First Class Mail or Email

Section 164.404 requires all covered entities to notify affected individuals of a breach either by first class mail, or if the individual has agreed, by email. In the interim final rule, we assumed that approximately one half of notices sent to affected individuals would be sent via first-class mail, while the rest would be sent via email. By comparison, in the Federal Trade Commission's (FTC) final breach notification rule, the FTC assumed that 90 percent of the notices sent to individuals affected by a breach requiring notification under the FTC rule would be emailed and only 10 percent would be sent by regular first class mail. Since the firms that the FTC regulates are primarily web-based, assuming that the vast majority of communications would be conducted through email is a reasonable assumption. For HIPAA covered entities, however, 90 percent of which are small businesses or nonprofit organizations that engage the entire U.S. population in providing health care services, we believed that notification through email would be much more limited than in the case of the entities the FTC regulates. Some physician offices have been slow to adopt email communication with their patients for various reasons. We, therefore, assumed that only 50 percent of individuals affected as a result of a breach of unsecured protected health information would receive email notices. As we did not receive any comments on this assumption, we retain it here.

As discussed in our analysis in the interim final rule, there will be certain costs that both email and first-class mail notification will share. The cost of drafting and preparing the notice will apply to both forms. The median hourly wage for the labor category of a healthcare practitioner and technical worker in 2011 was approximately $42.96, including 50 percent for fringe benefits.[31] If we assume 30 minutes per breach for composing the letter, the cost equals $21.48. We assume that it will also take 30 minutes per breach for an administrative assistant to prepare the letter in either email or printed formats and to document the letter to comply with §§ 164.414(a) and 164.530(j). The median hourly wage for office and administrative support staff is $22.53, including 50 percent for benefits. For the 30 minutes, we estimate $11.27 per breach. The combined labor cost for composing and preparing the document is approximately $32.75 per breach. Half of this cost will be allocated to the first-class letter and the other half to the emails.

Although computer costs for sending email will be insignificant, it will take staff time to select the email address from the entity's mailing list. We assume that an office worker could process and send 200 emails per hour at a cost of $22.53 per hour. For each mailed notice, we assume $0.06 for paper and envelope and $0.45 for a first class stamp, totaling $0.51 per letter. We estimate another $22.53 per hour to prepare the mailing by hand at a rate of 100 letters per hour.

Based on our revised estimate of the number of breaches that will occur in a year, we can multiply the number of breaches by the cost of composing and preparing a notice (19,000 × $32.75) equals $622,250. Allocating half the costs to emailing and the same amount to regular mail yields $311,125 to each category.

Splitting our estimate of the number of affected individuals evenly between email and regular mail gives us 3,355,000 affected individuals for each notice category. As we did in the interim final rule, for emails we divide affected individuals by the number of emails processed in an hour (200) and multiply the result (16,775 hours) by the hourly cost of $22.53, giving us $377,940. To this number we add the $311,125 giving us an estimated cost for email notices of $689,066.

We follow the same method for estimating the cost of mailing notices using postal mail plus the cost of postage and supplies. Dividing 100 letters per hour into 3,355,000 yields 33,550 hours, which is then multiplied by $22.53 to reach $755,882 in labor costs to prepare the mailing. Adding to that the costs of postage and supplies ($1,711,050) and the costs of composing and drafting ($311,125) equals $2,778,057. Summing the cost of email and postal mail notices equals

[31] Department of Labor, Occupational Employment Statistics; Healthcare Practitioner and Technical Occupations. Available at *http://www.bls.gov/oes/current/oes_nat.htm.*

$3,467,122. Table 3 presents the results of our analysis in the order they are discussed above.

TABLE 3—COST OF E-MAIL AND FIRST CLASS MAIL TO AFFECTED INDIVIDUALS IN 2011 DOLLARS

(Annual)	Mail	Email	Total
Number of breaches	9,500	9,500	19,000
Number of affected individuals or records	3,355,000	3,355,000	6,710,000
Hours to compose and document notice	9,500 (1 hr per breach).	9,500 (1 hr per breach).	19,000
Cost to compose and document notice	$311,125	$311,125	$622,250
Hours to prepare mailing	33,550	16,775	50,325
Cost to prepare mailing	$755,882	$377,940	$1,133,822
Postage and supplies	$1,711,050	N/A	$1,711,050
Total	$2,778,057	$689,066	$3,467,122

Cost of Substitute Notice

In the event that a HIPAA covered entity is not able to contact an affected individual through email or postal mail, it must attempt to contact the person through some other means. If the number of individuals who cannot be reached through the mailings is less than ten, the entity may attempt to reach them by some other written means, or by telephone.

In the event that the covered entity is unable to contact 10 or more affected individuals through email or postal mail, the rule requires the entity to (1) publish a notice in the media (newspaper, television, or radio) or post a notice on its Web site, containing the same information contained in the mailed notice, and (2) set up a toll-free number. The toll-free number is to be included in the media notice or notice on the Web site.

Based on the breach notification reports received by the Secretary during calendar years 2010 and 2011, we project that approximately 1,190 breaches affecting 10 or more individuals will require substitute notice (including 5% of breaches involving fewer than 500 individuals, and all 250 breaches involving 500 or more individuals). While several breaches affecting only 1 individual have also required substitute notice, as stated in the interim final rule, we believe the costs for notifying fewer than 10 individuals through alternative written means or by telephone would be very small and as a result we have not attempted to estimate those costs.

The interim final rule estimated that it would cost approximately $240 to publish a public notice in a newspaper. Assuming the covered entity will publish two notices, the cost is $480. Multiplying this amount by the 1,190 estimated breaches yields $571,200. Also, as noted in the interim final rule, if a HIPAA covered entity has a Web site, we assume there will be no cost to post the notice to the Web site. We believe this overestimates the overall cost of publishing a notice, as many covered entities will elect to post the public notice only on their Web site, and not in a newspaper.

As outlined in the interim final rule, the cost of setting up a toll-free phone number is a straight forward process of contacting any one of a number of service providers who offer toll-free service. The interim final rule found that the prices for toll-free service range from $0.027 per minute for a basic mail box arrangement to $0.07 per minute. A major, national phone service company offers toll-free service for $15 per month per toll-free number and per minute charge of $0.07. There is a one-time charge of $15. As in the interim final rule, we use the costs of $15 per month plus $15 activation fee and $0.07 per minute.

Since the regulation requires providers to maintain a toll-free number for three months, the monthly charge plus initial fee per breach will be $60. To estimate the number of calls to the toll-free number, the interim final rule assumed that more individuals than those affected by the breach requiring substitute notice would call out of concern that their protected health information might have been compromised. The interim final rule estimated that a number equal to all affected individuals of all breaches would call the toll-free number. Based on our experience to date, and given that many individuals involved in breaches requiring substitute notice will receive regular notice, we now assume that less than 10 percent of individuals affected by breaches requiring substitute notice will call the toll-free line. Therefore, as we anticipate 6,605,500 total individuals will be affected by breaches requiring substitute notice,[32] we assume that no more than 10 percent, or 660,550, will call the toll-free number to determine if they are affected by the breach. We note that while this revision significantly reduces the overall cost to covered entities for providing substitute notice in situations in which there is insufficient or out-of-date contact information for 10 or more individuals, we believe this estimate is much more appropriate based on the information we have received from covered entities thus far.

Using this number and assuming that a call averages five minutes at $0.07 per minute, we estimate the total direct calling costs to equal $231,193. Added to this is $345,000 that represents the monthly fee per breach (1,190 breaches) for three months plus the one-time fee (totaling $60 per breach). This brings the total cost of setting up and maintaining toll-free lines to $576,193.

To this cost, we must also include the office staff time to answer the incoming calls at $22.53 per hour. Based on an average of five minutes per call, a staff person could handle 12 calls per hour. Dividing 12 into 660,550 equals approximately 55,046 hours and then multiplied by $22.53 equals $1,240,186. Summing all cost elements yields a total cost of $1,816,379.

To the degree that entities already maintain toll-free phone lines, our estimate overstates the costs of setting up a toll-free line as required under the rule. Table 4 presents our cost analysis for the toll-free line.

[32] This number includes all individuals affected by breaches involving 500 or more individuals (6,600,000) and 5 percent of individuals affected by breaches involving less than 500 individuals (5,500).

TABLE 4—ANNUAL COST FOR SETTING UP A TOLL-FREE LINE FOR THREE MONTHS IN 2011 DOLLARS

Costs	Number of breaches affecting fewer than 500 (5,500)	Number of breaches 500 + (250)	Number of calls	Total
Monthly Charges for 3 months + 1-time Charge ($60/breach)	$330,000	$15,000	N/A	$345,000
Direct Calling Charges @ $.07/min × 5 minutes			660,550	$231,193
Labor cost @ $22.53/hr × 5 min per call			660,550	$1,240,186
Cost to individuals @ $24.86/hr × 7.5 min per call			660,550	$2,052,665
Total				$3,869,044

As in the interim final rule, we have also imputed a cost to the time individuals will spend calling the toll-free number. In estimating the time involved, we assumed that a person will spend five minutes per call. However, the person may not get through the first time and thus may have to call back a second time which could add another 5 minutes. Taking the average between 5 and 10 minutes, we used an average time of 7.5 minutes per caller.

For purposes of imputing cost to an individual's time, we took the median compensation amount from the Bureau of Labor Statistics of $24.86 [33] for all occupations. Dividing 60 by 7.5 minutes yields 8 calls per hour. Dividing the number of calls per hour into 660,550 calls and then multiplying by $24.86, gives us a cost of $2,052,665.

Cost of Breaches Involving More Than 500 Individuals

If a covered entity experiences a breach of protected health information affecting more than 500 individuals of a State or jurisdiction, § 164.406 of the rule requires the entity to notify the media in the jurisdiction or State in which the individuals reside. In addition, § 164.408 of the rule requires the entity to notify the Secretary contemporaneously with notice to affected individuals in cases where 500 or more individuals are affected by a breach.

As stated in the interim final rule, we anticipate that a covered entity will issue a press release when it must notify the media under § 164.406. The tasks involved in issuing the press release will be the drafting of the statement and clearing it through the entity. As discussed in the interim final rule, we assume that drafting a one-page statement will contain essentially the same information provided in the notice to affected individuals and will take 1 hour of an equivalent to a GS–12 Federal employee, earning $29 per hour. Adding 50 percent to account for benefits equals $43.50. Approval of the release involves reading the document. We expect this activity to take 15 minutes. The median hourly rate for a public relations manager is approximately $44.86 in 2011.[34] Adding 50 percent for benefits equals $67.29, so one quarter of an hour equals $16.82 for approving the release. The total cost of the release equals $61.68, and multiplying this amount by the number of breaches affecting more than 500 individuals (250) equals $15,420. This amount is lower than our previous estimate because we have adopted the more customary and realistic approach of adding 50 percent to wages for benefits, rather than doubling standard wage rates to account for benefits. It should be noted that even this amount may overstate the actual costs of issuing a notice to the media.

The report to the Secretary that must be sent contemporaneously with the sending of the notices to the affected individuals will contain essentially the same information as the notice sent to the affected individuals. As stated in the interim final rule, we anticipate the time and cost to prepare the report will be the same as that required for issuing a notice to the media. The cost for reporting to the Secretary the 250 breaches affecting 500 or more individuals is $15,420.

Cost of Investigating a Breach

As a prerequisite to issuing a notice to individuals, to the media, and to the Secretary, the covered entity will need to conduct an investigation to determine the nature and cause of the breach. We estimate that the 95 percent of breaches in the under 500 category that affect fewer than 10 individuals will require 4 hours of investigation. The other 5 percent of under 500 breaches, which affect between 10 and 499 individuals, may require up to 8 hours to investigate. At an office manager's [35] time at $67 per hour ($44.65 median wage plus 50 percent for benefits) multiplied by 4 and 8 hours, results in per breach costs of approximately $268 and $536, respectively. Multiplying $268 by the number of breaches affecting fewer than 10 individuals (17,800 breaches) results in investigation costs of $4,773,616. We then multiply $536 by the number of breaches affecting 10 to 499 individuals (940 breaches), which produces investigation costs of $503,840. Adding the totals for the two groups results in investigation costs of $5,277,456 per year for breaches affecting less than 500 individuals. This estimate includes the time required to produce the documentation required by § 164.414(a). We note that this estimate is significantly higher than that in the interim final rule; however, this is due entirely to the revised estimate that there will be approximately 18,750 breaches affecting fewer than 500 individuals per year.

As stated in the interim final rule, for breaches involving 500 or more individuals, the breach investigation may take up to 100 hours to complete; however, we assume that the average investigation will take only 50 hours. At an office manager's time of $67 per hour multiplied by 50 hours, this cost equals $3,350 per breach. Multiplying this by the number of breaches (250) yields $837,500.

Cost of Submitting the Annual Breach Summary to HHS

Under § 164.408, covered entities must notify the Secretary of all breaches; however, covered entities reporting breaches affecting fewer than 500 individuals may report these breaches to the Secretary annually. Since the material for the submission has already been gathered and organized for the issuance of the notices to the affected individuals, we expect that notifying the Department will require at

[33] Department of Labor, Occupational Employment Statistics. *http://www.bls.gov/oes/current/oes_nat.htm.*

[34] *http://www.bls.gov/oes/current/oes_nat.htm.*

[35] See *www.bls.gov/oes/current/oes_nat.htm* for All Management Occupations.

most an hour of office staff time once per year. At $22.53 per hour multiplied by the total number of breaches (18,750) affecting fewer than 500 individuals, this cost equals $422,438.

2. Notifying Individuals of Their New Privacy Rights

Covered entities must provide individuals with NPPs that detail how the covered entity may use and disclose protected health information and explain individuals' rights with respect to their own health information. Because of changes to the HIPAA Rules as a result of the HITECH Act and GINA, the final rule requires covered entities to modify their NPPs and distribute them to individuals to advise them of the following: (1) For health plans that underwrite, the prohibition against health plans using or disclosing PHI that is genetic information about an individual for underwriting purposes; (2) the prohibition on the sale of protected health information without the express written authorization of the individual, as well as the other uses and disclosures for which the rule expressly requires the individual's authorization (i.e., marketing and disclosure of psychotherapy notes, as appropriate); (3) the duty of a covered entity to notify affected individuals of a breach of unsecured protected health information; (4) for entities that have stated their intent to fundraise in their notice of privacy practices, the individual's right to opt out of receiving fundraising communications from the covered entity; and (5) the right of the individual to restrict disclosures of protected health information to a health plan with respect to health care for which the individual has paid out of pocket in full.

For providers, the costs related to the NPP consist of developing and drafting the revised NPP, and, as discussed below, the potential to incur out-of-cycle printing costs for the revised notice. There are no new costs attributable to the distribution of the revised notice as providers have an ongoing obligation to hand out the NPPs when first-time patients come for their appointments. We estimate that drafting the updated NPPs will require approximately one-third of an hour of professional, legal time at a cost of about $28.[36] The total cost for attorneys for the approximately 697,000[37] health care providers in the U.S. is, therefore, expected to be approximately $20 million. Printing the NPPs involves production and supplies at a cost of $0.10 per notice. Based on our prior estimates, health care providers are currently required to print and provide the NPP to approximately 613 million new patients annually. We assume that most health care providers will spread the printing of their notices throughout the year, producing copies on a quarterly, monthly, or even more frequent schedule. Further, providers will have 8 months from the publication of the final rule before they will need to produce the revised NPPs, and, therefore, can use that time to adjust their inventory and printing schedule to transition to the revised notice without any additional expense. Thus, assuming a worst case scenario in which all providers would need to replace at most 4 months of old inventory with the revised notice, the need for off-schedule printing of the revised notice for this 4 month period would be attributed to this provision. We estimate, therefore, that providers will print not more than 204 million revised NPPs over and above their existing printing obligations ($4/12 \times 613$ million = 204 million). Printing costs for 204 million NPPs will be $20.4 million (204 million × $0.10 = $20.4 million). Therefore, the total cost for providers is approximately $40.4 million ($20 million + $20.4 million = $40.4 million).

For health plans, the costs related to the NPP consist of developing and drafting the revised NPP, and, for certain health plans, the costs of printing and mailing the notice out-of-cycle because the revision is a material change. See § 164.520(c)(1)(v)(A). With the exception of a few large health plans, most health plans do not self-administer their plans. Most plans are either health insurance issuers (approximately 730) or utilize third party administrators that act on their behalf in the capacity of business associates. We identified approximately 750 third party administrators acting as business associates for ERISA plans. We have revised our earlier estimate of 3,500 third party administrators after learning that the majority of these entities act as welfare administrators and do not administer health plans. In addition, some public non-Federal health plans may use third party administrators. Almost all of the public and ERISA plans, we believe, employ third party administrators to administer their health plans. While the third party administrators will bear the direct costs of issuing the revised NPPs, the costs will generally be passed on to the plans that contract with them. Those plans that self-administer their own plans will also incur the costs of issuing the revised NPPs. We do not know how many plans administer as well as sponsor health plans and invited comments on the number of self-administered plans. As we did not receive comments on this issue, we assume that there are not enough self-administered plans to have an effect on these estimates.

Each of the approximately 1,500 health insurance issuers and health plan administrators will experience the same kinds of costs as we estimated for providers for drafting ($28 per entity) and printing ($0.10 per notice) the NPPs. However, health insurers and plan administrators will have to mail the NPPs to policy holders. We recognize that, under the existing requirement to send new NPPs in a separate mailing to all policy holders, the costs of distributing new NPPs, including clerical time and in some cases, postage, constituted the majority of the overall costs of the rule to covered entities. However, in the proposed rule, we requested comments on alternative ways to inform individuals of material changes to their rights and protections that would be less burdensome and costly. Based on the comments and consistent with E.O. 13563, in this final rule, we have adopted an alternative to the requirement to send the new NPP to all policy holders within 60 days. After consideration, we decided to permit health plans and third party administrators working for health plans to include the revised NPP in their next annual mailing, rather than within 60 days of the material change, if they have a Web site with an NPP. See § 164.520(c)(1)(v)(A). We anticipate that most, if not all, affected entities will take advantage of this option and will not send the NPP in a separate mailing. As such, we expect that the vast majority of health insurers will not incur any out-of-cycle NPP dissemination costs.

Nonetheless, to account for any costs that might be incurred by a small

[36] See *http://www.bls.gov/oes/current/naics3_541000.htm#23–0000* for lawyers. Note that we generally calculate labor costs based on the median hourly rate, which for lawyers is $56.21 per hour. We add 50 percent to account for fringe benefits, resulting in an estimated hourly cost of $84.32.

[37] We identified 698,238 entities that must prepare and deliver NPPs that are shown in Table 1 above. This includes 696,758 HIPAA covered entities that are health care providers, including hospitals, nursing facilities, doctor offices, outpatient care centers, medical diagnostic, imaging service, home health service and other ambulatory care service covered entities, medical equipment suppliers, and pharmacies. For the purposes of our calculation, we have rounded this number to 697,000. Table 1 also includes 730 health insurance carriers and 750 third party administrators working on behalf of covered health plans. The cost estimates for these entities are addressed later.

minority of health insurers to distribute the revised NPPs in a separate mailing, we have calculated the costs to these entities of doing so. We describe our methodology in the following paragraphs, beginning with an estimated total number of NPP recipients. We then calculate the costs of printing and sending the revised NPP by separate mailings to all recipients and estimate that no more than 10 percent of these costs will actually be incurred.

Because the Privacy Rule requires that only the named insured or policy holder is notified of changes to the health plans' privacy practices even if that policy also covers dependents, we expect that only policy holders will receive the revised NPPs mandated by this rule. This assumption is consistent with the practices of public programs, such as Medicare, which has a policy of mailing one notice or a set of program materials to a household of four or fewer beneficiaries at the same address. As a result, although there are 50.7 million individual Medicare beneficiaries, the program only sends out approximately 36 million pieces of mail per mailing.

Actuarial Research Corporation (ARC), our consultant, estimated the number of policy holders for all classes of insurance products to be approximately 183.6 million, including all public programs. The data comes from the Medical Expenditure Panel Survey from 2004–2006 projected to 2010. ARC estimated 112.6 million private sector policy holders and 71.0 million public ''policy holders.'' The total, including more recent Medicare data, is 188.3 million persons (which results in roughly a split of 60 percent private policy holders and 40 percent public ''policy holders''), whom we expect to receive NPPs from their plans. The estimates do not capture policy holders who are in hospitals or nursing homes at the time of the survey, or individuals who may have been insured under more than one plan in a year, for example, because their job status changed, they have supplemental policies, or they have more than one employer, creating duplicate coverage. Therefore, ARC recommended we use 200 million for the number of NPPs that will actually be sent.

We estimate the costs of drafting, printing, and distributing the NPP to all potential recipients to be the following. First, drafting the NPP is estimated to require one-third hour of legal services at a cost of $28 × 1,500 insurance plans and insurance administrative entities, which equals $42,000. Second, we need to calculate printing and distribution costs for all potential recipients assuming the revised notice would be sent in a separate mailing. As with providers, we estimate the cost of printing the NPP, which includes the cost of paper and actual printing, to be $0.10 per notice. Therefore, we estimate the cost of printing 200 million notices for mail distribution at $20 million. Further, we estimate the cost of distributing the NPPs, including clerical time and postage in the same manner as these costs were estimated for the Breach Notification for Unsecured Protected Health Information Regulations. Thus, we assume that an office worker could process and send 100 mailings per hour at a cost of $22.53 per hour, plus a postage cost of $0.45 per mailing. If notices were required to be mailed to the 200 million beneficiaries in the sixty-day timeframe, the distribution costs would be $135 million (200 million/100 per hour × $22.53 = $45 million + $90 million (200 million × $0.45)). Total printing and distribution cost would have been $155 million, if all policy holders received separate NPP mailings. Third, as discussed above, we expect that nearly all plans and third party administrators will be able to avoid having to do a separate mailing of the revised notice under the new distribution provisions in this final rule, and that only 10 percent of these plans will incur the printing and distribution costs. Using the above estimates, we assume for this purpose that 20 million notices (200 million total notices × 10%) will be need to be printed and sent through a separate mailing, at a total cost of $15.5 million ($2 million printing + $13.5 million mailing). Therefore, the total cost to all plans for drafting, printing, and distributing the NPP is approximately $15.5 million. We note that even this total may be an overestimation of the costs because many insurers may use bulk mailing rates to distribute their NPPs which would reduce their mailing costs.

The total estimated cost for both providers and health plans to notify individuals and policy holders of changes in their privacy rights is approximately $55.9 million in the first year following implementation of the rule.

A number of commenters expressed general concern regarding the costs of printing and distributing new NPPs but did not provide estimates of the costs they anticipated or question our calculations. Two health plan commenters estimated that the costs of printing and mailing NPPs to their members could reach up to $100,000. However, they did not provide information about the facts and assumptions underlying their analyses, including the number of beneficiaries or mailings they anticipated, so we were unable to evaluate their estimates. We have addressed some of this concern by permitting health plans that maintain a notice on their web sites to include their NPPs in their annual mailings, rather than separately mailing the NPPs within 60 days of the material changes.

Table 5 below presents our analysis of costs to the providers, insurers, and third party administrators that are required to issue NPPs under the rule.[38]

TABLE 5—SUMMARY OF COMPLIANCE COST FOR NOTICES OF PRIVACY PRACTICES

Cost elements	Providers	Health insurers & third party administrators	Total (approx.)
Drafting NPPs	$20 million	$42,000	$20 million.
Printing NPPs	$20.4 million	$2 million	$22.4 million.
Mailing NPPs	N/A	$13.5 million	$13.5 million.
Total (approx.)	$40.4 million	$15.5 million	$55.9 million.

[38] Health care clearinghouses function almost exclusively as business associates with respect to the protected health information they maintain and process, and therefore have no NPP requirements.

3. Business Associates and Covered Entities and Their Contractual Relationships

The rule extends liability for failure to comply with certain provisions of the Privacy and Security Rules directly to business associates and business associate subcontractors. Prior to this rule and HITECH, these obligations applied to business associates and their subcontractors indirectly through §§ 164.504(e) and 164.314(a), which require that covered entities by contract require business associates to limit uses and disclosures and implement Security Rule-like safeguards.

This final rule implements Section 13401 of HITECH Act, which makes business associates directly liable for compliance with many of the same standards and implementation specifications, and applies the same penalties to business associates that apply to covered entities, under the Security Rule. Additionally, in accord with Section 13404 of the HITECH Act, the rule requires business associates to comply with many of the same requirements, and applies the same penalties to business associates that apply to covered entities, under the Privacy Rule. Business associates must also obtain satisfactory assurances in the form of a business associate agreement from subcontractors that the subcontractors will safeguard any protected health information in their possession. Finally, business associates must furnish any information the Secretary requires to investigate whether the business associate is in compliance with the regulations.

In the proposed rule, we assumed that business associates' compliance with their contracts range from the minimal compliance to avoid contract termination to being fully compliant. Further, we assumed that business associates in compliance with their contracts would have already designated personnel to be responsible for formulating the organization's privacy and security policies, performed a risk analysis, and invested in hardware and software to prevent and monitor for internal and external breaches of protected health information.

We also stated in the proposed rule that while business associates were previously required to comply with the HIPAA Rules according to the terms of their contracts with covered entities, and we expected that most business associates did so already, the risk of criminal and/or civil monetary penalties may spur some business associates to increase their efforts to comply with the Rules. We explained that we have no information on the degree of contract enforcement and compliance among business associates, and lack information regarding the size or type of business associates that contract with covered entities. We have only rough estimates as to the overall number of business associates, which range from approximately one million to two million depending on the number of business associates that serve multiple covered entities.

While we did not have specific information in this regard, we assumed that some business associates and subcontractors already comply with existing privacy and security standards in accordance with their indirect and contractual obligations. For them, the proposed rule would impose only a limited burden. For other business associates, depending on the current level of compliance, the proposed rule could impose significant burdens. We requested comments regarding the amount of burden and the number of affected business associates.

Several commenters stated that requiring business associates to undertake compliance with the rule in the same way as covered entities is excessive and burdensome, especially because in some cases business associates do not have the same type of relationship with individuals. Several commenters pointed to the burden on covered entities and business associates to renegotiate business associate agreements and train staff, and many specifically mentioned that compliance with the Security Rule is particularly costly. One commenter stated that it was a business associate party to ''tens of thousands'' of business associate contracts, with a significant cost to bring all into compliance.

We continue to expect that most business associates and subcontractors have made and continue to make a good-faith effort to follow the terms of their contracts. The burden of the rule on business associates and subcontractors depends on the terms of the contracts between covered entities and business associates and between the business associates and subcontractors, and the degree to which business associates and subcontractors established privacy policies and adopted security measures that comport with the HIPAA Rules. For business associates and subcontractors that have already taken HIPAA-compliant measures to protect the privacy and security of the protected health information in their possession, as required by their existing contracts, the rule imposes limited burden. We estimate the costs to other business associates later in this section.

A few commenters cited concerns about unfair competition for smaller business associate entities that they believe will not be able to compete with larger business associate entities, especially with regard to contract negotiations including indemnification and other risk allocation issues.

We understand that many small business associates are concerned about the allocation of risk and indemnification in conjunction with their business associate contracts. However, as we discuss in section IV D above, as with any contracting relationship, business associates and covered entities may include other provisions that dictate and describe their business relationship. While these may or may not include indemnification clauses or other risk-shifting provisions, these contractual provisions and relationships are outside the governance of the HIPAA Rules.

Because we understand that covered entities and business associates remain concerned with the cost to bring their business associate agreements into compliance with the final rule, we allow contracts to be phased in over one year from the compliance date or 20 months from the publication date of the final rule, and we expect and encourage covered entities and business associates to incorporate the costs of modifying contracts into the normal renegotiation of contracts as the contracts expire. As we did not receive comments to the contrary, we believe that most contracts will be renegotiated over the phase-in period. In addition, the Department has issued on its web site revised sample business associate provisions, which should lessen the costs associated with contract modifications.

As we believe covered entities generally are operating under HIPAA compliant contracts with their business associates, the transition period and availability of sample contract provisions should make it possible for these entities to incorporate any minor contract modifications into normal contract renegotiations without any appreciable added costs. We continue to believe that all covered entities have established business associate agreements with their business associates that are consistent with the requirements of the HIPAA Rules, as covered entities have been subject to direct liability under the Rules since their inception and have had more than half a dozen years to make their contracts compliant. However, to the extent that some contracts between covered entities and business associates

are not currently in full compliance with the business associate agreement provisions, these entities may experience limited costs to revise their contracts.

Although we are less certain about the current state of business associate-subcontractor relationships, we believe that most business associates have made a good faith attempt to include the appropriate contractual requirements. Still, we anticipate that some small business associates, now that they are subject to direct liability under the rules, might establish or significantly modify their subcontracts to come into compliance for the first time. Such business associates would not be eligible for the extended transition period and, as a result, would incur the costs of creating new contracts or renegotiating contracts out of cycle. In the Final Privacy Rule published in 2002, we estimated that entities would need between one and two hours to develop and tailor a business associate agreement to their particular needs. See 67 FR 53182, 53257. Taking the average of the lower and upper estimates provided in the earlier rulemaking, we estimate that developing and tailoring contract language normally would take approximately 90 minutes of professional legal services at $84.32 per hour.[39] However, as in the 2002 Final Privacy Rule (67 FR 53257), we estimate that providing model language will reduce the time required to develop contract language by at least one third. Thus, we estimate that each new or significantly modified contract between a business associate and its subcontractors will require, at most, one hour of a lawyer's time at a cost of $84.32.

We believe that no more than 25 percent of 1–2 million business associates, or 250,000–500,000 entities, would not have already made good faith efforts to achieve compliance and will need to create or significantly modify subcontracts, resulting in total costs of between $21 million and $42 million.

We expect that each business associate's lawyer will draw up one standard contract to use for all of its subcontracts. We do not attribute contract revision costs to subcontractors because the required contract provisions are not negotiable and subcontractors will need to only sign the agreement. We note that our estimated cost likely is an overestimate because the group of small business associates that may be less likely than others to have compliant contracts in place with subcontractors are, because of their size, also less likely to have any subcontractors at all.

Finally, in response to the commenters concerned with the cost and burden on business associates to come into full compliance with the Security Rule, we have taken another look at the underlying assumptions in the proposal. We continue to believe that business associates have engaged in privacy practices in compliance with their contractual obligations to use and disclose protected health information as limited by the Privacy Rule and their particular contracts with covered entities. Therefore, as we have stated above, we do not believe that the extension of liability for compliance with Privacy Rule requirements as identified in this rulemaking will impose any new costs or burdens.

With regard to the Security Rule, which was of particular concern to commenters as to the compliance costs on business associates, we also continue to believe that business associates, in providing their adequate assurances to safeguard electronic protected health information through their business associate contracts, have implemented security protections that meet the standards and required implementation specifications in the Security Rule. Further, we continue to believe that business associates have made the necessary investment in hardware and software to secure the electronic protected health information as part of the investment in the hardware and software needed for their management and processing of this information to perform their business associate functions and comply with the contract requirements at § 164.314(a). However, based on the comments, we now believe that some business associates, particularly smaller business associates that may have access to electronic protected health information for limited purposes, may not have engaged in certain of the formal administrative safeguards. For example, these entities may not have performed a risk analysis, established a risk management program, or designated a security official, and may not have written policies and procedures, conducted employee training, or documented compliance as required under §§ 164.308 and 164.316 of the Security Rule.

We do not have information on what percentage of business associates may have to engage in efforts to comply with some of the administrative safeguard standards, including documenting their policies and procedures and training their employees on the policies and procedures, nor did the comments on the impact statement offer any specific information to provide an estimate. We assume that up to 80 percent of the 1–2 million business associates, or between 800,000 and 1.6 million business associates, may handle electronic protected health information and thus may have to document their existing security protocols. Further, of these business associates, we assume that no more than 25 percent are likely to incur some cost to document their administrative safeguards and their policies and procedures as now required by statute and these regulations. We believe that our original assumption of compliance with all Security Rule requirements remains sound for the rest of the business associates, and we received no substantive comments to the contrary.

The costs of coming into full compliance with the administrative safeguard procedures, such as performance of a risk analysis and development of a risk management plan, will vary depending on the size and complexity of the business associate, the scope of their duties for the covered entity and the protected health information they must secure, and the degree to which their prior documentation of their security protocols falls short of compliance with the standards in the Security Rule. In the original Security Rule, we estimated that covered entities would need approximately 16 hours to document their policies and procedures. See 68 FR 8334, 8368. As these policies and procedures are the reflection of the risk management plan, which in turn is based on the risk analysis, we believe that this estimate would be inclusive of that time. We believe it will take business associates on average much less time to document their security related policies and procedures, because they have likely already engaged in most of the analysis associated with the adoption of security protocols, even if they may not have formally reduced all such protocols to writing, and because the scope of their responsibilities will generally be much more constrained than that of the covered entity with whom they have contracted. In addition, while covered entities must perform these tasks with respect to their entire business, generally only a small part of any business associate is involved with electronic protected health information.

Extrapolating from our estimate in the original Security Rule that entities would require approximately 16 hours to implement and document Security

[39] See *http://www.bls.gov/oes/current/naics3_541000.htm#23–0000* for lawyers. Note that we generally calculate labor costs based on the median hourly rate, which for lawyers is $56.21 per hour. We add 50 percent to account for fringe benefits, resulting in an estimated hourly cost of $84.32.

Rule compliance measures for the first time, and applying the assumption that most of these measures already are in place, we estimate that these business associates will need only between 2 and 5 hours to formalize or update their applicable administrative safeguards. We would cost the time needed to come into compliance at $56.61/hour.[40] According to these assumptions, the range of costs that any one business associate would incur to comply with the new statutory and regulatory requirements would be between $113 and $283, as first year, one-time costs. Assuming that businesses associates with access to electronic protected health information represent 80 percent of 1 to 2 million total business associates (or 800,000 to 1.6 million total), the aggregated costs for all business associates are estimated to be between approximately $22.6 million and $113 million. (25 percent of 800,000 business associates = 200,000; 200,000 × $113 (2 hr @ $56.61/hr) = $22.6 million. 25 percent of 1.6 million business associates = 400,000; 400,000 × $283 (5 hr @ $56.61/hr) = $113 million.) These costs represent one time first year costs for full compliance by business associates with the Security Rule requirements.

Table 6 below presents the range of our estimates of the costs to business associates of achieving compliance with the rules.

TABLE 6—BUSINESS ASSOCIATE COST ESTIMATES IN 2011 DOLLARS

Data element	Security rule compliance documentation	BAA between business associates and subcontractors
Estimated number of affected entities	200,000–400,000 BAs	250,000–500,000 BAs.
Hours needed to complete compliance activities	2–5 hours per BA	1 hour per BA.
Cost per hour	$56.61	$84.32.
Total cost	$22.6 million–$113 million	$21 million–$42 million.

Response to Other Public Comments

Comment: One commenter suggested that business associates will be reluctant to contract with covered entities due to perceived increased risks associated with such contracts, and covered entities will be forced to hire more staff at additional costs.

Response: While the HIPAA Rules now impose direct liability with regard to compliance, business associates were previously contractually liable for compliance with these provisions. Further, whether a covered entity uses workforce members or business associates to perform its operations remains a decision for the covered entity. As this commenter did not provide specific information about his concerns, we cannot quantify the costs associated with this comment, nor do we have a basis for concluding that business associates will refuse to contract with covered entities as a result of this rule.

Comment: One commenter suggested that requiring business associate agreements will increase the costs of litigation.

Response: As business associate agreements were required under the HIPAA Rules previously, and as the commenter did not include specific information about what costs he believes will increase, we do not believe such a requirement will increase litigation generally.

4. Qualitative Analysis of Unquantified Costs

a. Authorization for Uses and Disclosures of Protected Health Information for Marketing and Sale of Protected Health Information

The final rule modifies the definition of ''marketing'' to encompass treatment and health care operations communications to individuals about health-related products or services if the covered entity receives financial remuneration in exchange for making the communication from or on behalf of the third party whose product or service is being described. A covered entity must obtain an individual's written authorization prior to sending marketing communications to the individual.

In the proposed rule, we requested comment on the extent to which covered entities currently receive financial remuneration from third parties in exchange for sending information to individuals about the third parties' health-related products or services. In general, commenters did not indicate that complying with the final rule would be administratively burdensome, but some commenters expressed a general concern over the potential loss of revenue given the new restrictions on receiving financial remuneration from a third party to send health-related communications to an individual. These comments appear to indicate that most covered entities would not attempt to obtain authorizations for the now prohibited communications but rather would forgo making them altogether. We acknowledge the potential for some lost revenue due to these modifications in cases where covered entities are currently receiving financial remuneration from third parties to send health-related communications to individuals. However, as we do not know to what extent covered entities today currently operate in this manner, and commenters did not include specific information in this regard, we do not have data that could inform quantifying such loss.

The final rule also requires an individual's authorization before a covered entity may disclose protected health information in exchange for remuneration (i.e., ''sell'' protected health information), even if the disclosure is for an otherwise permitted disclosure under the Privacy Rule. The final rule includes several exceptions to this authorization requirement. In the proposed rule, we stated that on its face, this new prohibition would appear to increase the burden to covered entities by requiring them to obtain authorizations in situations in which no authorization is currently required. However, we believed such a scenario to be unlikely. We believed most individuals would not authorize disclosures of their protected health information when they were informed the covered entity would be remunerated for the disclosure. Thus, we believed covered entities would simply discontinue making such disclosures as it would not be

[40] We have used the median wage rate described by the U.S. Bureau of Labor Statistics in its 2011 National Compensation Survey for the category of Management Analysts (including responsibilities for designing systems and procedures), which is approximately $37.74/hr. See *http://www.bls.gov/oes/current/oes_nat.htm* . To this wage rate we have added 50 percent for benefits, which results in a total cost of $56.61/hr.

worthwhile for covered entities to continue to attempt to obtain such authorizations. We requested comment on these assumptions.

As noted above, the requirement to obtain authorization to receive remuneration to make a disclosure of protected health information contains several exceptions. In the proposed rule, we expressed our belief that covered entities would not incur additional costs to continue making most of the excepted disclosures as such exceptions were not constrained or limited in any way and thus, would not change the status quo. However, we recognized that the exception for research disclosures may impose additional burden on researchers as it was, consistent with the statute, a conditional exception. Covered entities would be able to disclose protected health information under the research exception only to the extent any remuneration received in exchange for the information did not exceed the cost to produce and transmit the information. Thus, we recognized that researchers who purchase data from covered entities may now incur additional costs as a result of the final rule, in order to obtain newly required authorizations, if they are currently paying a covered entity more than the cost to produce and transmit the protected health information (e.g., an incentive payment to produce the data) and the covered entity is not willing to accept only the costs to prepare and transmit the data. It was also recognized that some research may be jeopardized to the extent that authorizations for the entity to receive these incentive payments could not be obtained from subjects. On the other hand, to the extent covered entities agreed to receive only the costs to prepare and transmit the data, these entities would experience a loss of revenue while researchers would experience a corresponding decrease in costs, and current disclosures for research purposes could continue without authorization. While we acknowledged the potential costs under this provision, we stated that we have no information on the amounts currently paid to covered entities by researchers for protected health information, and thus, had no way to estimate the impact of the provision. We solicited comment in this area.

Overall, commenters did not indicate that obtaining authorization prior to disclosing protected health information in exchange for remuneration would result in an increased burden or cost for the covered entity. However, one commenter did estimate that obtaining additional authorizations may cost approximately $22 to $28, per patient. Some commenters indicated it may be burdensome to determine if remuneration was in fact received by the entity.

The comments on this provision did not alter our belief that, in general, covered entities would discontinue making disclosures in exchange for remuneration that require the individual's authorization, given the unlikelihood most individuals would agree to authorize such disclosures. Further, there are a number of exceptions to the general prohibition that allow a covered entity to continue to operate ''status quo'' with respect to a number of types of disclosures, even if the covered entity receives remuneration. In response to the comments, we acknowledge that it may be difficult to determine whether remuneration has been received by a covered entity, particularly since the prohibition encompasses both direct and indirect (i.e., non-financial) remuneration. We expect to issue future guidance on this topic to assist entities in complying.

With respect to the amounts currently paid to covered entities by researchers, some commenters indicated as a general concern that limiting remuneration received by covered entities from researchers may provide a disincentive for covered entities to continue assisting researchers in their efforts. However, commenters did not quantify what they are paying covered entities above the costs to prepare and transmit the data, nor did they provide information that would give the Department an idea of the extent to which covered entities receive such payments. Therefore, while we acknowledge the potential for some lost revenue to covered entities due to these modifications or some additional costs to researchers to obtain authorizations, we do not have data that could inform quantifying such costs. At the same time, we note that we have made some clarifications in the above preamble discussion regarding these provisions that we believe would lessen any such impact. Specifically, the preamble explains that we do not consider a sale of protected health information to encompass payments a covered entity may receive in the form of grants, or contracts or other arrangements to perform programs or activities, such as a research study, where any provision of protected health information to the payer is a byproduct of the service being provided. Thus, the payment by a research sponsor to a covered entity to conduct a research study is not considered a sale of protected health information even if the study involves disclosing research results that include protected health information to the sponsor. In contrast, a sale of protected health information includes disclosures of protected health information where a covered entity is receiving remuneration from or on behalf of the recipient of the data for the information itself. Thus, a disclosure of protected health information by a covered entity to a third party researcher that is conducting the research in exchange for remuneration would fall within these provisions, unless the only remuneration received is a reasonable, cost-based fee to cover the cost to prepare and transmit the data for such purposes.

b. Individual Right To Opt Out of Fundraising Communications

The current Privacy Rule requires covered entities give individuals the opportunity to opt out of receiving future fundraising communications from the entity. The HITECH Act and final rule strengthens the opt out by requiring that it be clear and conspicuous and that an individual's choice to opt out should be treated as a revocation of authorization. While the rule specified that a clear and conspicuous opt out method must not cause an individual to incur an undue burden or more than a nominal cost, proposed rule did not specify the method to be employed but rather left it up to the discretion of the covered entity. We requested comment on the extent to which the requirement that the opportunity to elect not to receive further fundraising communications be clear and conspicuous would have an impact on covered entities and their current fundraising materials.

Overall, commenters did not indicate that requiring the opt out for further fundraising to be clear and conspicuous would greatly impact covered entities and their current fundraising efforts or provide specific anticipated costs in this regard. Rather, some commenters indicated that they already provide pre-paid, pre-printed postcards for this purpose with fundraising mailings and doing so is neither costly nor imposes a significant burden on the individual who wishes to opt out of further communications. Based on this feedback and the continued flexibility in the final rule to choose the opt out method (e.g., toll-free number, post-card), we do not believe that the requirement that fundraising opt-outs be clear and conspicuous will result in significant new costs to covered entities.

Further, while some commenters did indicate that a pre-solicitation opt out would be costly for covered entities in

response to our request for comment on this issue, as a result of this general opposition, the final rule does not change the current requirement that covered entities only need to include an opt-out with any solicitation sent to an individual rather than to the first fundraising communication.

c. Individuals' Access to Protected Health Information

In this final rule, we strengthen an individual's right to receive an electronic copy of his or her protected health information. Specifically, as was proposed, the final rule requires that if an individual requests an electronic copy of protected health information that is maintained electronically in one or more designated record sets, the covered entity must provide the individual with access to the electronic information in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual. Also, as in the proposed rule, the final rule provides that a covered entity may charge a fee for costs associated with labor and supplies for creating an electronic copy, including electronic portable media if agreed to by the individual, and clarifies that a covered entity may charge for postage if an individual requests that the covered entity transmit portable media containing an electronic copy through mail or courier. However, covered entities may not include fees associated with maintaining systems, retrieval costs, or infrastructure costs in the fee they charge to provide an electronic copy.

We continue to believe that this requirement will not result in significant new burdens on covered entities. Individuals already had a right to access protected health information maintained in electronic designated record sets under the prior Rule, and already had a right to receive an electronic copy of such information to the extent the electronic copy was readily producible by the covered entity. The Rule provides significant flexibility to covered entities in honoring individuals' request for electronic access. While a covered entity must provide some type of electronic copy to an individual who requests one, a covered entity is not required to provide the exact form of the copy or access requested by the individual if it is not readily producible in such form. Thus, covered entities may provide readily producible electronic copies of protected health information that are currently available on their various systems. A covered entity is not required to purchase new software or systems in order to accommodate an electronic copy request for a specific form that is not readily producible by the covered entity at the time of the request, provided that the covered entity is able to provide some form of electronic copy. Further, in cases where an individual chooses not to accept the electronic copy that is readily producible by the covered entity, a hard copy may be offered.

We did hear from several commenters that some legacy or other systems, while capable of producing a hard copy as previously required under the existing access requirement, may not be capable of producing any electronic copy at present. In these cases, covered entities may incur some cost burden in order to purchase software or hardware to produce some kind of electronic copy for electronic information held in designated record sets on such legacy systems. However, covered entities are not required to purchase additional software or hardware to meet individuals' specific requests, as long as at least one type of electronic copy is available. We anticipate some cost will be incurred by covered entities with such systems; however we did not receive comments on the extent of these costs, or the number of covered entities with legacy systems that will need to incur such costs.

d. Right To Restrict Certain Disclosures to a Health Plan

The final rule requires that a covered health care provider agree in most cases to an individual's request to restrict disclosure to a health plan of the individual's protected health information that pertains to a health care service for which the individual has paid the health care provider in full out of pocket. This is a change from the prior rule, which provided individuals with the right to request a restriction on certain disclosures; however, a covered entity was not required to agree to the restriction, whatever the circumstances. We do not believe that covered health care providers will incur substantial costs to implement this expanded right for a number of reasons. First, in order to comply with the rule prior to this change, a covered entity is already required to have processes and procedures in place for accepting and considering individuals' requests for restrictions, even if, as a general matter, the covered entity declines to agree to such requests. This final rule does not require new or different processes for receiving and reviewing requests for restrictions, just that the covered entity honor, in most cases, a self-pay patient's request for a restriction to a health plan. Second, for those covered health care providers that do not currently, but will now be required to, accommodate requests by self-pay patients to restrict disclosures to a health plan, the final rule provides significant flexibility in how providers are to honor an individual's request and the preamble makes various clarifications in response to comments as to how to operationalize this new requirement. For example, the final rule makes clear that a health care provider is not required to separate or segregate records in order to ensure an individual's restriction request is honored. Rather, the final rule leaves it to the discretion of the provider as to how to flag information that is the subject of a restriction. Further, the final rule provides flexibility as to how restriction requests for certain services, such as bundled services, are to be handled, as well as what reasonable efforts should be made to obtain payment from an individual whose original form of payment has been dishonored, prior to resorting to billing the health plan for the service. Finally, in response to comments regarding the potential burden and cost of doing so, the final rule does not require health care providers to inform downstream providers who may receive the individual's protected health information, such as a pharmacy or specialist, of a restriction, given the lack of automated technologies to support such a requirement.

Notwithstanding the above, we acknowledge that there will be some additional burden on certain health care providers to ensure an individual's request to restrict a disclosure to a health plan is honored where such a request would not have been honored in the past. However, we do not have data to inform quantifying an estimated cost in this area. For example, we do not have data on the number of providers that currently accommodate requests from self-pay patients to restrict disclosures versus those that do not, the number of requests that covered health care providers receive today that would now require a restriction, nor even the number of requests for restrictions generally that covered health care providers currently receive.

e. Impact of the Genetic Information Underwriting Prohibition on Health Plans

The final rule prohibits health plans that are HIPAA covered entities, except issuers of long term care policies, from using or disclosing an individual's protected health information that is

genetic information for underwriting purposes. As we explained in the proposed rule, the rule does not affect health plans that do not currently use or disclose protected health information for underwriting purposes. Further, even with respect to health plans that perform underwriting, plans and issuers in the group market previously commented to the Department that they do not, even prior to the passage of GINA, use genetic information for underwriting purposes because pre-GINA laws and regulations prohibit them from discriminating against individuals based on any health status related factors, including genetic information. With respect to issuers in the individual health insurance market, the Department acknowledged in the proposed rule that there may be more significant policy changes associated with the prohibition on using or disclosing protected health information that is genetic information for underwriting purposes. However, the Department explained in the proposed rule that it did not have sufficient information to determine the extent of such changes, that is, to what extent issuers in the individual health insurance market use genetic information for underwriting purposes. Regardless, as we explained in the proposed rule, in the case of either the individual or group market, the Department assumed, because a prohibited use or disclosure of genetic information for underwriting purposes would also be a discriminatory use of such information under the nondiscrimination provisions of GINA Title I and its implementing regulations, that there would be no costs associated with conforming a plan's practices to comply with the underwriting prohibition that are above and beyond the costs associated with complying with the regulations implementing sections 101–103 of GINA. With respect to the health plans not covered by GINA but subject to the proposed prohibition in the Privacy Rule, the Department also assumed that the costs to comply would be minimal because such plans either: (1) do not perform underwriting, as is the case generally with public benefit plans; or (2) perform underwriting but do not in most cases use genetic information (including family medical history) for such purposes.

In general, most comments in response to the proposed rule did not provide information that contradicted the above assumptions. However, concern was expressed regarding the adverse impact of such an underwriting prohibition on the long-term care market. Given the concern regarding the impact of the underwriting prohibition on the long-term care market, the final rule exempts such plans from the prohibition. Thus, there are no costs to be attributed to long term care plans with this rule. Further, given we did not receive other comments that would lead us to question the underlying assumptions in the proposed rule, we do not expect this provision of the final rule to result in substantial new costs on health plans, particularly those that have been required to comply with the regulations implementing GINA's nondiscrimination provisions for several years now.

f. Enforcement Provisions

The amendments contained within this final rule to the HIPAA Enforcement Rule conform the regulatory language of the Rule to the enhanced enforcement provisions of the HITECH Act. Consistent with its reasoning in prior HIPAA Enforcement rulemakings,[41] the Department expects the costs covered entities, and now business associates, may incur with respect to their compliance with the Enforcement Rule, itself, should be low in most cases. That is, covered entities and business associates that comply with the HIPAA rules voluntarily, as is expected, should not incur any additional, significant costs as a result of the Enforcement Rule. Further, we believe the increased penalties and other enhancements provided by the HITECH Act and which are reflected in this final rule provide even more incentive to covered entities and business associates to take steps necessary to comply and thus not be liable for violations.

D. Qualitative Analysis of Unquantified Benefits

While we are certain that the regulatory changes in this final rule represent significant benefits, we cannot monetize their value. Many commenters agreed with our assumptions regarding the benefits to individuals, but we did not receive any comments that included specific information about quantifying those benefits. The following sections describe in greater detail the qualitative benefits of the final rule. In addition to greater privacy protections for individuals, these benefits include the results of our efforts to reduce burdens. Consistent with E.O. 13563, we conducted a retrospective review of our regulations and identified areas, such as certain research authorization requirements and disclosures to schools regarding childhood immunizations, in which we could decrease costs and increase flexibilities under the HIPAA Rules. The resulting changes are discussed below.

1. Greater Privacy Protections for Individuals

The benefits for individuals include added information on their rights through an expanded NPP, and greater rights with regard to the uses and disclosures of their personal health information through expanded requirements to: (1) Obtain authorization before a covered entity or business associate may disclose their protected health information in exchange for remuneration, (2) restrict certain disclosures to a health plan at the request of the individual, (3) strengthen the ability of individuals to opt out of further fundraising communications, and (4) limit uses and disclosures of protected health information for marketing. Individuals also will benefit from increased protection against discrimination based on their genetic information, achieved through the prohibition against health plans using or disclosing protected health information that is genetic information for underwriting purposes. Individuals also will have increased access to their protected health information in an electronic format.

Finally, under the rule, individuals' health information will be afforded greater protection by business associates of covered entities who share liability and responsibility with the covered entity for safeguarding against impermissible uses and disclosures of protected health information.

2. Breach Notification

The analysis of benefits of the breach notification regulation is as stated in the interim final rule. In summary, we stated that notifying individuals affected by a breach would alert them to and enable them to mitigate potential harms, such as identity theft resulting from the exposure of certain identifiers, and reputational harm that may result from the exposure of sensitive medical information. Further, the breach notification requirements provide incentive to covered entities and business associates to better safeguard protected health information, such as by encrypting the information, where possible.

We also believe that the modifications to the definition of breach to remove the harm standard and revise the risk assessment will ensure that covered

[41] See the preambles to the proposed and final Enforcement Rules at 70 FR 20224, 20248–49 (April 18, 2005) and 71 FR 8390, 8424 (February 16, 2006).

entities and business associates apply the rule in a more objective and uniform manner. We believe that these modifications will make the rule easier for covered entities and business associates to implement and will result in consistency of notification across entities which will benefit consumers.

3. Compound Authorizations for Research Uses and Disclosures

We proposed to permit compound authorizations for the use or disclosure of protected health information for conditioned and unconditioned research activities provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. We believed that the proposed provision would reduce burden and costs on the research community by eliminating the need for multiple forms for research studies involving both a clinical trial and a related biospecimen banking activity or study and by harmonizing the Privacy Rule's authorization requirements with the informed consent requirements under the Common Rule. This change to the Rule had long been sought by the research community. While we expected burden reduction and cost savings due to these modifications, we had no data which to quantify an estimate of such savings. We requested comment on the anticipated savings that this change would bring to the research community.

As explained above, the final rule adopts the proposal to permit compound research authorizations. While almost all commenters on this topic were supportive and agreed that the change would result in reduced burdens and costs due to a reduction in forms and harmonization with the Common Rule, we did not receive significant comment that could inform our quantifying the anticipated cost-savings associated with this modification.

4. Authorizations for Future Research Uses or Disclosures

We requested comment on the Department's previous interpretation that an authorization for research uses and disclosures must include a description of each purpose of the requested use or disclosure that is study specific, and the possibility of modifying this interpretation to allow for the authorization of future research uses and disclosures. We believed that this change in interpretation would reduce burden on covered entities and researchers by reducing the need for researchers to obtain multiple authorizations from the same individual for research and further harmonizing the Privacy Rule authorization requirements with the informed consent requirements under the Common Rule.

The final rule adopts the new interpretation to allow covered entities to obtain authorizations for future research uses and disclosures to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research. While we did receive comments supporting our assertions that permitting authorizations for future research uses and disclosures would reduce burden to covered entities and researchers by obviating the need for researchers to seek out past research participants to obtain authorization for future studies which they may be able to authorize at the initial time of enrollment into a study, and additionally by reducing the waivers of authorization that researchers would need to obtain from Institutional Review Boards, we did not receive specific comment on cost savings that could inform our quantifying the savings in this final rule.

5. Period of Protection for Decedent Information

We proposed to modify the current rule to limit the period for which a covered entity must protect an individual's health information to 50 years after the individual's death. We believed this would reduce the burden on both covered entities and those seeking the protected health information of persons who have been deceased for many years by eliminating the need to search for and find a personal representative of the decedent, who in many cases may not be known or even exist after so many years, to authorize the disclosure. We believed this change would also benefit family members and historians who may seek access to the medical information of these decedents for personal and public interest reasons. However, we lacked any data to be able to estimate the benefits (or any unanticipated costs) of this provision and requested comment on these assertions.

The final rule adopts the modification to limit the period of protection for decedent health information to 50 years after the date of death. While most comments responding to this proposal were very supportive of the change, agreeing with the anticipated benefits the Department had articulated (i.e., easier access to old or ancient patient health information by family, historians, archivists), the comments did not provide specific information that could inform our quantifying a cost-savings or reduction in burden associated with this change in policy.

The Department did receive one comment asserting that covered entities may keep decedent information, particularly the information of famous individuals, for longer than 50 years past the date of death in order to monetize those records. The commenter cited an example of an x-ray of a deceased celebrity being sold at an auction for $45,000. However, we do not anticipate that this is or will be a typical scenario.

6. Disclosures About a Decedent

We proposed to permit covered entities to disclose a decedent's protected health information to family members and others who were involved in the care or payment for care prior to the decedent's death, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity. In the preamble to the proposed rule, we stated our belief that the proposed change would reduce burden by permitting covered entities to disclose protected health information about a decedent to family members and other persons who were involved in an individual's care while the individual was alive, without having to obtain written permission in the form of an authorization from the decedent's personal representative, who may not be known or even exist, and may be more difficult to locate as time passes. However, we had no data to permit us to estimate the reduction in burden and requested public comment on this issue.

The final rule adopts the modification as proposed. However, as with the proposed rule, we are unable to quantify any cost-savings with respect this change. While commenters confirmed that permitting such disclosures would help facilitate communications with family members and other persons who were involved in an individual's care or payment for care prior to death, we did not receive any information that could inform estimating a savings.

7. Public Health Disclosures

We proposed to create a new public health provision to permit disclosure of proof of a child's immunization by a covered entity to a school in States that have school entry or similar laws. This proposed change would have allowed a covered health care provider to release

proof of immunization to a school without having to obtain a written authorization, provided the provider obtained the agreement, which may be oral, to the disclosure from a parent, guardian or other person acting *in loco parentis* for the individual, or from the individual, if the individual was an adult or emancipated minor. We anticipated that the proposed change to the regulations would reduce the burden on parents, schools, and covered entities in obtaining and providing written authorizations, and would minimize the amount of school missed by students. However, because we lacked data on the burden reduction, we were unable to provide an estimate of the possible savings and requested comment on this point.

The final rule adopts the proposal to permit covered entities to disclose, with the oral or written agreement of a parent or guardian, a child's proof of immunization to schools in States that have school entry or similar laws. This obviates the need for a covered entity to receive formal, executed HIPAA authorizations for such disclosures. While the final rule requires that covered entities document the agreement, the final rule is flexible and does not prescribe the nature of the documentation and does not require signature by the parent, allowing covered entities the flexibility to determine what is appropriate for their purposes. For example, as the preamble indicates above, if a parent or guardian submits a written or email request to a covered entity to disclose their child's immunization records to the child's school, a copy of the request would suffice as documentation of the agreement. Likewise, if a parent or guardian calls the covered entity and requests over the phone that their child's immunization records be disclosed to the child's school, a notation in the child's medical record or elsewhere of the phone call would suffice as documentation of the agreement.

Given that the rule no longer requires a formal, executed HIPAA authorization for such disclosures and provides significant flexibility in the form of the documentation required of a parent's or guardian's agreement to the disclosure, this modification is expected to result in reduced burden and cost to covered health care providers in making these disclosures, as well as to the parents and schools involved in the process. We acknowledge that covered health care providers who wish to use these less formal processes in lieu of the authorization will need to explain their new procedure to office staff. However, given the provision's flexibility and narrow scope, we do not expect that the providers will need to do more than ensure office staff have a copy of the new procedure. Further, any one-time costs to develop and deploy the new procedure will be offset by the savings that are expected to accrue from the change over time as the disclosures are carried out. While we acknowledge the overall savings associated with this change, as with other provisions in this rule providing increased flexibility for compliance, we are unable to quantify them. For example, we do not have data on how many family doctors and other providers generally make these types of disclosures and how many requests such providers generally receive for proof of immunization, and we did not receive data from commenters that could inform our estimating savings in this area.

E. Additional Regulatory Analyses

1. Regulatory Flexibility Act

The Regulatory Flexibility Act requires agencies to analyze and consider options for reducing regulatory burden if the regulation will impose a significant burden on a substantial number of small entities. The Act requires the head of the agency to either certify that the rule would not impose such a burden or perform a regulatory flexibility analysis and consider alternatives to lessen the burden.

For the reasons stated below, it is not expected that the cost of compliance will be significant for small entities. Nor is it expected that the cost of compliance will fall disproportionately on small entities. Although many of the covered entities and business associates affected by the rule are small entities, they do not bear a disproportionate cost burden compared to the other entities subject to the rule. Further, with respect to small business associates, only the fraction of these entities that has not made a good faith effort to comply with existing requirements will experience additional costs under the rule. The Department did not receive any comments on its certification in the proposed rules. Therefore, the Secretary certifies that this rule will not have a significant economic impact on a substantial number of small entities.

The RFA generally defines a ''small entity'' as (1) a proprietary firm meeting the size standards of the Small Business Administration (SBA), (2) a nonprofit organization that is not dominant in its field, or (3) a small government jurisdiction with a population of less than 50,000. The SBA size standard for health care providers ranges between $7.0 million and $34.5 million in annual receipts. Because 90 percent or more of all health care providers meet the SBA size standard for a small business or are nonprofit organizations, we generally treat all health care providers as small entities for purposes of performing a regulatory flexibility analysis.

With respect to health insurers and third party administrators, the SBA size standard is $7.0 million in annual receipts. While some insurers are classified as nonprofit, it is possible they are dominant in their market. For example, a number of Blue Cross/Blue Shield insurers are organized as nonprofit entities; yet they dominate the health insurance market in the States where they are licensed and therefore would not be considered small businesses. Using the SBA's definition of a small insurer as a business with less than $7 million in revenues, premiums earned as a measure of revenue,[42] and data obtained from the National Association of Insurance Commissioners,[43] the Department estimates that approximately 276 out of 730 insurers had revenues of less than $7 million.[44]

From the approximately $225.4 million (upper estimate) in costs we are able to identify, the cost per covered entity may be as low as $80 (for the vast majority of covered entities) and as high as $843 (for those entities that experience a breach), and we estimate that the cost per affected business associate will be between $84.32 and $282. These costs are discussed in detail in the regulatory impact analysis and below. We do not view this as a significant burden because, for example, even the highest average compliance cost per covered entity we have identified ($843) represents just 0.0001% of annual revenues for a small entity with only $7 million in receipts (see the low end of SBA's size standard for health care providers). We include 750 third party administrators in the calculation of covered entities, to represent approximately 2.5 million ERISA plans,[45] most of which are small entities, on whose behalf they carry our

[42] U.S. Small Business Administration, ''Table of Small Business Standards Matched to North American Industry Classification System Codes,'' available at *http://www.sba.gov/content/small-business-size-standards.*

[43] HHS ASPE analysis of 2010 NAIC Supplemental Health Care Exhibit Data.

[44] These counts could be an overestimate. Only health insurance premiums from both the group and individual market were counted. If insurers also offered other types of insurance, their revenues could be higher.

[45] Source: 2010 Medical Expenditure Survey—Insurance Component.

compliance activities. We have no information on how many of these plans self-administer, and we did not receive any information from commenters in this area and so do not include a separate estimate for plans that self-administer.

We estimate that the breach notification requirements will result in $14.5 million in annual costs to covered entities. Dividing that amount by the approximately 19,000 entities that will actually experience a breach of protected health information each year, we estimate that the costs of complying with the breach notification requirements will amount to, on average, $763 per covered entity that must respond to a breach. Smaller covered entities likely will face much lower costs, as these entities generally have protected health information for far fewer individuals than do larger covered entities and breach notification costs are closely linked to the number of individuals affected by a given breach incident.

The other source of costs for covered entities arises from the requirement to provide revised NPPs to the individuals they serve. We estimate that the approximately 700,000 covered entities will experience total costs of approximately $55.9 million for compliance with the NPP requirements, or about $80 per covered entity.

We estimate the costs for 200,000–400,000 business associates to come into full compliance with the Security Rule to be approximately $22.6–$113 million. The average cost per affected business associate would be approximately $198.

Finally, we estimate that 250,000 to 500,000 business associates will incur costs totaling between $21 million and $42 million, respectively, to establish or significantly modify contracts with subcontractors to be in compliance with the rule's requirements for business associate agreements. The average cost per business associate would be approximately $84.

Based on the relatively small cost per covered entity and per business associate, the Secretary certifies that the Rule will not have a significant impact on a substantial number of small entities. Still, we considered and adopted several solutions for reducing the burden on small entities.

First, we combined several required rules into one rulemaking, which will allow affected entities to revise and distribute their notices of privacy practices at one time rather than multiple times, as each separate rule was published. Second, in the final rule we increase flexibility for health plans by allowing them to send the revised notices with their annual mailings rather than requiring plans to send them to individuals in a separate mailing.

Third, we allow covered entities and business associates with existing HIPAA compliant contracts twelve months from the date of the rule to renegotiate their contracts unless the contract is otherwise renewed or modified before such date. This amount of time plus the eight months from the publication date of the rule to the compliance date generally gives the parties 20 months to renegotiate their agreements. We believe that the added time will reduce the cost to revise agreements because the changes the rule requires will be incorporated into the routine updating of covered entities' and business associates' contracts.

Finally, the Department has also published on its web site sample language for revising the contracts between covered entities and business associates. While the language is generic and may not suit all entities and agreements, particularly larger entities and those with more complex business relationships, we believe that it will particularly help small entities with their contract revisions and save them time and money in redrafting their contracts to conform to the rule.

2. Unfunded Mandates Reform Act

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) requires that agencies assess anticipated costs and benefits before issuing any rule whose mandates would require spending in any one year $100 million in 1995 dollars, updated annually for inflation. In 2011, that threshold is approximately $136 million. UMRA does not address the total cost of a rule. Rather, it focuses on certain categories of cost, mainly those ''Federal mandate'' costs resulting from: (1) Imposing enforceable duties on State, local, or Tribal governments, or on the private sector; or (2) increasing the stringency of conditions in, or decreasing the funding of, State, local, or Tribal governments under entitlement programs.

We are able to identify between $114 and $225.4 million in costs on both the private sector and State and Federal entities for compliance with the final modifications to the HIPAA Privacy and Security Rules, and for compliance with the final Breach Notification Rule. As stated above, there may be other costs we are not able to monetize because we lack data, and the rule may produce savings that may offset some or all of the added costs. We must also separately identify costs to be incurred by the private sector and those incurred by State and Federal entities.

Some of the costs of the regulation will fall on covered entities, which are primarily health care providers and health plans.[46] For the purpose of these calculations, we included all provider costs as private sector costs. While we recognize that some providers are State or Federal entities, we do not have adequate information to estimate the number of public providers, but we believe the number to be significantly less than 10 percent of all providers shown in Table 1. Therefore, as we did for the RFA analysis and for ease of calculation, we assumed that all provider costs are private sector costs. We did not receive any comments on this assumption.

With respect to health plans, based on the data discussed in section C, we estimate that 60 percent of policy holders are served by private sector health plans and 40 percent of policy holders are served by public sector plans. Therefore, we attribute 60 percent of health plan costs to the private sector and 40 percent of plan costs to the public sector.

The remaining costs of complying with the regulation will be borne by business associates of covered entities. We do not have data with which to estimate the numbers of private versus public entity business associates. However, we believe that the vast majority of, if not all, business associates, are private entities. Therefore, we assumed all business associate costs are private sector costs.

Of the specific costs we can identify, we estimate that approximately 91 percent of all costs, or between $103.7 and $205 million, will fall on private sector health care providers, health plans, and business associates. The remaining costs, approximately $10.3–20.4 million, will fall on public sector health plans. The following paragraphs outline the distribution of costs arising from the four cost-bearing elements of the final rule: (1) Covered entities must revise and distribute notices of privacy practices, (2) Covered entities that experience a breach of protected health information must comply with the breach notification requirements, (3) certain business associates must revise contracts with subcontractors to meet business associate agreement requirements, and (4) Certain business associates must make efforts to achieve full compliance with the administrative requirements of the Security Rule.

[46] Another type of covered entity, health care clearinghouses, generally will not bear these costs, as clearinghouses are not required to provide a notice of private practices to individuals and are involved in a miniscule fraction of breach incidents, if any.

We estimate the costs for to comply with the NPP provisions will reach about $55.9 million, which will be shared by providers and health plans. Providers will bear approximately $40.4 million of these costs, all of which we attribute to the private sector. Health plans will bear approximately $15.5 million and, as explained above, we have allocated 60 percent of health plan costs for NPPs, or $9.3 million, as private sector costs. Public plans will bear the remaining $6.2 million.

We estimate that private entities will bear 93 percent of the costs of compliance with the breach notification requirements, or about $13.5 million. This is because the majority of breach reports are filed by health care providers, all of whose costs we attribute to the private sector. Consistent with our estimate that 60 percent of health plan members are enrolled in private sector plans, we also include as private costs 60 percent of the breach notification costs borne by health plans (based on the number of health plans that have filed breach reports).

Finally, we estimate that all of the costs for business associates to create or revise business associate agreements with subcontractors ($42 million outer estimate), and to come into full compliance with the Security Rule ($113 million outer estimate), will be private sector costs.

As the estimated costs to private entities alone may exceed the $136 million threshold, UMRA requires us to prepare an analysis of the costs and benefits of the rule. We have already done so, in accordance with Executive Orders 12866 and 13563, and present this analysis in sections C and D.

3. Federalism

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a rule that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has Federalism implications.

The Federalism implications of the Privacy and Security Rules were assessed as required by Executive Order 13132 and published as part of the preambles to the final rules on December 28, 2000 (65 FR 82462, 82797) and February 20, 2003 (68 FR 8334, 8373), respectively. Regarding preemption, the preamble to the final Privacy Rule explains that the HIPAA statute dictates the relationship between State law and Privacy Rule requirements. Therefore, the Privacy Rule's preemption provisions do not raise Federalism issues. The HITECH Act, at section 13421(a), provides that the HIPAA preemption provisions shall apply to the HITECH provisions and requirements. While we have made minor technical changes to the preemption provisions in Subpart B of Part 160 to conform to and incorporate the HITECH Act preemption provisions, these changes do not raise new Federalism issues. The changes include: (1) Amending the definitions of ''contrary'' and ''more stringent'' to reference business associates; and (2) further amending the definition of contrary to provide that State law would be contrary to the HIPAA Administrative Simplification provisions if it stands as an obstacle to the accomplishment and execution of the full purposes and objectives of not only HIPAA, but also the HITECH Act.

We do not believe that the rule will impose substantial direct compliance costs on State and local governments that are not required by statute. It is our understanding that State and local government covered entities do not engage in marketing, the sale of protected health information, or fundraising. Therefore, the modifications in these areas would not cause additional costs to State and local governments. We anticipate that the most significant direct costs on State and local governments will be the cost for State and local government-owned covered entities of drafting, printing, and distributing revised notices of privacy practices, which would include the cost of mailing these notices for State health plans, such as Medicaid. However, the costs involved can be attributed to the statutory requirements, which provide individuals with strengthened rights about which they need to be notified.

In considering the principles in and requirements of Executive Order 13132, the Department has determined that these modifications to the Privacy and Security Rules will not significantly affect the rights, roles, and responsibilities of the States.

F. Accounting Statement

Whenever a rule is considered a significant rule under Executive Order 12866, we are required to develop an accounting statement indicating the costs associated with promulgating the rule. Below, we present overall monetary annualized costs discounted at 3 percent and 7 percent as described in the Regulatory Impact Analysis.

ESTIMATED COSTS OF THE FINAL RULE

[In 2011 millions]

Costs (annualized)	Primary estimate ($M)	Minimum estimate ($M)	Maximum estimate ($M)
Discounted @7%	42.8	34.8	50.6
@3%	35.2	28.7	41.7

In the RIA, we acknowledged several potential sources of costs that we were unable to quantify. Because we have no way to determine the extent to which entities currently engage in certain activities for which they now need authorization, or who will need to take on a new burden because of the rule, we cannot predict the magnitude of these costs with any certainty. These potential sources of cost include:

1. Potential lost revenue to covered entities who forgo making certain subsidized health-related communications to individuals rather than obtain those individuals' authorization for such communications;

2. Costs to researchers to obtain authorization to make incentive payments (above the costs to prepare the data) to covered entities to produce data or, alternatively, a loss in revenue for covered entities who agree to accept only the costs to prepare and transmit the data;

3. Potential costs to certain covered entities who purchase software or hardware to allow them to produce an electronic copy of individuals' protected health information; and

4. The burden to some health care providers of ensuring that an individual's request to restrict a disclosure to a health plan is honored where it might not have been before the final rule.

While we are certain the changes in this final rule also represent distinct

benefits to individuals with regard to the privacy and security of their health information, and with regard to their rights to that information, we are unable to quantify the benefits. Other expected qualitative benefits, which are described in detail above, include savings due to provisions simplifying and streamlining requirements and increasing flexibility. Such savings arise from:

1. Eliminating the need for multiple forms for certain research studies by permitting compound authorizations;
2. Obviating the need to find past research participants and obtain new authorizations for new research by allowing individuals to authorize future research uses and disclosures at the time of initial enrollment;
3. Limiting the period of protection for decedent information to permit family members and historians to obtain information about a decedent without needing to find a personal representative of the deceased individual to authorize the disclosure;
4. Permitting disclosures to a decedent's family members or others involved in the care or payment for care prior to the decedent's death; and
5. Permitting covered entities to document a parent's informal agreement to disclose immunization information to a child's school rather than requiring a signed authorization form.

VIII. Collection of Information Requirements

This final rule contains the following information collections (i.e., reporting, recordkeeping, and third-party disclosures) under the Paperwork Reduction Act. Some of those provisions involve changes from the information collections set out in the proposed and interim final rules. These changes are noted below.

A. Reporting

• Notification to the Secretary of breaches of unsecured protected health information (§ 164.408). In the final rule, we revise our estimated number of respondents and responses to reflect our experience administering the interim final rule.

B. Recordkeeping

• Documentation of safeguards and policies and procedures under the Security Rule (§ 164.316). In the proposed rule, we assumed that all business associates were in compliance with the Security Rule's documentation standard because of their contractual obligations to covered entities under the HIPAA Rules. In the final rule, we recognize that a minority of business associates, who have not previously maintained documentation of their policies and procedures and administrative safeguards under the Security Rule, may experience a burden coming into compliance with the documentation standard for the first time because they are now subject to direct liability under the Security Rule.

• Business Associate Agreements (§ 164.504(e)). We assumed in the proposed rule that business associates and their subcontractors were complying with their existing contractual obligations but acknowledged that some contracts would have to be modified to reflect changes in the law. We requested comments on how many entities would be unable able to revise contracts, in the normal course of business, within the phase-in period. We did not receive comments that would allow us to make a specific estimate; nonetheless, in the final rule we assume that a significant minority of business associates will need to revise their business associate agreements with subcontractors (or establish such agreements for the first time if they were not previously in compliance).

C. Third-Party Disclosures

• Breach notification to affected individuals and the media (§§ 164.404 & 164.406). We revise our estimates of the numbers of breaches, covered entities, and individuals affected to reflect our experience in administering the breach notification requirements under the interim final rule.

• Revision and dissemination of notices of privacy practices for protected health information (§ 164.520). Our burden estimates for this provision in the proposed rule were based on the requirement for covered entities to send a separate mailing containing the new notice to each policy holder. As part of an effort to reduce overall burden, the final rule instead permits health plans to send the revised notice of privacy practices in their next annual mailing to policy holders, allowing them to avoid additional distribution burdens. We also revise the estimated number of affected covered entities based on updated information from the Department of Labor and the Small Business Administration.

In addition to the changes summarized above, the information collections described in this final rule have been submitted to the Office of Management and Budget for review and approval.

List of Subjects

45 CFR Part 160

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Investigations, Medicaid, Medical research, Medicare, Penalties, Privacy, Reporting and record keeping requirements, Security.

45 CFR Part 164

Administrative practice and procedure, Computer technology, Electronic information system, Electronic transactions, Employer benefit plan, Health, Health care, Health facilities, Health insurance, Health records, Hospitals, Medicaid, Medical research, Medicare, Privacy, Reporting and record keeping requirements, Security.

For the reasons set forth in the preamble, the Department amends 45 CFR Subtitle A, Subchapter C, parts 160 and 164, as set forth below:

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS

■ 1. The authority citation for part 160 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); 5 U.S.C. 552; secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279; and sec. 1104 of Pub. L. 111–148, 124 Stat. 146–154.

■ 2. Revise § 160.101 to read as follows:

§ 160.101 Statutory basis and purpose.

The requirements of this subchapter implement sections 1171–1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104–191, section 105 of Public Law 110–233, sections 13400–13424 of Public Law 111–5, and section 1104 of Public Law 111–148.

■ 3. Amend § 160.102 as follows:
■ a. Redesignate paragraph (b) as paragraph (c); and
■ b. Add new paragraph (b) to read as follows:

§ 160.102 Applicability.

* * * * *

(b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

* * * * *

■ 4. Amend § 160.103 as follows:
■ a. Revise the definitions of ''Business associate'', ''Compliance date'',

''Disclosure'', ''Electronic media'', the introductory text of the definition of ''Health information'', paragraphs (1)(vi) through (xi), and (xv) of the definition of ''Health plan'', paragraph (2) of the definition of ''Protected health information,'' and the definitions of ''Standard'', ''State'', and ''Workforce''; and

■ b. Add, in alphabetical order, new definitions of ''Administrative simplification provision'', ''ALJ'', ''Civil money penalty or penalty'', ''Family member'', ''Genetic information'', ''Genetic services'', ''Genetic test'', ''Manifestation or manifested'', ''Respondent'', ''Subcontractor'', and ''Violation or violate''.

The revisions and additions read as follows:

§ 160.103 Definitions.

* * * * *

Administrative simplification provision means any requirement or prohibition established by:

(1) 42 U.S.C. 1320d–1320d–4, 1320d–7, 1320d–8, and 1320d–9;

(2) Section 264 of Pub. L. 104–191;

(3) Sections 13400–13424 of Public Law 111–5; or

(4) This subchapter.

ALJ means Administrative Law Judge.

* * * * *

Business associate: (1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Civil money penalty or *penalty* means the amount determined under § 160.404 of this part and includes the plural of these terms.

* * * * *

Compliance date means the date by which a covered entity or business associate must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

* * * * *

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

* * * * *

Electronic media means:

(1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

* * * * *

Family member means, with respect to an individual:

(1) A dependent (as such term is defined in 45 CFR 144.103), of the individual; or

(2) Any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half-siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents).

(i) First-degree relatives include parents, spouses, siblings, and children.

(ii) Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces.

(iii) Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins.

(iv) Fourth-degree relatives include great-great grandparents, great-great grandchildren, and children of first cousins.

Genetic information means:

(1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

(i) The individual's genetic tests;

(ii) The genetic tests of family members of the individual;

(iii) The manifestation of a disease or disorder in family members of such individual; or

(iv) Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

(2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

(i) A fetus carried by the individual or family member who is a pregnant woman; and

(ii) Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.

(3) Genetic information excludes information about the sex or age of any individual.

Genetic services means:

(1) A genetic test;

(2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or

(3) Genetic education.

Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

* * * * *

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: * * *

* * * * *

Health plan means * * *

(1) * * *

(vi) The Voluntary Prescription Drug Benefit Program under Part D of title XVIII of the Act, 42 U.S.C. 1395w–101 through 1395w–152.

(vii) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).

(viii) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.

(ix) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.

(x) The health care program for uniformed services under title 10 of the United States Code.

(xi) The veterans health care program under 38 U.S.C. chapter 17.

* * * * *

(xv) The Medicare Advantage program under Part C of title XVIII of the Act, 42 U.S.C. 1395w–21 through 1395w–28.

* * * * *

Manifestation or *manifested* means, with respect to a disease, disorder, or pathological condition, that an individual has been or could reasonably be diagnosed with the disease, disorder, or pathological condition by a health care professional with appropriate training and expertise in the field of medicine involved. For purposes of this subchapter, a disease, disorder, or pathological condition is not manifested if the diagnosis is based principally on genetic information.

* * * * *

Protected health information * * *

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.

* * * * *

Respondent means a covered entity or business associate upon which the Secretary has imposed, or proposes to impose, a civil money penalty.

* * * * *

Standard means a rule, condition, or requirement:

(1) Describing the following information for products, systems, services, or practices:

(i) Classification of components;

(ii) Specification of materials, performance, or operations; or

(iii) Delineation of procedures; or

(2) With respect to the privacy of protected health information.

* * * * *

State refers to one of the following:

(1) For a health plan established or regulated by Federal law, State has the meaning set forth in the applicable section of the United States Code for such health plan.

(2) For all other purposes, *State* means any of the several States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Subcontractor means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

* * * * *

Violation or *violate* means, as the context may require, failure to comply with an administrative simplification provision.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

■ 5. Add § 160.105 to subpart A to read as follows:

§ 160.105 Compliance dates for implementation of new or modified standards and implementation specifications.

Except as otherwise provided, with respect to rules that adopt new standards and implementation specifications or modifications to standards and implementation specifications in this subchapter in accordance with § 160.104 that become effective after January 25, 2013, covered entities and business associates must comply with the applicable new standards and implementation specifications, or modifications to standards and implementation specifications, no later than 180 days from the effective date of any such standards or implementation specifications.

■ 6. Revise § 160.201 to read as follows:

§ 160.201 Statutory basis.

The provisions of this subpart implement section 1178 of the Act, section 262 of Public Law 104–191, section 264(c) of Public Law 104–191, and section 13421(a) of Public Law 111–5.

■ 7. In § 160.202, revise the definition of ''Contrary'' and paragraph (1)(i) of the definition of ''More stringent'' to read as follows:

§ 160.202 Definitions.

* * * * *

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

(1) A covered entity or business associate would find it impossible to comply with both the State and Federal requirements; or

(2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part C of title XI of the Act,

section 264 of Public Law 104–191, or sections 13400–13424 of Public Law 111–5, as applicable.

More stringent * * *

(1) * * *

(i) Required by the Secretary in connection with determining whether a covered entity or business associate is in compliance with this subchapter; or

* * * * *

■ 8. Revise § 160.300 to read as follows:

§ 160.300 Applicability.

This subpart applies to actions by the Secretary, covered entities, business associates, and others with respect to ascertaining the compliance by covered entities and business associates with, and the enforcement of, the applicable provisions of this part 160 and parts 162 and 164 of this subchapter.

§ 160.302 [Removed and Reserved]

■ 9. Remove and reserve § 160.302.

■ 10. Revise § 160.304 to read as follows:

§ 160.304 Principles for achieving compliance.

(a) *Cooperation.* The Secretary will, to the extent practicable and consistent with the provisions of this subpart, seek the cooperation of covered entities and business associates in obtaining compliance with the applicable administrative simplification provisions.

(b) *Assistance.* The Secretary may provide technical assistance to covered entities and business associates to help them comply voluntarily with the applicable administrative simplification provisions.

■ 11. In § 160.306, revise paragraphs (a) and (c) to read as follows:

§ 160.306 Complaints to the Secretary.

(a) *Right to file a complaint.* A person who believes a covered entity or business associate is not complying with the administrative simplification provisions may file a complaint with the Secretary.

* * * * *

(c) *Investigation.* (1) The Secretary will investigate any complaint filed under this section when a preliminary review of the facts indicates a possible violation due to willful neglect.

(2) The Secretary may investigate any other complaint filed under this section.

(3) An investigation under this section may include a review of the pertinent policies, procedures, or practices of the covered entity or business associate and of the circumstances regarding any alleged violation.

(4) At the time of the initial written communication with the covered entity or business associate about the complaint, the Secretary will describe the acts and/or omissions that are the basis of the complaint.

■ 12. Revise § 160.308 to read as follows:

§ 160.308 Compliance reviews.

(a) The Secretary will conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions when a preliminary review of the facts indicates a possible violation due to willful neglect.

(b) The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

■ 13. Revise § 160.310 to read as follows:

§ 160.310 Responsibilities of covered entities and business associates.

(a) *Provide records and compliance reports.* A covered entity or business associate must keep such records and submit such compliance reports, in such time and manner and containing such information, as the Secretary may determine to be necessary to enable the Secretary to ascertain whether the covered entity or business associate has complied or is complying with the applicable administrative simplification provisions.

(b) *Cooperate with complaint investigations and compliance reviews.* A covered entity or business associate must cooperate with the Secretary, if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of the covered entity or business associate to determine whether it is complying with the applicable administrative simplification provisions.

(c) *Permit access to information.* (1) A covered entity or business associate must permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a covered entity or business associate must permit access by the Secretary at any time and without notice.

(2) If any information required of a covered entity or business associate under this section is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, the covered entity or business associate must so certify and set forth what efforts it has made to obtain the information.

(3) Protected health information obtained by the Secretary in connection with an investigation or compliance review under this subpart will not be disclosed by the Secretary, except if necessary for ascertaining or enforcing compliance with the applicable administrative simplification provisions, if otherwise required by law, or if permitted under 5 U.S.C. 552a(b)(7).

■ 14. Revise § 160.312 to read as follows:

§ 160.312 Secretarial action regarding complaints and compliance reviews.

(a) *Resolution when noncompliance is indicated.* (1) If an investigation of a complaint pursuant to § 160.306 or a compliance review pursuant to § 160.308 indicates noncompliance, the Secretary may attempt to reach a resolution of the matter satisfactory to the Secretary by informal means. Informal means may include demonstrated compliance or a completed corrective action plan or other agreement.

(2) If the matter is resolved by informal means, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

(3) If the matter is not resolved by informal means, the Secretary will—

(i) So inform the covered entity or business associate and provide the covered entity or business associate an opportunity to submit written evidence of any mitigating factors or affirmative defenses for consideration under §§ 160.408 and 160.410 of this part. The covered entity or business associate must submit any such evidence to the Secretary within 30 days (computed in the same manner as prescribed under § 160.526 of this part) of receipt of such notification; and

(ii) If, following action pursuant to paragraph (a)(3)(i) of this section, the Secretary finds that a civil money penalty should be imposed, inform the covered entity or business associate of such finding in a notice of proposed determination in accordance with § 160.420 of this part.

(b) *Resolution when no violation is found.* If, after an investigation pursuant to § 160.306 or a compliance review pursuant to § 160.308, the Secretary determines that further action is not

warranted, the Secretary will so inform the covered entity or business associate and, if the matter arose from a complaint, the complainant, in writing.

■ 15. In § 160.316, revise the introductory text to read as follows:

§ 160.316 Refraining from intimidation or retaliation.

A covered entity or business associate may not threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for—

* * * * *

■ 16. In § 160.401, revise the definition of ''Reasonable cause'' to read as follows:

§ 160.401 Definitions.

* * * * *

Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect.

* * * * *

■ 17. Revise § 160.402 to read as follows:

§ 160.402 Basis for a civil money penalty.

(a) *General rule.* Subject to § 160.410, the Secretary will impose a civil money penalty upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision.

(b) *Violation by more than one covered entity or business associate.* (1) Except as provided in paragraph (b)(2) of this section, if the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate.

(2) A covered entity that is a member of an affiliated covered entity, in accordance with § 164.105(b) of this subchapter, is jointly and severally liable for a civil money penalty for a violation of part 164 of this subchapter based on an act or omission of the affiliated covered entity, unless it is established that another member of the affiliated covered entity was responsible for the violation.

(c) *Violation attributed to a covered entity or business associate.* (1) A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member or business associate, acting within the scope of the agency.

(2) A business associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency.

■ 18. In § 160.404, revise the introductory text of paragraphs (b)(2)(i), (b)(2)(iii), and (b)(2)(iv) to read as follows:

§ 160.404 Amount of a civil money penalty.

* * * * *

(b) * * *

(2) * * *

(i) For a violation in which it is established that the covered entity or business associate did not know and, by exercising reasonable diligence, would not have known that the covered entity or business associate violated such provision,

* * * * *

(iii) For a violation in which it is established that the violation was due to willful neglect and was corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

* * * * *

(iv) For a violation in which it is established that the violation was due to willful neglect and was not corrected during the 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred,

* * * * *

■ 19. Revise § 160.406 to read as follows:

§ 160.406 Violations of an identical requirement or prohibition.

The Secretary will determine the number of violations of an administrative simplification provision based on the nature of the covered entity's or business associate's obligation to act or not act under the provision that is violated, such as its obligation to act in a certain manner, or within a certain time, or to act or not act with respect to certain persons. In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision.

■ 20. Revise § 160.408 to read as follows:

§ 160.408 Factors considered in determining the amount of a civil money penalty.

In determining the amount of any civil money penalty, the Secretary will consider the following factors, which may be mitigating or aggravating as appropriate:

(a) The nature and extent of the violation, consideration of which may include but is not limited to:

(1) The number of individuals affected; and

(2) The time period during which the violation occurred;

(b) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

(1) Whether the violation caused physical harm;

(2) Whether the violation resulted in financial harm;

(3) Whether the violation resulted in harm to an individual's reputation; and

(4) Whether the violation hindered an individual's ability to obtain health care;

(c) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the current violation is the same or similar to previous indications of noncompliance;

(2) Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

(3) How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

(4) How the covered entity or business associate has responded to prior complaints;

(d) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

(1) Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

(2) Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

(3) The size of the covered entity or business associate; and

(e) Such other matters as justice may require.

■ 21. Revise § 160.410 to read as follows:

§ 160.410 Affirmative defenses.

(a) The Secretary may not:

(1) Prior to February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that the violation is punishable under 42 U.S.C. 1320d–6.

(2) On or after February 18, 2011, impose a civil money penalty on a covered entity or business associate for an act that violates an administrative simplification provision if the covered entity or business associate establishes that a penalty has been imposed under 42 U.S.C. 1320d–6 with respect to such act.

(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:

(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or

(2) The violation is—

(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated and is not due to willful neglect; and

(ii) Corrected during either:

(A) The 30-day period beginning on the first date the covered entity liable for the penalty knew, or by exercising reasonable diligence would have known, that the violation occurred; or

(B) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

(c) For violations occurring on or after February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity or business associate for a violation if the covered entity or business associate establishes to the satisfaction of the Secretary that the violation is—

(1) Not due to willful neglect; and

(2) Corrected during either:

(i) The 30-day period beginning on the first date the covered entity or business associate liable for the penalty knew, or, by exercising reasonable diligence, would have known that the violation occurred; or

(ii) Such additional period as the Secretary determines to be appropriate based on the nature and extent of the failure to comply.

■ 22. Revise § 160.412 to read as follows:

§ 160.412 Waiver.

For violations described in § 160.410(b)(2) or (c) that are not corrected within the period specified under such paragraphs, the Secretary may waive the civil money penalty, in whole or in part, to the extent that the payment of the penalty would be excessive relative to the violation.

■ 23. Revise § 160.418 to read as follows:

§ 160.418 Penalty not exclusive.

Except as otherwise provided by 42 U.S.C. 1320d–5(b)(1) and 42 U.S.C. 299b–22(f)(3), a penalty imposed under this part is in addition to any other penalty prescribed by law.

■ 24. Amend § 160.534 as follows:

■ a. Revise paragraph (b)(1)(iii);

■ b. Add paragraph (b)(1)(iv); and

■ c. Revise paragraph (b)(2).

The revisions read as follows:

§ 160.534 The hearing.

* * * * *

(b)(1) * * *

(iii) Claim that a proposed penalty should be reduced or waived pursuant to § 160.412 of this part; and

(iv) Compliance with subpart D of part 164, as provided under § 164.414(b).

(2) The Secretary has the burden of going forward and the burden of persuasion with respect to all other issues, including issues of liability other than with respect to subpart D of part 164, and the existence of any factors considered aggravating factors in determining the amount of the proposed penalty.

* * * * *

PART 164—SECURITY AND PRIVACY

■ 25. The authority citation for part 164 is revised to read as follows:

Authority: 42 U.S.C. 1302(a); 42 U.S.C. 1320d–1320d–9; sec. 264, Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2(note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

■ 26. Revise § 164.102 to read as follows:

§ 164.102 Statutory basis.

The provisions of this part are adopted pursuant to the Secretary's authority to prescribe standards, requirements, and implementation specifications under part C of title XI of the Act, section 264 of Public Law 104–191, and sections 13400–13424 of Public Law 111–5.

■ 27. In § 164.104, revise paragraph (b) to read as follows:

§ 164.104 Applicability.

* * * * *

(b) Where provided, the standards, requirements, and implementation specifications adopted under this part apply to a business associate.

■ 28. Amend § 164.105 as follows:

■ a. Revise the introductory text of paragraph (a)(1), the introductory text of paragraph (a)(2)(i), paragraph (a)(2)(ii), the introductory text of paragraph (a)(2)(iii), and paragraphs (a)(2)(iii)(A) and (B);

■ b. Redesignate paragraph (a)(2)(iii)(C) as paragraph (a)(2)(iii)(D) and add new paragraph (a)(2)(iii)(C);

■ c. Revise newly redesignated paragraph (a)(2)(iii)(D); and

■ d. Revise paragraph (b).

The revisions read as follows:

§ 164.105 Organizational requirements.

(a)(1) *Standard: Health care component.* If a covered entity is a hybrid entity, the requirements of this part, other than the requirements of this section, § 164.314, and § 164.504, apply only to the health care component(s) of the entity, as specified in this section.

(2) * * *

(i) *Application of other provisions.* In applying a provision of this part, other than the requirements of this section, § 164.314, and § 164.504, to a hybrid entity:

* * * * *

(ii) *Safeguard requirements.* The covered entity that is a hybrid entity must ensure that a health care component of the entity complies with the applicable requirements of this part. In particular, and without limiting this requirement, such covered entity must ensure that:

(A) Its health care component does not disclose protected health information to another component of the covered entity in circumstances in which subpart E of this part would prohibit such disclosure if the health care component and the other component were separate and distinct legal entities;

(B) Its health care component protects electronic protected health information with respect to another component of the covered entity to the same extent that it would be required under subpart C of this part to protect such information if the health care

component and the other component were separate and distinct legal entities;

(C) If a person performs duties for both the health care component in the capacity of a member of the workforce of such component and for another component of the entity in the same capacity with respect to that component, such workforce member must not use or disclose protected health information created or received in the course of or incident to the member's work for the health care component in a way prohibited by subpart E of this part.

(iii) *Responsibilities of the covered entity.* A covered entity that is a hybrid entity has the following responsibilities:

(A) For purposes of subpart C of part 160 of this subchapter, pertaining to compliance and enforcement, the covered entity has the responsibility of complying with this part.

(B) The covered entity is responsible for complying with § 164.316(a) and § 164.530(i), pertaining to the implementation of policies and procedures to ensure compliance with applicable requirements of this part, including the safeguard requirements in paragraph (a)(2)(ii) of this section.

(C) The covered entity is responsible for complying with § 164.314 and § 164.504 regarding business associate arrangements and other organizational requirements.

(D) The covered entity is responsible for designating the components that are part of one or more health care components of the covered entity and documenting the designation in accordance with paragraph (c) of this section, provided that, if the covered entity designates one or more health care components, it must include any component that would meet the definition of a covered entity or business associate if it were a separate legal entity. Health care component(s) also may include a component only to the extent that it performs covered functions.

(b)(1) *Standard: Affiliated covered entities.* Legally separate covered entities that are affiliated may designate themselves as a single covered entity for purposes of this part.

(2) *Implementation specifications.*

(i) *Requirements for designation of an affiliated covered entity.*

(A) Legally separate covered entities may designate themselves (including any health care component of such covered entity) as a single affiliated covered entity, for purposes of this part, if all of the covered entities designated are under common ownership or control.

(B) The designation of an affiliated covered entity must be documented and the documentation maintained as required by paragraph (c) of this section.

(ii) *Safeguard requirements.* An affiliated covered entity must ensure that it complies with the applicable requirements of this part, including, if the affiliated covered entity combines the functions of a health plan, health care provider, or health care clearinghouse, § 164.308(a)(4)(ii)(A) and § 164.504(g), as applicable.

* * * * *

■ 29. Revise § 164.106 to read as follows:

§ 164.106 Relationship to other parts.

In complying with the requirements of this part, covered entities and, where provided, business associates, are required to comply with the applicable provisions of parts 160 and 162 of this subchapter.

■ 30. The authority citation for subpart C of part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d–2 and 1320d–4; sec. 13401, Pub. L. 111–5, 123 Stat. 260.

■ 31. Revise § 164.302 to read as follows:

§ 164.302 Applicability.

A covered entity or business associate must comply with the applicable standards, implementation specifications, and requirements of this subpart with respect to electronic protected health information of a covered entity.

■ 32. In § 164.304, revise the definitions of ''Administrative safeguards'' and ''Physical safeguards'' to read as follows:

§ 164.304 Definitions.

* * * * *

Administrative safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

* * * * *

Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

* * * * *

■ 33. Amend § 164.306 as follows:

■ a. Revise the introductory text of paragraph (a) and paragraph (a)(1);

■ b. Revise paragraph (b)(1), the introductory text of paragraph (b)(2), and paragraphs (b)(2)(i) and (b)(2)(ii);

■ c. Revise paragraph (c);

■ d. Revise paragraph (d)(2), the introductory text of paragraph (d)(3), paragraph (d)(3)(i), and the introductory text of paragraph (d)(3)(ii); and

■ e. Revise paragraph (e).

The revisions read as follows:

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

* * * * *

(b) * * *

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

* * * * *

(c) *Standards.* A covered entity or business associate must comply with the applicable standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

(d) * * *

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity or business associate must implement the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a

reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

(ii) As applicable to the covered entity or business associate—

* * * * *

(e) *Maintenance.* A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures in accordance with § 164.316(b)(2)(iii).

■ 34. Amend § 164.308 as follows:

■ a. Revise the introductory text of paragraph (a), paragraph (a)(1)(ii)(A), paragraph (a)(1)(ii)(C), paragraph (a)(2), paragraph (a)(3)(ii)(C), paragraph (a)(4)(ii)(C), paragraph (a)(6)(ii), and paragraph (a)(8); and

■ b. Revise paragraph (b).

The revisions read as follows:

§ 164.308 Administrative safeguards.

(a) A covered entity or business associate must, in accordance with § 164.306:

(1) * * *

(ii) * * *

(A) *Risk analysis (Required).* Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

* * * * *

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.

* * * * *

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.

(3) * * *

(ii) * * *

(C) *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

(4) * * *

(ii) * * *

(C) *Access establishment and modification (Addressable).* Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

* * * * *

(6) * * *

(ii) *Implementation specification: Response and reporting (Required).* Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.

* * * * *

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

(b)(1) *Business associate contracts and other arrangements.* A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with § 164.314(a), that the subcontractor will appropriately safeguard the information.

(3) *Implementation specifications: Written contract or other arrangement (Required).* Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

■ 35. Revise the introductory text of § 164.310 to read as follows:

§ 164.310 Physical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

* * * * *

■ 36. Revise the introductory text of § 164.312 to read as follows:

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

* * * * *

■ 37. Amend § 164.314 by revising paragraphs (a) and (b)(2)(iii) to read as follows:

§ 164.314 Organizational requirements.

(a)(1) *Standard: Business associate contracts or other arrangements.* The contract or other arrangement required by § 164.308(b)(4) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.

(2) *Implementation specifications (Required).*

(i) *Business associate contracts.* The contract must provide that the business associate will—

(A) Comply with the applicable requirements of this subpart;

(B) In accordance with § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section; and

(C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.

(ii) *Other arrangements.* The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of § 164.504(e)(3).

(iii) *Business associate contracts with subcontractors.* The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by § 164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(b) * * *

(2) * * *

(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and

* * * * *

■ 38. Revise the introductory text of § 164.316 and the third sentence of paragraph (a) to read as follows:

§ 164.316 Policies and procedures and documentation requirements.

A covered entity or business associate must, in accordance with § 164.306:

(a) * * * A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

* * * * *

■ 39. Revise § 164.402 to read as follows:

§ 164.402 Definitions.

As used in this subpart, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

(1) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(2) Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.

■ 40. In § 164.406, revise paragraph (a) to read as follows:

§ 164.406 Notification to the media.

(a) *Standard.* For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach as provided in § 164.404(a)(2), notify prominent media outlets serving the State or jurisdiction.

* * * * *

■ 41. In § 164.408, revise paragraph (c) to read as follows:

§ 164.408 Notification to the Secretary.

* * * * *

(c) *Implementation specifications: Breaches involving less than 500 individuals.* For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches discovered during the preceding calendar year, in the manner specified on the HHS web site.

■ 42. In § 164.410, revise paragraph (a) to read as follows:

§ 164.410 Notification by a business associate.

(a) *Standard*—(1) *General rule.* A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

(2) *Breaches treated as discovered.* For purposes of paragraph (a)(1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the Federal common law of agency).

* * * * *

■ 43. The authority citation for subpart E of part 164 is revised to read as follows:

Authority: 42 U.S.C. 1320d–2, 1320d–4, and 1320d–9; sec. 264 of Pub. L. 104–191, 110 Stat. 2033–2034 (42 U.S.C. 1320d–2 (note)); and secs. 13400–13424, Pub. L. 111–5, 123 Stat. 258–279.

■ 44. In § 164.500, redesignate paragraph (c) as paragraph (d) and add new paragraph (c) to read as follows:

§ 164.500 Applicability.

* * * * *

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

* * * * *

■ 45. Amend § 164.501 as follows:

■ a. Revise paragraphs (1) and (3) of the definition of ''Health care operations'';

■ b. Revise the definition of ''Marketing''; and

■ c. Revise paragraph (1)(i) of the definition of ''Payment''.

The revisions read as follows:

§ 164.501 Definitions.

* * * * *

Health care operations means * * *

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

* * * * *

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting,

enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

* * * * *

Marketing: (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(2) Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) *Financial remuneration* means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Payment means:

(1) * * *

(i) Except as prohibited under § 164.502(a)(5)(i), a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

* * * * *

■ 46. In § 164.502, revise paragraphs (a), (b)(1), (e), and (f) to read as follows:

§ 164.502 Uses and disclosures of protected health information: General rules.

(a) *Standard.* A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(1) *Covered entities: Permitted uses and disclosures.* A covered entity is permitted to use or disclose protected health information as follows:

(i) To the individual;

(ii) For treatment, payment, or health care operations, as permitted by and in compliance with § 164.506;

(iii) Incident to a use or disclosure otherwise permitted or required by this subpart, provided that the covered entity has complied with the applicable requirements of §§ 164.502(b), 164.514(d), and 164.530(c) with respect to such otherwise permitted or required use or disclosure;

(iv) Except for uses and disclosures prohibited under § 164.502(a)(5)(i), pursuant to and in compliance with a valid authorization under § 164.508;

(v) Pursuant to an agreement under, or as otherwise permitted by, § 164.510; and

(vi) As permitted by and in compliance with this section, § 164.512, § 164.514(e), (f), or (g).

(2) *Covered entities: Required disclosures.* A covered entity is required to disclose protected health information:

(i) To an individual, when requested under, and required by § 164.524 or § 164.528; and

(ii) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the covered entity's compliance with this subchapter.

(3) *Business associates: Permitted uses and disclosures.* A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) *Prohibited uses and disclosures.*

(i) *Use and disclosure of genetic information for underwriting purposes:* Notwithstanding any other provision of this subpart, a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan,* shall not use or disclose protected health information that is genetic information for underwriting purposes. For purposes of paragraph (a)(5)(i) of this section, underwriting purposes means, with respect to a health plan:

(A) Except as provided in paragraph (a)(5)(i)(B) of this section:

(*1*) Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(*2*) The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);

(*3*) The application of any pre-existing condition exclusion under the plan, coverage, or policy; and

(*4*) Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

(B) Underwriting purposes does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

(ii) *Sale of protected health information:*

(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

(*1*) Except as provided in paragraph (a)(5)(ii)(B)(*2*) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

(*2*) Sale of protected health information does not include a disclosure of protected health information:

(*i*) For public health purposes pursuant to § 164.512(b) or § 164.514(e);

(*ii*) For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(*iii*) For treatment and payment purposes pursuant to § 164.506(a);

(*iv*) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a);

(*v*) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(*vi*) To an individual, when requested under § 164.524 or § 164.528;

(*vii*) Required by law as permitted under § 164.512(a); and

(*viii*) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

(b) * * *

(1) *Minimum necessary applies.* When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

* * * * *

(e)(1) *Standard: Disclosures to business associates.* (i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) *Implementation specification: Documentation.* The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of § 164.504(e).

(f) *Standard: Deceased individuals.* A covered entity must comply with the requirements of this subpart with respect to the protected health information of a deceased individual for a period of 50 years following the death of the individual.

* * * * *

■ 47. In § 164.504, revise paragraphs (e), (f)(1)(ii) introductory text, and (f)(2)(ii)(B) to read as follows:

§ 164.504 Uses and disclosures: Organizational requirements.

* * * * *

(e)(1) *Standard: Business associate contracts.* (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) *Implementation specifications: Business associate contracts.* A contract between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any

subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with § 164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with § 164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with § 164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the requirements of this subpart that apply to the covered entity in the performance of such obligation.

(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

(3) *Implementation specifications: Other arrangements.* (i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in § 160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.

(4) *Implementation specifications: Other requirements for contracts and other arrangements.* (i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the protected health information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the protected health information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(*1*) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and

(*2*) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) *Implementation specifications: Business associate contracts with subcontractors.* The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.

(f)(1)* * *

(ii) Except as prohibited by § 164.502(a)(5)(i), the group health plan, or a health insurance issuer or HMO with respect to the group health plan, may disclose summary health information to the plan sponsor, if the plan sponsor requests the summary health information for purposes of:

* * * * *

(2) * * *

(ii) * * *

(B) Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;

* * * * *

■ 48. In § 164.506, revise paragraphs (a) and (c)(5) to read as follows:

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations.

(a) *Standard: Permitted uses and disclosures.* Except with respect to uses or disclosures that require an authorization under § 164.508(a)(2) through (4) or that are prohibited under § 164.502(a)(5)(i), a covered entity may use or disclose protected health information for treatment, payment, or health care operations as set forth in paragraph (c) of this section, provided that such use or disclosure is consistent with other applicable requirements of this subpart.

* * * * *

(c) * * *

(5) A covered entity that participates in an organized health care arrangement

may disclose protected health information about an individual to other participants in the organized health care arrangement for any health care operations activities of the organized health care arrangement.

■ 49. Amend § 164.508 as follows:
■ a. Revise the headings of paragraphs (a), (a)(1), and (a)(2);
■ b. Revise paragraph (a)(3)(ii);
■ c. Add new paragraph (a)(4); and
■ d. Revise paragraphs (b)(1)(i), and (b)(3).

The revisions and additions read as follows:

§ 164.508 Uses and disclosures for which an authorization is required.

(a) *Standard: Authorizations for uses and disclosures*—(1) *Authorization required: General rule.* * * *

(2) *Authorization required: Psychotherapy notes.* * * *

(3) * * *

(ii) If the marketing involves financial remuneration, as defined in paragraph (3) of the definition of marketing at § 164.501, to the covered entity from a third party, the authorization must state that such remuneration is involved.

(4) *Authorization required: Sale of protected health information.*

(i) Notwithstanding any provision of this subpart, other than the transition provisions in § 164.532, a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information, as defined in § 164.501 of this subpart. (ii) Such authorization must state that the disclosure will result in remuneration to the covered entity.

(b) * * *

(1) * * *

(i) A valid authorization is a document that meets the requirements in paragraphs (a)(3)(ii), (a)(4)(ii), (c)(1), and (c)(2) of this section, as applicable.

* * * * *

(3) *Compound authorizations.* An authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization, except as follows:

(i) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. Where a covered health care provider has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted under paragraph (b)(4)(i) of this section, any compound authorization created under this paragraph must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization.

(ii) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

(iii) An authorization under this section, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other such authorization under this section, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under paragraph (b)(4) of this section on the provision of one of the authorizations. The prohibition in this paragraph on combining authorizations where one authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits under paragraph (b)(4) of this section does not apply to a compound authorization created in accordance with paragraph (b)(3)(i) of this section.

* * * * *

■ 50. Amend § 164.510 as follows:
■ a. Revise paragraph (a)(1)(ii) introductory text;
■ b. Revise paragraph (b)(1)(i), the second sentence of paragraph (b)(1)(ii), paragraph (b)(2)(iii), the first sentence of paragraph (b)(3), and paragraph (b)(4); and
■ c. Add new paragraph (b)(5).

The revisions and additions read as follows:

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object.

* * * * *

(a) * * *

(1) * * *

(ii) Use or disclose for directory purposes such information:

* * * * *

(b) * * *

(1) * * *

(i) A covered entity may, in accordance with paragraphs (b)(2), (b)(3), or (b)(5) of this section, disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the protected health information directly relevant to such person's involvement with the individual's health care or payment related to the individual's health care.

(ii) * * * Any such use or disclosure of protected health information for such notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.

* * * * *

(2) * * *

(iii) Reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

(3) * * * If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the protected health information that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes. * * *

(4) *Uses and disclosures for disaster relief purposes.* A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

(5) *Uses and disclosures when the individual is deceased.* If the individual is deceased, a covered entity may disclose to a family member, or other persons identified in paragraph (b)(1) of this section who were involved in the individual's care or payment for health care prior to the individual's death, protected health information of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

■ 51. Amend § 164.512 as follows:
■ a. Revise the paragraph heading for paragraph (b), the introductory text of

paragraph (b)(1) and the introductory text of paragraph (b)(1)(v)(A);
■ b. Add new paragraph (b)(1)(vi);
■ c. Revise the introductory text of paragraph (e)(1)(iii) and paragraph (e)(1)(vi);
■ d. Revise paragraph (i)(2)(iii); and
■ e. Revise paragraphs (k)(1)(ii), (k)(3), and (k)(5)(i)(E).

The revisions and additions read as follows:

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required.

* * * * *

(b) *Standard: Uses and disclosures for public health activities.* (1) *Permitted uses and disclosures.* A covered entity may use or disclose protected health information for the public health activities and purposes described in this paragraph to:

* * * * *

(v) * * *

(A) The covered entity is a covered health care provider who provides health care to the individual at the request of the employer:

* * * * *

(vi) A school, about an individual who is a student or prospective student of the school, if:

(A) The protected health information that is disclosed is limited to proof of immunization;

(B) The school is required by State or other law to have such proof of immunization prior to admitting the individual; and

(C) The covered entity obtains and documents the agreement to the disclosure from either:

(1) A parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

(2) The individual, if the individual is an adult or emancipated minor.

* * * * *

(e) * * *

(1) * * *

(iii) For the purposes of paragraph (e)(1)(ii)(A) of this section, a covered entity receives satisfactory assurances from a party seeking protected health information if the covered entity receives from such party a written statement and accompanying documentation demonstrating that:

* * * * *

(vi) Notwithstanding paragraph (e)(1)(ii) of this section, a covered entity may disclose protected health information in response to lawful process described in paragraph (e)(1)(ii) of this section without receiving satisfactory assurance under paragraph (e)(1)(ii)(A) or (B) of this section, if the covered entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of paragraph (e)(1)(iii) of this section or to seek a qualified protective order sufficient to meet the requirements of paragraph (e)(1)(v) of this section.

* * * * *

(i) * * *

(2) * * *

(iii) *Protected health information needed.* A brief description of the protected health information for which use or access has been determined to be necessary by the institutional review board or privacy board, pursuant to paragraph (i)(2)(ii)(C) of this section;

* * * * *

(k) * * *

(1) * * *

(ii) *Separation or discharge from military service.* A covered entity that is a component of the Departments of Defense or Homeland Security may disclose to the Department of Veterans Affairs (DVA) the protected health information of an individual who is a member of the Armed Forces upon the separation or discharge of the individual from military service for the purpose of a determination by DVA of the individual's eligibility for or entitlement to benefits under laws administered by the Secretary of Veterans Affairs.

* * * * *

(3) *Protective services for the President and others.* A covered entity may disclose protected health information to authorized Federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056 or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.

* * * * *

(5) * * *

(i) * * *

(E) Law enforcement on the premises of the correctional institution; or

* * * * *

■ 52. In § 164.514, revise paragraphs (e)(4)(ii)(C)(*4*), (f), and (g) to read as follows:

§ 164.514 Other requirements relating to uses and disclosures of protected health information.

* * * * *

(e) * * *

(4) * * *

(ii) * * *

(C) * * *

(*4*) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

* * * * *

(f) *Fundraising communications.*

(1) *Standard: Uses and disclosures for fundraising.* Subject to the conditions of paragraph (f)(2) of this section, a covered entity may use, or disclose to a business associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization meeting the requirements of § 164.508:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to an individual;

(iii) Department of service information;

(iv) Treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(2) *Implementation specifications: Fundraising requirements.* (i) A covered entity may not use or disclose protected health information for fundraising purposes as otherwise permitted by paragraph (f)(1) of this section unless a statement required by § 164.520(b)(1)(iii)(A) is included in the covered entity's notice of privacy practices.

(ii) With each fundraising communication made to an individual under this paragraph, a covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

(iii) A covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

(iv) A covered entity may not make fundraising communications to an individual under this paragraph where the individual has elected not to receive such communications under paragraph (f)(1)(ii)(B) of this section.

(v) A covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

(g) *Standard: uses and disclosures for underwriting and related purposes.* If a health plan receives protected health information for the purpose of underwriting, premium rating, or other activities relating to the creation,

renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may only use or disclose such protected health information for such purpose or as may be required by law, subject to the prohibition at § 164.502(a)(5)(i) with respect to genetic information included in the protected health information.

* * * * *

■ 53. Amend § 164.520:
■ a. Revise paragraphs (b)(1)(ii)(E), (b)(1)(iii), (b)(1)(iv)(A), (b)(1)(v)(A), (c)(1)(i) introductory text, and (c)(1)(i)(B);
■ b. Remove paragraph (c)(1)(i)(C); and
■ c. Add paragraph (c)(1)(v).

The revisions and addition read as follows:

§ 164.520 Notice of privacy practices for protected health information.

* * * * *

(b) * * *

(1) * * *

(ii) * * *

(E) A description of the types of uses and disclosures that require an authorization under § 164.508(a)(2)–(a)(4), a statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization, and a statement that the individual may revoke an authorization as provided by § 164.508(b)(5).

(iii) *Separate statements for certain uses or disclosures.* If the covered entity intends to engage in any of the following activities, the description required by paragraph (b)(1)(ii)(A) of this section must include a separate statement informing the individual of such activities, as applicable:

(A) In accordance with § 164.514(f)(1), the covered entity may contact the individual to raise funds for the covered entity and the individual has a right to opt out of receiving such communications; (B) In accordance with § 164.504(f), the group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan; or

(C) If a covered entity that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of *health plan,* intends to use or disclose protected health information for underwriting purposes, a statement that the covered entity is prohibited from using or disclosing protected health information that is genetic information of an individual for such purposes.

(iv) * * *

(A) The right to request restrictions on certain uses and disclosures of protected health information as provided by § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction, except in case of a disclosure restricted under § 164.522(a)(1)(vi);

* * * * *

(v) * * *

(A) A statement that the covered entity is required by law to maintain the privacy of protected health information, to provide individuals with notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;

* * * * *

(c) * * *

(1) * * *

(i) A health plan must provide the notice:

* * * * *

(B) Thereafter, at the time of enrollment, to individuals who are new enrollees.

* * * * *

(v) If there is a material change to the notice:

(A) A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.

(B) A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.

* * * * *

■ 54. Amend § 164.522 as follows:
■ a. Revise paragraph (a)(1)(ii);
■ b. Add new paragraph (a)(1)(vi); and
■ c. Revise the introductory text of paragraph (a)(2), and paragraphs (a)(2)(iii), and paragraph (a)(3).

The revisions and additions read as follows:

§ 164.522 Rights to request privacy protection for protected health information.

(a)(1) * * *

(ii) Except as provided in paragraph (a)(1)(vi) of this section, a covered entity is not required to agree to a restriction.

* * * * *

(vi) A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

(2) *Implementation specifications: Terminating a restriction.* A covered entity may terminate a restriction, if:

* * * * *

(iii) The covered entity informs the individual that it is terminating its agreement to a restriction, except that such termination is:

(A) Not effective for protected health information restricted under paragraph (a)(1)(vi) of this section; and

(B) Only effective with respect to protected health information created or received after it has so informed the individual.

(3) *Implementation specification: Documentation.* A covered entity must document a restriction in accordance with § 160.530(j) of this subchapter.

* * * * *

■ 55. Amend § 164.524 as follows:
■ a. Remove paragraph (b)(2)(ii) and redesignate paragraph (b)(2)(iii) as paragraph (b)(2)(ii);
■ b. Revise newly designated paragraph (b)(2)(ii);
■ c. Revise paragraph (c)(2)(i);
■ d. Redesignate paragraph (c)(2)(ii) as paragraph (c)(2)(iii);
■ e. Add new paragraph (c)(2)(ii);
■ f. Revise paragraphs (c)(3) and (c)(4)(i);
■ g. Redesignate paragraphs (c)(4)(ii) and (c)(4)(iii) as paragraphs (c)(4)(iii) and (c)(4)(iv), respectively; and
■ h. Add new paragraph (c)(4)(ii).

The revisions and additions read as follows:

§ 164.524 Access of individuals to protected health information.

* * * * *

(b) * * *

(2) * * *

(ii) If the covered entity is unable to take an action required by paragraph (b)(2)(i)(A) or (B) of this section within the time required by paragraph (b)(2)(i) of this section, as applicable, the covered entity may extend the time for such actions by no more than 30 days, provided that:

(A) The covered entity, within the time limit set by paragraph (b)(2)(i) of

this section, as applicable, provides the individual with a written statement of the reasons for the delay and the date by which the covered entity will complete its action on the request; and

(B) The covered entity may have only one such extension of time for action on a request for access.

(c) * * *

(2) *Form of access requested.* (i) The covered entity must provide the individual with access to the protected health information in the form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual.

(ii) Notwithstanding paragraph (c)(2)(i) of this section, if the protected health information that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the covered entity must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

* * * * *

(3) *Time and manner of access.* (i) The covered entity must provide the access as requested by the individual in a timely manner as required by paragraph (b)(2) of this section, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy of the protected health information at the individual's request. The covered entity may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

(ii) If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

(4) * * *

(i) Labor for copying the protected health information requested by the individual, whether in paper or electronic form;

(ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;

* * * * *

■ 56. In § 164.532, revise paragraphs (a), (c)(2), (c)(3), (d), (e)(1), and (e)(2), and add paragraphs (c)(4) and (f) to read as follows:

§ 164.532 Transition provisions.

(a) *Standard: Effect of prior authorizations.* Notwithstanding §§ 164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, a waiver of informed consent by an IRB, or a waiver of authorization in accordance with § 164.512(i)(1)(i).

* * * * *

(c) * * *

(2) The informed consent of the individual to participate in the research;

(3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with § 164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or

(4) A waiver of authorization in accordance with § 164.512(i)(1)(i).

(d) *Standard: Effect of prior contracts or other arrangements with business associates.* Notwithstanding any other provisions of this part, a covered entity, or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), only in accordance with paragraph (e) of this section.

(e) *Implementation specification: Deemed compliance.* (1) *Qualification.* Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§ 164.308(b), 164.314(a), 164.502(e), and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:

(i) Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and

(ii) The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.

(2) *Limited deemed compliance period.* A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:

(i) The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or

(ii) September 22, 2014.

* * * * *

(f) *Effect of prior data use agreements.* If, prior to [January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of:

(1) The date such agreement is renewed or modified on or after September 23, 2013; or

(2) September 22, 2014.

* * * * *

Dated: January 15, 2013.

Kathleen Sebelius,

Secretary.

[FR Doc. 2013–01073 Filed 1–17–13; 4:15 pm]

BILLING CODE 4153–01–P