Report on
PATIENT PRIVACY

Volume 10, Number 8 • August 2010

Practical News and Strategies for Complying With HIPAA

Contents

The Sept. issue of *RPP* will include additional coverage of the exhaustive new rules proposed by HHS in the July 14 *Federal Register,* with stories on minimum necessary, the sale of PHI, the notice of privacy practices, and new enforcement and tiered penalty provisions.

Editor
Liana Heitin
lheitin@aispub.com

Contributing Editor
Nina Youngstrom

Executive Editor
Jill Brown

Confusion Reigns in HHS's Regulation of Data Security Breach Notifications

HHS said July 29 it is withdrawing the final rule for breach notification of unsecured protected health information that it submitted to OMB for regulatory review on May 14, 2010, in order "to allow for further consideration." The interim final rule published in the *Federal Register* on Aug. 24, 2009 (which became effective Sept. 23, 2009) remains in effect.

According to an announcement on the HHS website, "This is a complex issue.…We intend to publish a final rule in the *Federal Register* in the coming months." The Office for Civil Rights tells *RPP*, "The interim final rule continues in full force and effect until a final rulemaking is issued. The final rulemaking will take into account the comments received on the interim final rule and our experiences with administering the new breach notification provisions since last September. These are routine, formal regulatory processes."

While HHS claims this is all very routine, federal agencies do not typically submit regulations for OMB approval and then withdraw them on their own. One wonders whether there may be a reconsideration of the controversial "harm standard," which was a surprise when the interim final rules were released last August (see *RPP 10/09, p. 1*). At the time, privacy advocates felt the harm standard guts the breach notice rules — since it permits CEs to avoid breach notices if they determine (all on their own) that a breach does not create a sufficient risk of harm to individuals — and they vowed to have it removed from HHS's final regulations.

See the HHS statement at tinyurl.com/2a5dk5j. ✧

Draft HITECH Rules Expand List of Business Associates, Restrict Marketing, Fundraising

The exhaustive proposed rulemaking that ostensibly amends HIPAA to reflect requirements in last year's HITECH Act goes well beyond the act in many respects and could result in huge new burdens for many covered entities and business associates.

The proposed rules — which consume 57 pages of the July 14 *Federal Register* — clamp down on fundraising and marketing, and require CEs to rewrite and reissue their notices of privacy practices to better reflect opt-out and other rights that patients have, developments that are likely to be a massive national undertaking (see stories, p. 6 and 8). But on another front, the proposal also seeks to lighten some of the compliance load for researchers (see story, p. 9).

The proposed rules also lay out the new security requirements that business associates (BAs) must meet, as the HITECH Act specified *(RPP 3/09, p. 1)*. They also set up a timetable for new business associate agreements to be hammered out reflecting the new requirements. But perhaps the biggest surprise, which is likely to have a monumental impact in the health care industry generally, is the appearance in the proposed rules of the term "subcontractor." These organizations handle protected health information for BAs, but until now, never had to comply with the privacy and security rules (see story, p. 4).

The proposed rulemaking has a 60-day comment period, which began July 14 with its publication in the *Federal Register*, after which HHS will issue a final rule, a process

that could take several additional months. While the final rule will not be enforced until 180 days after it is published, covered entities and business associates would be well-advised to begin planning their compliance with a variety of new provisions.

HHS says the purpose of the rulemaking, drafted by the Office for Civil Rights, is to "implement recent statutory amendments" (namely, the HITECH Act), and "to strengthen the privacy and security protection of health information, and to improve the workability and effectiveness of" the privacy and security rules.

Kristen Rosati, a partner at Coppersmith Schermer & Brockelman PLC, in Phoenix, sums up the proposed rulemaking as a "mixed bag" for CEs and BAs. "While OCR is proposing to fix a few long-standing problems in the privacy rule, such as the prohibition against using compound authorizations in research and communications with family members about deceased patients, the proposed rule is very disappointing in other ways," such as the requirement for amendments to business associate agreements, she says.

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Editor, Liana Heitin; Contributing Editor, Nina Youngstrom; Executive Editor, Jill Brown; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Corey Hughes; Production Coordinator, Russell Roberts

Call Liana Heitin at 800-521-4323 with story ideas for *RPP*.

Subscribers to **Report on Patient Privacy** also receive access to **AIS's HIPAA Compliance Center** at www.AISHIPAA.com, with archives of past issues of the newsletter, links to government documents, and 30 searchable narratives written by experts in privacy and security compliance. Subscribers receive e-mail notification when a new issue of **Report on Patient Privacy** is posted on the Web site. Please whitelist aishipaa@aispub.com to ensure e-mail delivery.

To order **Report on Patient Privacy:**

(1) Call 800-521-4323 (major credit cards accepted), or

(2) Order online at www.AISHealth.com, or

(3) Staple your business card to this form and mail it to:
AIS, 1100 17th St., NW, Suite 300, Wash., DC 20036.

Payment Enclosed* ❑ $429

Bill Me ❑ $404

*Make checks payable to Atlantic Information Services, Inc.
D.C. residents add 6% sales tax.

Tanya Forsheit, a founding partner of the InformationLawGroup, based in Los Angeles, says that, while many of the proposed changes were expected, they undoubtedly will require a great deal of compliance effort, which should begin in earnest.

"CEs, BAs and other companies that do work for BAs should all be in the process of identifying their obligations under the proposed rule," Forsheit says. "These are changes that require focus. If the regulations go into effect in their current form, there will be a lot of work to be done."

New Business Associates Identified

As a result of the proposed rules, covered entities will now need to sign business associate agreements (BAAs) with new types of BAs.

Under HIPAA, a "business associate" is defined as a "person who perform functions or activities on behalf of, or certain services for, a CE that involve the use of protected health information." The following are examples of BAs:

◆ Third-party administrators

◆ Pharmacy benefit managers

◆ Claims processing or billing companies,

transcription companies,

◆ Persons who perform legal, actuarial, accounting, management, or administrative services for covered entities and who require access to protected health information. (For a more detailed discussion of "who is a BA," see *RPP 4/10, p. 8.*)

However, the proposed rulemaking, reflecting the HITECH Act provisions, adds a number of new organizations to the list of BAs. These are:

◆ Patient safety organizations (PSOs) and external organizations that perform similar activities,

◆ Health information organizations (formerly referred to as health information exchange organizations),

◆ E-prescribing gateways,

◆ Regional health organizations, and

◆ Personal health records vendors.

The rulemaking clarifies that a hospital that has a "component PSO that performs patient safety activities" on its behalf would not be a BA because the PSO's staff would be considered members of the hospital's workforce.

The HITECH Act had already specified that an organization that provides data transmission of PHI to CEs or BAs and "requires regular access on a routine basis to such PHI" would be a business associate. These include health information exchange organizations, e-prescribing gateways, or regional health organizations. The proposed rules confirm that these are BAs and exempts another group from BA obligations: organizations that are "mere

conduits for the transport of protected health information but do not access the information other than on a random or infrequent basis."

Similarly, HITECH said that "a vendor that contracts with a CE to allow the covered entity to offer a personal health record to patients as part of the CE's electronic health record shall be treated as a BA," so the proposed rules add PHR vendors to the definition of "business associate."

As noted above, the rulemaking added a whole new category of BAs, called "subcontractors" (see story, p. 4).

BA Agreements Must Be Amended

The HITECH Act specified that "additional privacy and security requirements of subtitle D of the Act are applicable to business associates and that *such requirements shall be incorporated into business associate contracts* (emphasis added)."

Since the HITECH Act was passed, CEs and BAs have been debating whether BAAs needed to be amended to specify the new privacy and security provisions for which BAs are now responsible, or whether a blanket provision that some BAAs contain specifying that the BA will comply with all applicable laws and regulations would suffice. The prospect of the new requirements for BAs had already made many CE-BA relationships testy and contentious *(RPP 4/10, p. 1)*.

The proposed rulemaking appears to settle the debate, with the inclusion of grandfathering provisions and a transition period during which time BAs and CEs must bring their agreements into compliance.

Rosati notes that many CEs and BAs had already begun the process of amending their BAAs, but others felt it wasn't necessary. Now this is no longer an option.

"This triggers the need for thousands and thousands of contracts to be amended, which I think is a silly waste of resources," she says. "The HITECH Act gives OCR the authority to directly regulate business associates, and it doesn't add any protection for patients to add these contract provisions to the BAAs."

BAAs Must Describe Obligations

The rulemaking gives CEs and BAs somewhat of a grandfathering period that will affect when their agreements need to be updated. It states that those BAAs in compliance with the pre-July 2010 requirements may remain in place for up to a year and 240 days from the date of publication of a final rule. (For Rosati's examples of how this would work, see box, p. 4).

"Some large hospital systems have thousands and thousands of BAAs," she says. "They need to catalogue when the BAAs expire, or roll over."

Each time a BAA is amended, or it is even opened up for amendment, negotiations may ensue that strain relationships. So be prepared for the time this might take, Rosati says.

The proposed rules state that a contract between a CE and a BA must:

◆ Establish the permitted and required uses and disclosures of protected health information by the BA;

◆ Prohibit the BA from the use or further disclosure of the information other than as permitted or required by the contract or as required by law;

◆ Require the BA to use appropriate safeguards and comply, where applicable, with [the security rule] with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

◆ 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;

◆ Contract with subcontractors; and

◆ Return or properly dispose of the CE's PHI when the contract is over.

Minimum Necessary Would Apply to BAs

Another possible BA-related change that is tucked into the proposed regulation: BAs and their subcontractors would have to comply with the minimum necessary requirement that CEs must meet.

This onerous concept is widely derided as causing unnecessary and inappropriate restrictions on the exchange of PHI. The prospect that BAs and subcontractors, which are just learning their new obligations, would also have to honor this requirement could lead to near chaos amid the thousands of transactions health care entities engage in daily.

The government has known for years that the minimum necessary standard has been misunderstood and misapplied; a study it commissioned in 2007 showed that many organizations were applying minimum necessary to treatment, and some even applied it in-house *(RPP 5/07, p. 3)*.

The HITECH Act required HHS to issue guidance on the minimum necessary standard within 18 months of

Access the comprehensive HITECH Act rules issued in the July 14 *Federal Register* at the subscriber-only website www.AISHIPAA.com, where all significant HIPAA (and related) laws and regulations are archived. If you don't have your password, please call 800-521-4323 or e-mail customerserv@aispub.com.

passage (by Aug. 18), and in the meantime, required CEs to share only limited data sets whenever practical, bypassing the typical minimum necessary analysis.

Yet few CEs seemed aware of this *(RPP 5/10, p. 1)*. The July 14 proposed rulemaking would require business associates to comply with the minimum necessary standard, a prospect that is undoubtedly going to lead to more confusion, especially because this new requirement for BAs comes prior to the issuance of the new minimum necessary guidance.

Rosati notes one other revision: "One of the other provisions that changed is the removal of the 'rat rule.'" Under the previous regulations, if the CE knew that a BA was violating the terms of its business associate agreement, the CE was required to take steps to remedy the issue or terminate the agreement. If for some reason termination wasn't possible, such as where the BA was a sole-source provider, the CE was required to contact HHS and describe the noncompliance.

Contact Rosati at krosati@csblaw.com and Forsheit at tforsheit@infolawgroup.com. ✧

Thousands of 'Subcontractors' May Soon Have to Comply with HIPAA

Perhaps the biggest surprise in HHS's July 14 proposed rulemaking (see story, p. 1) was a concept that went beyond language contained in the HITECH Act, namely the appearance of the term "subcontractors" in the list of organizations that would have to comply with the same privacy and security regulations as business associates.

"This will have a huge impact because it means that there are many, many people who have to comply with the HIPAA rules who didn't have to before," Kristen Rosati, a partner with Coppersmith Schermer & Brockelman PLC in Phoenix, tells *RPP.* "It really vastly expands the universe of organizations that have to comply with these regulations."

These subcontractors are one tier further down on the chain of those who handle protected health information. Subcontractors are akin to business associates of business associates. They do for BAs what BAs do for CEs.

Whether it is necessary to include them in the HIPAA regulations can be debated, and it remains to be

Some BAAs Would Be Grandfathered

The notice of proposed rulemaking issued by HHS on July 14 gave covered entities (CEs) and business associates (BAs) time to get their agreements updated to comply with the new HITECH Act requirements that now apply to BAs.

It allowed some agreements to remain unchanged for more than a year if certain somewhat confusing conditions are met.

Kristen Rosati, a partner with Coppersmith Schermer & Brockelman PLC, in Phoenix, offers the following practical on advice on what changes are needed and when.

CEs and BAs can continue to operate under business associate agreements that are in place at the time the final rule is published in the *Federal Register* — if those agreements comply with the current requirements — for up to one year and 240 days from the date of publication.

However, if those contracts are renewed or modified 60 days or later past the date of publication, the agreement will require modification when the final rule is issued to comply with the new requirements.

The Office for Civil Rights interprets evergreen contracts that automatically renew without any change in terms as not being a renewal or modification under the regulations.

Rosati gives an example of how these transition provisions would apply, assuming that the final rule is published on Jan. 1, 2011:

◆ A business associate agreement in place on Dec. 1, 2010, would be in compliance until Aug. 1, 2012 (one year, 240 days after the final rule is published), as long as that business associate agreement complies with the "old" HIPAA business associate agreement requirements.

◆ If that business associate agreement is amended on Feb. 1, 2011 (fewer than 60 days after the publication of the final rule), the amended business associate agreement would be in compliance, as long as the business associate agreement complies with the "old" HIPAA business associate agreement requirements.

◆ If that business associate agreement is amended on April 1, 2011 (more than 60 days after the publication of the final rule), the business associate agreement must comply with the new HIPAA business associate agreement requirements.

◆ If that business associate agreement automatically renews without amendment, it must comply with the new HIPAA business associate agreement requirements one year and 240 days after publication of the final rule (or by Aug. 1, 2012).

seen whether they make it into the final rule. But for now, the concept is giving BAs and HIPAA experts a huge headache. They expect that the concept is here to stay and recommend the creation of compliance strategies to address this issue now.

Desire to Avoid a 'Lapse'

As the rulemaking explains, "we propose to add language…to the definition 'business associate' to provide that subcontractors of a covered entity — that is, 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."

Perhaps recognizing the magnitude of this expansion, HHS says these "proposed modifications are similar in structure and effect to the privacy rule's initial extension of privacy protections from CEs to BAs through contract requirements to protect downstream protected health information."

HHS believes it must extend requirements to subcontractors to keep with Congress' intent and hold business associates fully accountable. "The proposed provisions 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," the rulemaking states. "Allowing such a lapse in privacy and security protections may allow business associates to avoid liability imposed upon them" by relevant portions of the HITECH Act.

HHS also says that even if the business associate, perhaps because it isn't aware of this new provision, fails to execute a BAA, the government would consider that the definition "would apply to an agent or other person who acts on behalf of the BA." This means that, under the proposed regulation, both the BA and its subcontractor are still required to comply whether contracted to each other or not.

Determine Who Is a Subcontractor

Tanya Forsheit, a founding partner of the InformationLawGroup, based in Los Angeles, says CEs need to contact their BAs and find out which entities might qualify as subcontractors.

"If you are a CE, you should be doing due diligence to find out who your BAs are sharing data with," she says. "And subcontractors will have to figure out if they are doing work for a BA" that would put them under HIPAA according to the proposed rulemaking.

As CEs should be doing with BAs, BAs may also choose to scrutinize the list of subcontractors to determine if they appear to be a good risk, or whether they pose an unnecessary risk. While the HITECH Act holds BAs directly liable for fines, penalties and other enforcement actions, and the proposed rules now do the same for subcontractors, it is still the CE that might have to notify patients, the media and OCR if there is a breach. It is the CE's reputation that will be on the line if something goes wrong.

Asked who could be a subcontractor, Forsheit says the list is almost endless. "It could even be an ISP or a cloud vendor," she says.

If so, this might prove problematic, Forsheit says. "Generally, a lot of cloud vendors have really pushed back when CEs and other data owners wanted them to accept liability for any privacy and security compliance obligations of the data owners," she says. The July 14 rulemaking gives the example of a document-shredding company hired by a BA, such as a third-party administrator, as one possible subcontractor.

Rosati says that the new obligations are likely to come as a shock. "There are going to be a lot of companies that are not aware of their compliance obligations," she says. "One of my concerns is making sure there is adequate education about this."

Once a BA (and a CE, if interested) has vetted a subcontractor, the BA must sign an agreement with the subcontractor, which would still technically be a BAA.

Agreement Must Contain Specifics

Forsheit notes that these agreements between BAs and subcontractors will need to spell out the subcontractor's obligations to the BA in much the same way the BA is obligated to the CE.

For example, the agreement with the subcontractor should require the subcontractor to notify the BA when there is a breach, and to do so within a specified period of time.

The BAA may ask for such notice to occur "as soon as possible," Forsheit says. In her practice, she has seen BAAs that specify as little as a few hours or a few days, with a verbal notice to be made first, followed by a written report within a few days.

She cautions that the reporting time frame should also be calculated to comply with any state notification requirements, which can be shorter than 60 days.

In addition, the BAA should spell out who notifies patients, OCR and the media in the event of a breach that exceeds 500 affected individuals.

The proposed rulemaking makes it clear that the CE itself does not have to have a relationship with the subcontractor. "[T]his 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," HHS says.

Finally, the agreement with the subcontractor will need to address indemnification issues and costs associated with breaches, such as the offering of credit monitoring for affected individuals, so that, in the event of a breach, it is clear what the BA expects of its subcontractor.

Objections Should Be Raised with HHS

The BA's agreement with the subcontractor may be instructive for the subcontractor in and of itself, Rosati says, as it will help explain the subcontractor's duties. Her fear, she says, is that "a subcontractor might sign an agreement without knowing that signing this triggers HIPAA compliance responsibilities."

Rosati feels strongly that affected organizations should comment on the proposed rulemaking, including the issue of including the subcontractors. In her mind, there is some question as to whether HHS has the legal authority to undertake such an expansion of organizations that must comply with HIPAA.

She suggests that CEs and BAs (and subcontractors) send comments to HHS on areas where HHS "may have gone too far," she says. "Identify areas where there are potential operational problems that will be difficult to implement or will cause substantial expense," Rosati adds.

Contact Rosati at krosati@csblaw.com and Forsheit at tforsheit@infolawgroup.com. ✧

Marketing Regs Clear Up Some Provisions, Further Muddle Others

Within the massive set of proposed regulations published in the July 14 *Federal Register*, HHS re-addressed the HIPAA privacy rule's marketing provisions, which most people agree have been murky from the start. While some experts say the rule merely explains the statute, others contend it further narrowed and complicated the already intricate provisions.

According to Kirk Nahra, an attorney in Wiley Rein's Washington, D.C., office, the new opt-out requirements for treatment communications — which will prove burdensome to covered entities — are the most significant additions. But overall, he says, the regulations did little more than explain the statute.

The regulations weren't as "shocking…as the subcontractor BAs, for example," says Brian Annulis, an attorney with Meade & Roach in Chicago, but there were a few notable changes, such as the distinction between treatment and health care operations. Jacqueline Saue, a Washington, D.C.-based attorney with Foley & Lardner LLP, says marketing provisions have always been "fairly controversial" and that the new regulations narrow the definition of "marketing."

Under the HIPAA privacy rule, marketing using protected health information (PHI) requires a patient's prior written consent. The two types of marketing that do not require authorization are face-to-face communications and communications that involve products or services of nominal value. Furthermore, a communication is not considered "marketing" — and consequently does not require authorization — if it falls under one of the three HIPAA exceptions for treatment, payment and/or health care operations (TPO):

◆ It describes a health-related product or service (or payment for a product or service) that is provided by, or included in a plan of benefits of, the CE making the communication;

◆ It is made for treatment; or

◆ It is made for case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

The HITECH Act, passed in February 2009 *(RPP 2/09, p. 1)*, added another restriction for communications that fall under TPO: The CE cannot have received payment for the communication.

However, the HITECH Act makes three exceptions here as well. If the CE did receive payment for the communication, authorization is still not necessary when:

(1) The communication describes only a drug or biologic currently being prescribed for the individual, and the amount of payment received for making the communication is reasonable;

(2) The CE making the communication has received a valid HIPAA authorization from the individual; or

(3) The communication is made by a business associate and is consistent with the terms of its BA agreement.

HHS Proposes Changing Definitions

The new regulations make a few linguistic clarifications. For starters, the rulemaking proposes using the term "financial remuneration" in place of "direct or indirect payment" within the definition of "marketing." As it states, this will help "to avoid confusion" since "payment" in the privacy rule means payment for health care services.

The proposed regulations also emphasize that financial remuneration, under 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." The proposed rules

include examples of potentially confusing situations related to this nuance (see examples below).

Under the HITECH Act exceptions to marketing, a communication for a drug or biologic currently being prescribed is exempt if the payment received for making the communication is "reasonable in amount" (as stated above). The new rules propose changing the exception to say that the communication is exempt provided the financial remuneration received is "reasonably related to the covered entity's cost of making the communication."

Stephen Weiser, an attorney with Meade & Roach in Chicago, explains that Congress tightened the language here because it does "not want pharmaceutical companies paying an amount that would serve as an inducement for the health plan or health care provider to promote a particular medication."

HHS is requesting comments on this exception to determine whether communications for generic alternatives or new formulations of a drug should fall under it as well. Weiser says this may be a "touchy subject" because "while a health plan's promoting generic alternatives may reduce the costs of coverage, it may not be in the interest of pharmaceutical companies who make the equivalent of the medication."

In the rulemaking's most notable change to the marketing provisions, HHS proposes adding three requirements to the treatment exception. A written treatment communication for which a provider receives remuneration would be permitted without authorization as long as the provider:

(1) States in the notice of privacy practices (NPP) that the provider may send treatment communications for which it received remuneration and that the individual has the ability to opt out of such communications;

(2) Discloses in the communication itself that the provider received financial remuneration for making the communication; and

(3) Gives the individual a "clear and conspicuous opportunity to elect not to receive any further such communications."

The notice and opt-out were not in the initial HITECH Act provisions.

The opt-out is "a big deal," asserts Nahra. "It's a big burden for people to set up an opt-out mechanism. I don't think [HHS] realizes how big a deal that is." For instance, he says, if a hospital issues treatment-related marketing communications for a chiropractic firm that involve payment from the chiropractic firm, the communications might be relevant only to 5% of patients. Should the hospital give the opt-out to 100% of patients, perhaps with the notice of privacy practices, knowing that it won't be pertinent to most patients? Or should the hospital develop a system for giving it to only the 5% for whom it is relevant? How does the hospital keep track of who receives which opt-out forms or, if everyone receives them, who has opted out and who hasn't? "I'm not saying it's not doable; I'm saying it's harder than they seem to recognize," says Nahra.

Weiser says it's significant that the rule requires providers to amend their NPPs again. The notice of privacy practices may become even more confusing and overwhelming to patients if providers have to keep "cramming more information into it," he says.

According to the proposed rulemaking, CEs should use a "simple, quick, and inexpensive" opt-out method, such as a toll-free number or e-mail address. It states that requiring individuals to write and send a letter to the CE would "constitute an undue burden on the individual." HHS requests comments on "whether the opt out should prevent all future subsidized treatment communications by the provider or just those dealing with the particular product or service described in the current communication."

Elizabeth Litten, a Princeton, N.J.-based attorney with Fox Rothschild LLP, says it probably makes the

Is Prior Authorization Required for Communication?

Example	Is Authorization Required?	Why?
A covered entity (CE) makes a communication to its patients regarding the acquisition of new state-of-the-art medical equipment, which the equipment manufacturer pays for.	Yes	The equipment manufacturer paid the CE to send the communication to its patients.
A local breast cancer foundation funds a CE's mailing to patients about the availability of new state-of-the-art mammography screening equipment.	No	The CE did not receive remuneration by or on behalf of the entity whose product or service was being described.
A hospital sends flyers to its patients announcing the opening of a new wing where the funds for the new wing were donated by a third party.	No	The financial remuneration to the hospital from the third party was not in exchange for the mailing of the flyers.

SOURCE: July 14 Proposed Rulemaking

most sense for an opt-out to cover only that particular product or service. "It's impossible to cross-check every source. A patient could say, 'I didn't want that cardiac stuff, but the wound stuff is of interest to me.' To say once you opt out you're opting out of any treatment-related communication in the future, I think is not the right result."

Since the new opt-out requirements apply differently for treatment and health care operations, the proposed rules clarify the two categories. A communication about health-related products or services for case management or care coordination, or to recommend alternative treatments or settings of care, falls under health care operations if it is made in a "population-based fashion" — if the communication is not specific to an individual's condition. For instance, a blanket mailing sent to all patients about a physical therapy practice would fall under the health care operations umbrella. The opt-out and notice are not necessary.

On the other hand, a communication made "to further the treatment of a particular individual based on that individual's health care status or condition" falls under treatment. Sending a pregnant patient a brochure about a birthing center would require the notice and opt-out.

New Definition Closes a 'Major Loophole'

In another substantial change, the rule proposes removing language that defines "marketing" as "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." The rulemaking states that situation would constitute "sale of PHI" rather than marketing. Saue says the previous language provided a major loophole. "It required individual authorization for marketing, but only in that one particular circumstance where the third party was making the communication. It did not apply where you as a CE were not disclosing PHI to a third party but receiving remuneration from the third party to communicate with your customers.…It's one of the major changes the regulations make, to close that loophole."

HHS is forthright in the rule about seeking outside advice, which Annulis says is a positive sign for CEs. "I give [HHS] kudos for being willing to take comments," he says. "They could have published this as a final rule, but they didn't."

Contact Nahra at (202) 719-7335 or knahra@wileyrein.com, Annulis at (773) 907-8343 or bannulis@meaderoach.com, Saue at (202) 672-5306 or jsaue@foley.com, Weiser at (312) 403-4284 or sweiser@meaderoach.com and Litten at (609) 895-3320. ✧

Simple Mailing Mistakes Could Be HIPAA Violations Under New Rules

Covered entities would be wise to become familiar with the new July 14 proposed rules for fundraising, which could turn an accidental mailing into a costly mistake. One expert says the proposed fundraising rules are straightforward overall but that it is more revealing to look at the areas where HHS is seeking comments. The final rule, she says, is likely to tighten some fundraising restrictions while loosening others.

The original privacy rule permits some fundraising activities by a CE without patient authorization, including appeals for money and sponsorship of events. The CE may not use or disclose protected health information (PHI) for fundraising unless there is an explicit statement in its notice of privacy practices (NPP) about such uses and disclosures. In addition, the CE must include in any fundraising materials it sends to an individual a description of how the individual may opt out.

The new regulations propose strengthening the language regarding the opt-out notification, stating that CEs must provide individuals with a "clear and conspicuous" opportunity for the individual to elect not to receive future fundraising communications.

Elizabeth Callahan-Morris, an attorney for Hall, Render, Killian, Heath & Lyman, PLLC, says HHS likely included the "clear and conspicuous" language for emphasis — not because of any problem. "I don't think it was a response to fundraising communications that had it in small font or where it wasn't conspicuous.…I think this was a message to the health care industry that they really want people to understand they have the opportunity to opt out. It's reinforcement of the public policy consideration rather than trying to correct a wrong in the industry, she says."

Opt-Out Notice Is Stronger

According to the proposed rules, the opt-out "may not cause the individual to incur an undue burden or more than nominal cost." As with the section on marketing restrictions (see story, p. 6), the new proposed guidelines suggest the use of a toll-free number or e-mail address to "provide individuals with a simple, quick, and inexpensive" means of opting out. Requiring individuals to write a letter would be considered burdensome, it states. Callahan-Morris says it's likely the information on opt-out methods will be included in the guidance or frequently asked questions after the final rule is issued.

Currently, the privacy rule states that covered entities must make "reasonable efforts" to ensure those who have opted out don't receive future communications. The new regulations up the ante here, proposing that CEs "may not

send fundraising communications to an individual who has elected not to receive such communications."

In fact, sending an individual who has opted out a communication would be considered a violation of the law and subject to the tiered enforcement penalties.

"Now there's an absolute prohibition and strict liability for contacting people who opted out already," says Stephen Weiser, an attorney with Meade & Roach in Chicago. If the CE had policies and procedures in place to specify the opt-out (thus exercising due diligence) but made a mistake, the violation would amount to a first-tier penalty, he says.

For violations due to reasonable cause, not willful neglect, the penalty is at least $1,000 and up to $50,000 for each violation *(RPP 11/09, p. 5).*

Weiser notes that it's not unusual for organizations to have duplicate fundraising lists, so CEs should be wary of these kinds of errors. "The nonprofits are going to be really up-in-arms about this total prohibition. They cannot make a mistake," he says.

Duplicate Lists Can Trip You Up

"It's something that if you overlook it, you could get tripped up," Callahan-Morris says. "If someone receives a fundraising communication and opted out — those types of people might be inclined to file a complaint…. With the new rule, I would recommend having a more formal process to ensure opt-outs are recognized."

The proposed rulemaking maintains the requirement that CEs notify individuals of their ability to opt out in the NPP. The rule also states, in a somewhat obvious clarification, that providers "may not condition treatment or payment on an individual's choice with respect to receiving fundraising communications."

"Really, what's more interesting than what's proposed in the rule are the issues OCR is asking the public to comment on," says Callahan-Morris.

First, HHS is seeking comment on how the opt-out should apply. If an individual opts out, should that apply to all future fundraising communications? Or just to the fundraising campaign described in the letter? And how can individuals opt back in? Should they be able to e-mail or use a toll-free number to get back on the fundraising list?

HHS also uses the proposed rulemaking as a forum for reopening discussion on an issue outside the HITECH Act: What kind of information should CEs be able to use or disclose for fundraising communications? As it stands, organizations can use only patient demographic information and dates of service. The proposed rules notes that many CEs have raised concerns that the inability to use information such as the department of service where care was received "harms their ability to raise funds from often willing and grateful patients."

The current rule "frustrates fundraisers tremendously," says Brian Annulis, an attorney with Meade & Roach in Chicago. "They have folks that are so pleased about the care they got at the Alzheimer's unit, that if they reached out and solicited them, they would do great. But there's no easy way to do that because disease-specific solicitation is not permitted."

The National Committee on Vital and Health Statistics held hearings and public testimonies on this issue in 2004 and recommended that the privacy rule allow for the disclosure of departments of service, using broad designations such as surgery or oncology. Callahan-Morris says HHS is "looking at what other changes make sense to do all in one fell swoop, and this would be one of them."

Overall, in the final rule, there's likely to be "both a tightening and loosening" of current requirements, says Callahan-Morris. Requirements concerning the "clear and conspicuous" opt-out, what goes in the NPP and the penalty for sending communications to an individual who opted out are all getting tighter.

"What I think is going to become looser is the amount of information CEs can use for fundraising," she says. "They haven't loosened anything in the proposed rule but I think we're going to see it in the final."

Contact Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com, Annulis at (773) 907-8343 or bannulis@meaderoach.com and Weiser at (312) 403-4284 or sweiser@meaderoach.com. ✧

Surprise Provisions in HITECH Rules Would Ease Research Burdens

Years after being warned by numerous organizations, including the Institute of Medicine (IOM), that redundant HIPAA requirements were hampering research, HHS has proposed changes that might solve some of the problems.

Buried in 57 pages of the July 14 *Federal Register* are proposed rules to permit use of a "compound" or single form to allow protected health information for research and treatment purposes. In addition, HHS is revisiting its belief that a separate authorization is required when tissue samples, data or other study material have a secondary use for another study. Both could be beneficial to researchers and ease compliance with HIPAA and the Common Rule, which is HHS's policy covering human subjects research supported by federal funding.

Quite unexpectedly, the proposed rulemaking does what the HITECH Act itself did not do for research. When the act was passed, research groups decried that

it did nothing to relieve burdens on them and figured they'd have to wait for health reform legislation to achieve that goal.

One of the groups that has pushed for improvements is the Association of American Medical Colleges. Ann Bonham, AAMC's chief scientific officer, says the proposed rulemaking showed that the government had taken notice of researchers' concerns. She acknowledges the efforts of the Office for Civil Rights, which enforces HIPAA and is responsible for drafting the rulemaking.

"The AAMC is pleased that the OCR recognizes the barriers that the current privacy rule has imposed on researchers who are engaged in improving the health of all Americans through their work," she says. "Protecting the privacy of health information of citizens who have generously chosen to participate in research, while at the same time allowing researchers to use that information to advance health, is in the best interest of the nation."

Bonham adds that AAMC will seek feedback from its members on the rulemaking. "We will be discussing the proposed changes in the NPRM with our members to determine the extent to which they address the problems, or need to be further modified, and will submit comments to OCR," Bonham says.

Mindy Steinberg, policy and program analyst for the Association of Academic Health Centers (AAHC), which also criticized HIPAA's effect on research, had a similar response. After reading the proposed rulemaking, "my feeling is generally positive," she says. "We are pleased to see that OCR has taken this opportunity to begin addressing some of the research-related concerns raised by AAHC…the IOM and others. Revising the prohibition on compound authorizations and considering changes to authorizations for future research are both significant steps towards alleviating the negative impact the HIPAA privacy rule has had on research."

As the rulemaking states, "Research-related treatment offered through a clinical trial is nearly always conditioned upon signing the informed consent to participate in the trial and the authorization to use or disclose the individual's protected health information for the trial."

HHS acknowledges this has been a problem. "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," it says in the rulemaking.

To address this issue, "We agree that allowing a covered provider to combine research authorizations would streamline the process for obtaining an individual's authorization for research and would make the documentation responsibilities of these covered entities more manageable," HHS says.

This change "would also result in an authorization that would be simpler and, therefore, more meaningful to the individual (in contrast to the individual receiving multiple forms that may be confusing)," HHS says. "We, therefore, propose 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 con-

ditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities."

Complaints Are Longstanding

The proposed changes address well-documented problems. Just 10 days before the final version of the legislation containing the HITECH Act passed the Senate, a committee impaneled by the Institute of Medicine issued a scathing report, "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research," which urged Congress to exempt research from the rules and impose an entirely new system, or at least make significant changes in the current requirements.

The proposed rulemaking notes that the IOM report made "specific recommendations to allow combined authorizations for clinical trials and biospecimen storage."

Five years earlier, in September 2004, Ernest Prentice, then chair of the Secretary's Advisory Committee on Human Research Protections (SACHRP), sent a letter to then HHS Secretary Tommy Thompson containing eight recommendations on how to lessen HIPAA's effect on research.

The fifth recommendation was that HHS "should revise HIPAA's compound authorization rules to permit the combining of research authorizations into one form when researchers seek to bank data and materials collected as part of an underlying clinical trial; however, in order to promote patients/subject choice, the rules should require that subjects be given the ability to 'opt in' to the banking portion of the authorization."

HHS acknowledges the combined authorizations would be beneficial in many situations.

continued

PATIENT PRIVACY COURT CASES

This monthly column is written by Kayla Tabela of the Washington, D.C., office of Sonnenschein Nath & Rosenthal LLP. It is designed to provide RPP *readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Tabela at ktabela@sonnenschein.com.*

◆ **Health Net Pays $250,000 to settle claims under the HITECH Act.** On July 6, 2010, Health Net of the Northeast Inc., agreed to pay $250,000 to resolve alleged violations of HIPAA. The allegations were brought by Connecticut Attorney General Richard Blumenthal under the HITECH Act, which is often credited with giving HIPAA "teeth" because it vests authority in state attorneys general to enforce the HIPAA provisions. Connecticut's attorney general launched the allegations after discovering that Health Net waited six months to notify individuals of a data breach *(RPP 12/09, p. 1)*. In May 2009, Health Net discovered that a portable computer disk drive containing unencrypted data was missing from the company's offices in Shelton, Conn. However, it did not inform the affected members or state officials of the loss of the disk drive until November 2009. The data on the disk included protected health information and other personally identifiable information for approximately 1.5 million current and former Health Net members, with Connecticut residents comprising more than one-third of the total number. As part of the settlement, Health Net has agreed to implement a corrective action plan that details the measures it will take to protect health information in accordance with HIPAA. In addition, although Health Net asserts there is no evidence that any Health Net member has suffered any harm as a result of the lost disk drive, the company has agreed to pay Connecticut $500,000 if it is determined that the data on the disk have been accessed and misused and 250 or more individuals file claims of identity theft, thereby linking the data to misuse. (*Connecticut v. Health Net NE Inc.*)

◆ **The Michigan Supreme Court has ruled that *ex parte* communications with physicians are allowed under HIPAA.** On July 13, 2010, the Michigan Supreme Court issued an opinion stating that *ex parte* interviews — informal interviews conducted outside the presence of counsel — of a plaintiff's treating physician by defense counsel are consistent with the regulations implementing HIPAA, provided that reasonable efforts have been made to secure a qualified protective order. Pursuant to 45 C.F.R. § 164.512(e)(1)(v), a "qualified protective order" is an order of the court or stipulation by the parties that (a) prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested, and (b) requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding. Notably, this ruling comes less than two months after a similar opinion by the Georgia Supreme Court. (*Holman v. Rasak*)

"These [new] provisions would allow covered entities to combine authorizations for scenarios that often occur in research studies," HHS says. "For example, a covered entity would be able to combine an authorization permitting the use and disclosure of protected health information associated with a specimen collection for a central repository and authorization permitting use and disclosure of protected health information for clinical research that conditions research-related treatment on the execution of a HIPAA authorization."

HHS asks for "comment on additional methods that would clearly differentiate to the individual the conditioned and unconditioned research activities on the compound authorization," In addition, the agency is looking for feedback on how authorizations and consents could address future research. ✧

This article was excerpted from the July issue of Report on Research Compliance*, which is copublished by AIS and the National Council of University Research Administrators. For more information, go to www.reportonresearchcompliance.com.*

PRIVACY BRIEFS

◆ **Rite Aid Corporation will pay $1 million to settle potential HIPAA violations, according to a July 27 HHS statement.** The Office for Civil Rights (OCR) began investigating Rite Aid after the media televised incidents of its pharmacies disposing of prescriptions and pill bottles — labeled with personally identifiable information — in publicly accessible trash containers. HIPAA requires pharmacies to safeguard private patient information and dispose of it in secure ways. As part of the settlement, Rite Aid must implement corrective actions for three years, including training workforce members, conducting internal monitoring and revising policies and procedures, according to HHS. Rite Aid also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act. Under the consent order, which will be in place for 20 years, Rite Aid agreed to external, independent assessments of its stores' compliance. Cheryl Slavinsky, director of public relations for Rite Aid, says, "When the agency first notified us as of the fall of 2007, of course we immediately cooperated with the request for information and began to review and strengthen the procedures we had in place for protecting the privacy of individuals' information." CVS Caremark Corp. paid $2.5 million in February 2009 in a similar settlement. Go to tinyurl.com/2au5evm to see the HHS statement.

◆ **A professional data management company lost back-up computer files containing personally identifiable information for 800,000 patients, employees and donors at South Shore Hospital in South Weymouth, Mass.** According to the hospital's July 19 announcement, South Shore had hired the company to destroy the files, which contained information — including full names, addresses, Social Security numbers, medical record numbers, diagnoses and treatments — for patients receiving services between Jan. 1, 1996, and Jan. 6, 2010. "Bank account information and credit card numbers for a very small subset of individuals also may have been on the back-up computer files," according to the statement. The data management company hired by the hospital shipped the files off-site for destruction Feb. 26, 2010, but only a portion of the files were received by the outside vendor. "When certificates of destruction were not provided to the hospital in a timely manner, the hospital pressed the data management company for an explanation," the statement notes. The investigation is ongoing, but the hospital says there is no evidence the files have been accessed. Find the statement at www.southshorehospital.org/news.

◆ **A couple making a drop-off at a recycling center in Land O'Lakes, Fla., found a dumpster full of intact medical records,** according to a July 19 article in the *Tampa Tribune*. The records contained individuals' Social Security, drivers' license and credit card numbers. The couple reported the data breach to the Pasco County sheriff's office. The facility owner moved the dumpster to a secured area after she learned about the files. There was no comment on whether the origin of the files has been determined. See the article at tinyurl.com/24p874w.

◆ **The Health Information Trust Alliance (HITRUST) says 50% of hospitals and 70% of health plans with more than 500,000 members are using the HITRUST Common Security Framework (CSF)**, an IT framework designed to help companies boost HIPAA and HITECH compliance. According to the HITRUST statement, the CSF Assurance program is now the most widely used approach in the health care industry for measuring third-party information security. See the statement at www.hitrustalliance.net/news.

If You Don't Already Subscribe to the Newsletter, Here Are Three Easy Ways to Sign Up:

1. Return to any Web page that linked you to this issue

2. Go to the MarketPlace at **www.AISHealth.com** and click on "newsletters."

3. Call Customer Service at 800-521-4323

If You Are a Subscriber And Want to Routinely Forward this PDF Edition of the Newsletter to Others in Your Organization:

Call Customer Service at **800-521-4323** to discuss AIS's very reasonable rates for your on-site distribution of each issue. (Please don't forward these PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)