Report on
PATIENT PRIVACY

Volume 10, Number 9 • September 2010

Practical News and Strategies for Complying With HIPAA

Contents

Many narrative sections at www.AISHIPAA.com *have now been updated to reflect new requirements contained in the HITECH Act, including a recently revised chapter on Business Associates and a brand-new section on Security Breach Notification. If you don't have a website password, call 800-521-4323 or e-mail customerserv@aishealth.com. Please whitelist* aishipaa@aishealth.com *to ensure e-mail delivery.*

Proposed Rules on Electronic Media Push CEs, BAs to Secure 'Materials' and Intranets

The proposed rule implementing portions of the HITECH Act, issued by HHS in the *Federal Register* of July 14, modified and expanded the definition of "electronic media," a change that many covered entities might not have noticed.

As repositories of protected health information (PHI), electronic media are pivotal to compliance. It is therefore essential to know what constitutes electronic media, in all of its many forms, so it can be safeguarded.

Covered entities (CEs) and business associates (BAs) — who are complying with the security rule for the first time — should begin paying extra attention to how they protect their intranets, the private networks where various members of different departments of an organization exchange information. For the first time, HHS has added the word "intranet" to the definition of "electronic media."

"The reason why the change in definition of 'electronic media' is so important is because the HIPAA security rules are based upon the protection of e-PHI," says Lee Kim, an attorney with the law firm of Tucker Arensberg, P.C., in Pittsburgh, whose expertise includes health information technology. "Many significant violations of the HIPAA security rule occur because many organizations do not have appropriate policies, procedures, and documentation in place to comply with the HIPAA security rule."

As is often the case, in the proposed rule HHS offered CEs and BAs little information to judge the practical impact of these changes, and experts *RPP* consulted are calling on the agency to clarify the definition when a final rule is issued, or to offer detailed guidance on implementation.

continued on p. 9

Business Associates Who Act as 'Agents' Create New Liability for Covered Entities

While the HITECH Act made business associates (BAs) directly responsible for following the privacy and security rules, and subjected them to fines for compliance failures as well, a little-noticed provision in the new July 14 proposed rule appears to shift at least some of their liability *back* to covered entities.

This issue is one that most covered entities (CEs) and BAs have never heard of: the so-called "common law of agency." What HHS did in its recent proposed rule was remove an exception in the current regulation that gave CEs a protection if their BAs failed to comply — an exception that would hold up as long as the CE had fully complied and had not ignored a pattern of previous business associate failures.

However, the proposed rule says that if the BA is an "agent" of the CE, the CE is back on the hook. And HIPAA experts are taking strong exception to HHS's contention that the change is appropriate and will have minimal impact.

"This is a problem for everyone — the BA and the CE," says Alan Goldberg, past president of the American Health Lawyers Association and a long-time HIPAA advisor. "I just don't know where they are going with this; I don't know why they had to say

this. I can't tell how this is going to play out. The issue is trying to predict the effects of this. It has made me very, very anxious. I just don't like it."

Adds Kirk Nahra, a partner in the Washington, D.C., law office of Wiley Rein LLP, "This is another opportunity for CEs and BAs to argue and fight," particularly over who is an agent and who isn't.

CEs Are Still Liable for 'Agents'

This provision is just now coming to the attention of some CEs, BAs and HIPAA experts, as they plow through the exhaustive July 14 proposed rule, which amends the HIPAA rules to implement new HITECH provisions. Comments on the proposed rule are being accepted until Sept. 13, and this area is ripe for feedback, they say.

The current regulation at 45 CFR 160.42 (c) states:

"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, acting within the scope of the agency, unless —

(1) The agent is a business associate of the covered entity;

(2) The covered entity has complied, with respect to such business associate, with the applicable requirements of §§164.308(b) and §164.502(e) of this subchapter; and

(3) The covered entity did not—

(i) Know of a pattern of activity or practice of the business associate, and

(ii) Fail to act as required by §§164.314(a)(1)(ii) and 164.504(e)(1)(ii) of this subchapter, as applicable."

The new proposed rule states that, related to a 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."

The current exception is apparently no longer appropriate, as HHS states: "We propose to remove this exception to principal liability for the covered entity so that the covered entity remains liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place. This change is necessary to ensure, where the covered entity has contracted out a particular obligation under the HIPAA rules, such as the requirement to provide individuals with a notice of privacy practices, that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf."

Provision Prompts Huge Questions

According to HHS, covered entities and business associates shouldn't view this as a big deal. "We do not believe this proposed change would place any undue burden on covered entities, since covered entities are customarily liable for the acts of their agents under agency common law," the proposed rule states.

That's hogwash, says Goldberg. "I am not sure they *are* 'customarily liable,'" he says. "And what if a state attorney general is involved? Is there state common law vs. federal law that might be applicable? And any time the government says to me there's 'no burden,' you can bet there is."

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@aishealth.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.

"What I see HHS doing here is creating new categories of entities that it had not looked at before," says Heidi Salow, an attorney with DLA Piper LLP's communications, e-commerce and privacy practice group in Washington, D.C. "In the past we had CEs and BAs, and it was black and white. But now we have CEs, BAs, agents and subcontractors." (For a story on subcontractors under the proposed rule, see *RPP 8/10, p. 4.*)

CEs should begin to review their existing BA relationships to assess whether they think the BA is an agent or not, Salow tells *RPP.* And business associates should be doing the same thing.

One problem, however, is the murkiness of the agency issue. Goldberg and Nahra contend there's no real test of who is an agent and who isn't.

BAs Are 'Pulling Their Hair Out'

The proposed rule provides little guidance, stating only: "The determination of whether a business associate is an agent of a covered entity, or whether a subcontractor is an agent of a business associate, will be based on the facts of the relationship, such as the level of control over the business associate's or subcontractor's conduct."

Even if the BA agreement said the BA *wasn't* an agent, in the event of an investigation the BA might try to argue it really was acting as an agent of the CE, if it relied on information and direction from the covered entity, Nahra says.

As Goldberg puts it: "Agency is easy to allege and hard to defend against."

A CE entering into a BA agreement is "going to want to structure the contract so that the BA is acting on your behalf as an independent contractor, not an agent," says Salow. And if the BA is initiating the contract, it might want to insist that it is acting as agent, she says.

When asked whether CEs and BAs could rewrite their BA agreements to address this issue of agency, the experts offered a qualified "yes." Nahra and Goldberg both say that regardless of what an agreement actually says, HHS's final interpretation would determine the accuracy of whether the BA is an agent or not.

As Goldberg says, "the facts and circumstances" are central to such a determination, not the words.

Salow says that CEs can expect some push-back from BAs that want to be labeled an agent to reduce some of their liability.

"The BA is not coming out ahead on any of this," says Salow. "I get calls from BAs all the time that are pulling their hair out." Some handle PHI as only a small part of their business, and are now facing huge compliance costs and demands from CEs.

In fact, Nahra says the proposed provision appears to increase the CE's exposure, but is also unlikely to reduce the BA's. "The government can clearly go after the BA. This does not lessen or replace that," he says. He speculates that perhaps HHS is simply confirming that it can tap any deep pockets it wants in a HIPAA prosecution.

Goldberg worries that, particularly with the agency issue looming, BAs, as well as CEs, may simply cave if accused by the government, even when innocent. "There is an inclination to settle," he says.

Linda Mendel, an attorney with Vorys, Sater, Seymour & Peace LLP in Columbus, Ohio, notes that HHS has even flowed the agent discussion down to BAs, saying they, too, might have their own agents, for whom they are liable.

The biggest danger from the CE perspective is lack of knowledge on the part of BAs that they are agents. "The issue for health plans [and other CEs] is that some of our vendors probably are agents — even if agency is disclaimed in our contracts," Mendel says.

Salow says that, "without a doubt," HHS needs to provide "concrete examples as to how these different relationships would work." In addition, CEs and BAs are going to have to "figure out what common law of agency means," Nahra says.

Investigate HIPAA Insurance

Goldberg agrees, and has drawn several other conclusions from the proposed provision and the proposed rulemaking itself.

"I am telling people they have to be more involved and more diligent than ever," he says. Specifically, CEs and BAs are going to need to consult their attorneys a lot more often, now that the stakes have been raised so high. He also says training the workforce cannot be stressed enough.

But finally, Goldberg says, CEs and BAs should investigate purchasing HIPAA liability insurance. Special policies are available that would pay for legal representation as well as penalties, he says. These policies vary, of course, and all have exclusions, deductibles and other features that mean they must be carefully scrutinized.

"A general liability policy doesn't cover data breaches and the like," Goldberg says. "Even if it is alleged that you did something wrong, you have to defend against that."

Contact Goldberg at Alan@GoldbergLawyer.com, KNarha@wileyrein.com and Salow at Heidi.Salow@dlapiper.com. ✧

Rule Clarifies Enforcement Issues But Raises a Host of New Questions

For many years, HIPAA enforcement consisted of a slap on the wrist for covered entities (CEs). But passage of the HITECH Act, which imposed direct liability on business associates (BAs) and introduced stronger civil monetary penalties through a tiered system, marked a push for accountability — and a much more perilous environment for CEs and BAs.

The July 14 proposed rule highlights HHS's enforcement power by obligating the HHS secretary to investigate certain complaints and allowing her to share information with state attorneys general. Experts agree that the examples provided in the proposed rule are more informative than the changes themselves, but there is debate as to whether those examples tighten or loosen the noose on covered entities and business associates.

Under the interim final enforcement rule, HIPAA violations due to "willful neglect" receive the most severe penalties — at least $50,000 per violation. The original enforcement rule defines "willful neglect" as "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated." The lowest tier of penalties goes to violators who "did not know" they violated the law.

The proposed rule leaves the tiered penalties intact (see box below) but modifies and clarifies some important terms and requirements:

◆ ***The term "business associates" is added everywhere.*** The rule proposes adding references to business associates throughout the HIPAA enforcement rule, since BAs are now directly liable for privacy and security violations and subject to the penalties. It lists more than a dozen sections in which to add "the term 'business associate' where appropriate, following a reference to 'covered entity.'" Robert Coffield, an attorney with Flaherty, Sensabaugh & Bonasso, PLLC, in Charleston, W. Va., says this "shows they're not just going to come after hospitals and doctors anymore. They're going to come after you as a BA."

◆ ***The HHS secretary "will" (not "may") investigate complaints.*** Currently, the HIPAA enforcement rule states that the secretary "may" investigate HIPAA complaints. The new rule proposes altering the language to say that the secretary "will" investigate complaints "when a preliminary review of the facts indicates a possible violation due to willful neglect."

HHS notes in the rule that it already "conducts a preliminary review of every complaint received" and investigates when the facts indicate willful neglect. Elizabeth Callahan-Morris, a Troy, Mich.-based attorney for Hall, Render, Killian, Heath & Lyman, PLLC, says "I don't see that as a change and I don't think HHS sees that as a change in how they're going to go about their reviews. They're just making it a formal requirement."

Coffield says this new language should not be overlooked. "Prior to this there was discretion to investigate," he explains. "This rule indicates this was done to stress Congress' desire to have increased enforcement in these egregious cases of breach/violation."

◆ ***HHS secretary's duty to investigate is clarified.*** In accordance with the above change, HHS proposes to "distinguish the Secretary's discretion with respect to complaints for which HHS's preliminary review of the facts does not indicate a possible violation due to willful

Greater Penalties Add Significant Risk for CEs and BAs

Previous civil penalties under HIPAA — which were rarely imposed — consisted of $100 fines per violation with a $25,000 yearly cap on identical violations *(RPP 4/09, p. 10)*.The interim final rule regarding HIPAA enforcement, published in the *Federal Register* on Oct. 30, 2009, incorporated four tiered ranges of penalty amounts as outlined in the HITECH Act. The new penalties apply to violations occurring since Feb. 17, 2009.

The rule categorized violations to "reflect increasing levels of culpability" and added teeth to the fines, as follows:

◆ ***First tier: If the violator did not know*** that he or she violated the law, and would not have known by exercising due diligence, the penalty for an identical violation is at least $100 and up to $50,000 for each violation.

◆ ***Second tier: If the violation was due to reasonable cause***, not willful neglect, the penalty is at least $1,000 and up to $50,000 for each violation.

◆ ***Third tier: If the violation was due to willful neglect and was corrected within 30 days*** of when the CE knew or should have known about it, the penalty is at least $10,000 and up to $50,000 for each violation.

◆***Fourth tier: If the violation was due to willful neglect and was not corrected***, the penalty is at least $50,000 for each violation.

For all tiers, the maximum penalty amount for violations of an identical provision is $1.5 million per calendar year.

neglect from the statutory requirement to investigate *all* complaints for which HHS's preliminary review of the facts indicates a possible violation due to willful neglect." Coffield says HHS included this language to clarify that the secretary is bound by Congress to investigate when willful neglect is involved, but can choose whether to investigate in other cases.

◆ ***Compliance reviews are required for willful neglect, even in the absence of complaints.*** The proposed rule requires the secretary to conduct a compliance review "when a preliminary review of the facts indicates a possible violation due to willful neglect." The previous rule mentioned only "complaints." Under this change, the secretary could initiate a compliance review even in the absence of a complaint, if facts indicating willful neglect come to light.

◆ ***HHS can disclose PHI to state AGs.*** According to the proposed rule, HHS can disclose protected health information, as permitted by the federal Privacy Act. This would allow the secretary to cooperate with state attorneys general, who can now pursue HIPAA enforcement on behalf of state residents under the HITECH Act.

◆ ***"Informal" resolution is no longer required if willful neglect exists.*** In another clarification, the proposed rule states that HHS is no longer "required to attempt to resolve cases of noncompliance due to willful neglect by informal means," which means the agency may in such cases take a more direct route to formal legal action. This language would continue to permit HHS to resolve complaints through informal means when they do not involve willful neglect.

Coffield explains that informal means is what HHS has historically used to address complaints. "Under the original privacy rule, HHS would investigate it and be very accommodating in suggesting you make changes to whatever the violation was — without any penalties, without teeth of enforcement," he says. "What this does is do away with that."

◆ ***The nature and extent of the harm must be considered.*** The rule also proposes to explicitly state that HHS must consider "the nature and extent of the violation" and "the nature and extent of the harm resulting from the violation," when determining a civil money penalty amount. According to the proposed rule, this would take into account "the time period during which the violation(s) occurred" and "the number of individuals affected."

◆ ***Harm to reputation is now a factor to consider.*** HHS also proposes adding reputational harm as a specific factor the secretary can choose to consider, "to make clear that reputational harm is as cognizable a form of harm as physical or financial harm." Harley Geiger, policy counsel with the Center for Democracy & Technology (CDT), says HHS does so "to demonstrate that the agency considers it on par with the other types of harm."

According to Geiger, CEs and BAs "may be somewhat troubled by the use of the term 'reputational harm' in the penalty factors because that term is not defined in the NPRM [i.e., notice of proposed rulemaking]." He says HHS is likely to receive comments on this piece of the rule.

◆ ***"Reasonable cause" is redefined.*** Though the penalty structure remains the same, the rule proposes modifying the definition of "reasonable cause." The current definition is "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." The proposed rule defines it as "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." The new definition broadens the scope of the reasonable cause category by including violations about which the CE or BA has knowledge but "lacks the conscious intent or reckless indifference associated with the willful neglect category."

The rule offers an example to explain the significance of this new definition. It poses the scenario that a covered entity received an individual's request for access but failed to respond within the required time period. The CE has appropriate policies and procedures in place, but had received an "unusually high volume of requests for access within the time period in question." The CE responded to most of the requests in a timely manner. According to the rule, this would constitute a second-tier violation due to "reasonable cause" — just above the lowest penalty for "did not know."

Examples May Highlight OCR's Priorities

Experts agree that none of these changes was shocking. Geiger says "they appear to be logical extensions of HITECH and consistent with congressional intent." According to Annulis, "It wasn't so much that they departed significantly from the plain language of the HITECH Act — we still have four categories now of violations and the attendant penalties." But he says the interpretation and application of those tiers — found in the examples — are what's new.

Callahan-Morris says the examples are "quite telling in terms of what types of situations OCR is going to make a priority." For instance, she says, there's "continued focus throughout the examples of a CE or BA not having any policies or procedures on a particular require-

ment. It appears they're going to make that a priority for enforcement action."

One example regarding restrictions of uses and disclosures of PHI has caused some discussion in the industry, she says. The scenario posed is that a CE failed to respond to an individual's request for restrictions. The CE does not have policies and procedures for considering restriction requests and refuses to accept such requests from patients who inquire. The violation would be deemed willful neglect, according to the rule.

Some Changes Are Surprising, 'Misplaced'

But covered entities do not have to grant such requests at all, says Callahan-Morris, save for the HITECH Act exception for individuals who pay for services out-of-pocket and request that a claim not be submitted to their health plan. "The fact that they chose to make that an example surprised me — first, that they would include it, and second, that they would put it under willful neglect," she says. The example "seems to be misplaced," she contends, especially given that "so many more examples of egregious violations could have been chosen." For instance, she says, "if a covered entity fails to give a copy of a designated record set, to me that's a more egregious violation than failing to respond to a request for restrictions you're not obligated to grant."

While the examples didn't change the definition of willful neglect, Callahan-Morris asserts, "based on the examples given, we may see a lower threshold for what could be considered willful neglect."

In contrast, Brian Annulis, attorney with Meade & Roach in Chicago, says that some of the examples HHS gives are "great for covered entities." He points to one in which a hospital employee accessed his ex-spouse's paper medical record to discover her current address, knowing that it was against the hospital's policies and procedures. The rule calls it an example of the "did not know" category.

"I always thought under that scenario you'd still be in a situation where [HHS] would be more stringent," says Annulis. "I think it's a positive thing for CEs. The takeaway is if you do what you're supposed to do — have policies and procedures, train employees — and if employees act contrary to that, it's not like a 'get out of jail free card,' but it will fall into the lowest category of violations."

The "did not know" category has been the most puzzling one from the start, says Annulis. "When I first read the HITECH Act and the enforcement rule that was published, I was hard-pressed to come up with a single example where a covered entity would be able to take advantage of that [lowest penalty tier]," he says. "I thought, 'What scenario could exist whereby exercising reasonable diligence a CE would not have known?'" He claims he's not entirely clear why the example in which the hospital employee acted inappropriately would fall under the first tier, yet the example about failure to provide timely request for access would be a second-tier violation, but he adds that CEs should "not look a gift horse in the mouth."

Coffield says he's hoping HHS will publish a concrete list of 20 or so actions that will fall under the willful neglect category, to clear up remaining ambiguity. "Otherwise," he says, "they have wide discretion in interpreting the willful neglect language.… At some point, I think they will [publish a list]. They have to put some procedures in place for themselves."

To review the full text of examples included in HHS's proposed rule, go to www.aishealth.com/Compliance/HIPAAResource.html, click on HITECH Act Proposed Regulation, and go to pages 40878 and 40879. Contact Annulis at (773) 907-8343 or bannulis@meadero-ach.com, Callahan-Morris at (248) 457-7854 or ecallahan@hallrender.com, Coffield at (304) 347-3791 and Geiger at (202) 407-8825 or harley@cdt.org. ✧

Variations Among State, Federal Breach Rules Complicate Compliance

One stolen laptop is causing a lot of breach-notification grief for a national provider, but not in the usual way — at least not yet. Because the laptop contained information about patients in 25 states, the provider has to analyze the breach under every state breach notification law as well as the HITECH Act to determine how to inform its patients that their personal information may have been compromised.

If the patient information — PHI, Social Security numbers, etc. — were encrypted, breach notification wouldn't be necessary. But it wasn't, so the provider is creating a big matrix of every state's breach law requirements and comparing them to federal law. Then a determination will be made about whether the provider is bound by the breach reporting obligations of each individual state versus the HITECH ACT.

That's the challenge covered entities (CEs) face as they assimilate their state breach notification laws with the HITECH Act's breach notification provision. "The bigger the breach in terms of the numbers of states, the more important it is to make sure you focus on the way all these requirements interact," says attorney Brad Rostolsky. "You can't approach breaches off the cuff. You need to be organized and diligent and work in close connection with your IT and public relations folks. Everyone needs to be on same team so you can get these things done in a timely fashion and comply with all your obligations."

Even hospitals located in a single state may have to consider the breach reporting requirements of multiple states because they may treat patients from bordering states. If there's a breach, the reporting law of the state where the patient lives is implicated, he says. For example, it's common for people who live in the Washington, D.C., metro area to see providers in D.C., Maryland and/or Virginia, so a Virginia hospital has to be attuned to breach notification laws in all three jurisdictions.

Like other HIPAA and HITECH provisions, the breach notification requirement is a baseline. "The federal law acts as a floor," he notes, and "the state rule must bow down to the federal if following the state law would make it impossible to comply with the federal requirements." However, when states have stricter requirements, both state and federal laws must be followed, says Rostolsky, with Reed Smith in Philadelphia.

All states in the nation have security breach notification laws except Alabama, Kentucky, New Mexico and South Dakota, according to the National Conference of State Legislatures. These laws keep rolling in. Mississippi — the most recent state to jump on the breach-notification bandwagon — enacted a law in April. "The HITECH security breach regulations generally incorporate key concepts and best practices from the state security breach notification laws, but with greater detail," notes attorney Reece Hirsch.

The laws vary. For example, there's some variation in the data elements that trigger breach notification in the event of improper use or disclosure. Rostolsky says "prototypical triggers" are name plus one of the following: Social Security number, driver's license number/state identification number or banking information.

Notice Is Triggered Differently Across the U.S.

Additional triggers exist in 22 states, he says. In Texas, for example, the law requires notification for "unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data." The definition of "data" extends to name plus medical information, in addition to the usual suspects, Rostolsky says.

California is in a league of its own. "There is more than just one California law" on breach notification, says Scott Morgan, national privacy and security compliance officer for Kaiser Permanente. Under one law, breach notification is required if "unencrypted personal information" is "acquired by an unauthorized person in an unauthorized manner," Morgan says. The personal information is the first name in combination with the last name, account number and Social Security number, Morgan says. The law was later modified to add medical and health information to the data elements that trigger breach reporting, he says.

A second California law was enacted in the wake of a number of celebrity snooping incidents at hospitals. It's targeted at licensed health facilities, requiring them to notify affected people and regulators when there has been unauthorized access to medical records.

Here are a few examples of additional data elements that trigger breach notification if compromised in these states:

- ***Georgia:*** A customer/patient's name is not needed to activate the breach notification law if the infiltrator obtains other information sufficient to attempt identity theft, Rostolsky says.
- ***Oregon:*** A passport number is an additional trigger.
- ***Wyoming:*** Tribal identification number.
- ***Arkansas:*** Medical information.
- ***Washington, D.C.:*** A phone number or address can substitute for a name.

'Harm' Not Always Required for Reporting

But breach of the data elements doesn't always mean reporting is required. There are two different types of states: (1) technical-breach states, such as California, Texas and Illinois, where a breach must be reported to patients or customers regardless of the impact on them; and (2) states where reporting is required only if the organization determines the breach could cause harm to affected patients or customers.

The latter category is similar to the harm standard in the HITECH Act and interim final rules that became effective one year ago, which require breach reporting if the privacy or security of the information is compromised *and* the CE determines there is significant risk of financial, reputational or other harm. But it is worth noting that HHS's July 29 withdrawal of final breach notice rules may involve a brouhaha related to the harm standard (see *RPP 08/10, p. 1*).

The new law in Mississippi, for example, is a risk-of-harm state, which does not require patient or customer notification if the breach probably will not result in harm to affected individuals.

"In states where there is no harm standard, the state is generally more stringent. You have to report no matter what," Morgan says. Anytime Kaiser has a problem in the states where it operates — California, Hawaii, Oregon, Washington, Colorado, Ohio, Georgia, Maryland, Virginia and D.C. — "you have to review where it occurred and what the prevailing laws are" and make

a notification decision based on the state and federal breach notification requirements, he says.

In states with a harm standard, the decision to report may come easily, Rostolsky says. If, for example, a hacker got hold of patients' or customers' first names and Social Security numbers, "it's pretty clear there is potential for financial harm. An identity thief could do something with first name and Social Security number," he says. However, suppose a covered entity has a potential breach involving the names and health information of 50,000 people. "This is onerous, but you'd need to determine for each of these people whether there is significant risk of harm," which obviously triggers the breach notification requirement.

For example, if the health information relates to HIV infection or mental health treatment, it's a no-brainer there's harm and patients must be notified, with HITECH taking precedence over state laws. But if "it's something seemingly more innocuous" — a patient's name and blood pressure — then notification likely won't be necessary, Rostolsky says. If it falls into a grayer area — the patient's name and the fact he had a stent placement — the covered entity has to decide whether notification is mandatory. "It's not always an easy decision to make," he says.

OCR Can Come Back and Bite You

Be careful, though, if you decide there's no significant risk of harm and a year later there is a breach warranting notification. If the Office for Civil Rights conducts an audit of your covered entity in response to the new breach and asks "so, nothing like this has ever happened before?" Rostolsky says, obviously "you will have to be honest and tell them about the earlier incident." OCR might require an explanation for why there was no notification in that case, and "you need to be able to show them why. You need a file documenting all your decisions." He recommends maintaining two sets of files: the "warts-and-all" file that's protected by attorney-client privilege, and a second file for OCR, which would include a chronology of events, IT determinations, the documentation surrounding the decision to hire an IT consultant to conduct an independent review to determine if PHI was unduly accessible, the consultant's determination that it wasn't and the final report on the matter. "You never know when you may need to show compliance," Rostolsky says.

Another complication in the state versus federal analysis is the content of the notification. The HITECH Act breach notification regulation says the content of the notification must include:

◆ A brief description of what transpired and the kind of unsecured PHI that was breached (e.g., name, SSN, address, diagnosis);

◆ The steps that affected people should take to protect themselves from harm the breach could cause;

◆ A description of actions the covered entity is taking to investigate the breach, mitigate harm to people and prevent additional breaches; and

◆ Contact procedures for follow-up questions or more information (e.g., website, toll-free phone number, e-mail address).

Content of Breach Letters Varies Widely

State laws vary on the content of breach notification letters. Some are pretty silent about what letters must include, while others are more prescriptive. Here is a small sampling:

◆ ***Maryland:*** Notification letters must explain the type of information involved in the breach; provide a business address and phone number; give a phone number for consumer reporting agencies, the FTC and the state attorney general; and explain to the patient/customer that they can obtain resources that will help avoid being a victim of identity theft.

◆ ***Puerto Rico:*** Notification letters must describe the number of people affected by the breach, estimate the time and money invested to mitigate the problem and whether criminal charges were filed.

◆ ***New Hampshire:*** Notification letters must describe the information breached, the date of the breach and a company contact.

◆ ***Vermont:*** Notification letters must explain the information that was breached and what the company is doing to fix the breach, provide a toll-free number for help and advise vigilance through monitoring of credit reports and financial accounts.

Even without these content requirements, if certain categories of sensitive information aren't part of the breach (e.g., SSNs), "it's prudent to indicate that as well," Rostolsky says.

The federal law and the states also differ with regard to the recipients of notifications, in addition to affected people. The HITECH Act requires covered entities to notify HHS and at least two prominent media outlets if the breach affects 500 or more people, and breaches involving fewer than 500 people must be put in a log that's submitted to HHS at year's end.

States have other things in mind, Rostolsky says. For example:

◆ ***Florida:*** If more than 1,000 residents are affected by the breach, entities must notify consumer reporting agencies.

◆ ***Maryland:*** If more than 1,000 residents are affected, entities must contact consumer reporting agencies and the

attorney general, who must approve breach-notification letters before they are sent to residents.

◆ ***Georgia:*** If more than 10,000 residents are affected, covered entities also must notify consumer reporting agencies.

◆ ***Hawaii:*** If more than 1,000 residents are affected, covered entities must notify consumer reporting agencies and the state Office of Consumer Protection.

◆ ***Louisiana:*** Breaches must be reported to the state AG.

State laws and HITECH breach notification provisions differ in other ways, says Hirsch, with Morgan, Lewis & Bockius in San Francisco. For example, media breach notification is not a popular state mandate, he says. And "most state breach notification laws allow you to delay sending notification when sending it would compromise an investigation, but HITECH is more detailed," Hirsch says.

HITECH also provides an absolute timing requirement for breaches: Covered entities must notify affected people without unreasonable delay but no later than 60 days. That's more detailed than most state laws in terms of the deadlines for sending notification letters, Hirsch says. Most states don't provide a drop-dead deadline. A few states, however, do have time frames (e.g., Florida, Ohio and Wisconsin set 45-day breach notification deadlines). When a breach implicates both state and federal laws, you must notify patients or customers by the earlier deadline, Rostolsky says.

Contact Rostolsky at brostolsky@reedsmith.com, Morgan at scott.morgan@kp.org and Hirsch at rhirsch@morganlewis.com. ✧

New e-Media Rules = New Risks

continued from p. 1

As a result of the expansion of the definition of "electronic media," Kim points out that "CEs and BAs will need to ensure all storage material is included in the required risk assessment," the analysis that must be done to determine appropriate security measures.

To John Parmigiani, a HIPAA consultant and author of the government's proposed security rule, the revised definition is more of a refinement that he termed "both appropriate and overdue."

In the proposed rule, HHS explains that it needed to revise the definition of "electronic media" because the 2003 version was outdated.

In part, the current definition says electronic media is: "electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.…"

The new proposed definition states that electronic media is "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…."

HHS says it is changing the definition, which has two parts, to reflect current usage, as set forth in Guidelines for Media Sanitization, issued by the National Institutes of Standards and Technology. This change recognizes the fact that other devices not considered "media" can house electronic data, Kim says.

Indeed, "the common understanding we have today of data storage material/media may not be the storage media/material of the future," Kim says.

Intranet Data Are Now Included

The proposed second part of the definition now has the word "intranet" among its examples. It reads that electronic media, in addition to the first paragraph, is defined as "transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet or intranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media." (The final sentence in the definition is discussed below.)

Parmigiani, president of Parmigiani & Associates, LLC, an information security consulting firm in Maryland, called the specific inclusion of intranet "not necessarily a big expansion," but reflective of "more granularity as to what are possible mechanisms for being the source and conduits of e-PHI in health care organizations."

He says organizations should already have been protecting their intranets under the requirement to ensure that employees follow access policies, which should have had attendant sanctions for violations.

The changes in the definition are a refinement to bring the government in line with "what the industry, in reality, has become increasingly aware of; namely, if the data are digitized and represent PHI, they must have safeguards in place to protect them from unauthorized access, use, and disclosure," he said.

An intranet can be protected with "access controls, requiring authentication, authorization, and auditing-monitoring and follow-up — through policies, administrative and technical controls and content filtering," Parmigiani says.

continued

Another security expert has a question on including "intranet" in the definition of "electronic transmission media." Kamal Govindaswamy, principal of Risk Compliance Consulting Group, thinks that HHS should clarify its intent behind the inclusion.

Govindaswamy says HHS needs to clarify in guidance or in the final rule whether the agency likes to see intranets having the same transmission safeguards as those of extranets or the Internet; after all, an intranet, by definition, is a private computer network with restricted access from the Internet or to outside parties.

The security rule requires CEs and BAs to conduct periodic risk analysis in order to ascertain the risk levels and then implement appropriate safeguards depending on the risk level. Govindaswamy says some instances would clearly need better safeguards than others.

For example, a hospital may allow physicians who are not a part of its workforce in an offsite location access to its intranet for certain business reasons. A risk analysis would probably reveal the need for stronger safeguards on such access to the intranet.

"Does this mean that if PHI were to be transferred between the pediatrics and radiology departments of a hospital, that has to be encrypted just as you would encrypt PHI transmission between the physician practice and the hospital? If you had a malicious insider or malware on the intranet, there is certainly a risk that unencrypted PHI in transmission may be compromised, but the risk level is not quite the same as that associated with transmitting unencrypted PHI on the Internet or extranet," Govindaswamy says.

One Exception Is Clarified

A third change is sure to have privacy compliance officers huddling with their security counterparts. The last sentence in the second part of the proposed definition reads, "Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media ***if*** [emphasis added] the information being exchanged did not exist in electronic form before the transmission."

The current regulation uses the word "because" in place of "if." As the proposed rule states, the current 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."

HHS says the word substitution has the effect of extending "the policy" and "correct[s] its application to current technology, where some voice technology is digitally produced from an information system and transmitted by phone."

To understand the definition of "electronic media," it is important to view the two parts of the definition together. As Kim describes, "in the first sense, electronic storage media involves PHI which stays 'at rest.' However, the second sense of electronic storage media — per the second half of the definition — involves data 'in motion' by way of 'transmission media.'" Transmission media, Kim notes, "may be thought of as the conduit for transmitting electronic information."

New Policies, Retraining May Be Required

Kim offers another word of caution: "As types of 'storage material' evolve, so will the conduits that we know as 'transmission media.' In the true sense of the word, electronic storage media are any electronic devices used to store data, hard drives, USB/thumb drives, etc.," she says.

"However, even storage media as we know it today are other than 'electronic,'" she says. Floppy drives and tapes are magnetic storage media, Kim notes. She also notes that "DVDs, Blu-Ray discs, CDs, etc. are types of optical storage media."

The message for CEs and BAs, says Kim, is if your risk assessment just stopped at electronic "media," you'll have to go back and include all "materials," assuming the proposed rule becomes final as drafted.

"The procedural steps for a risk analysis typically include defining the e-PHI that the entity has or may come into contact with, identifying security threats and vulnerabilities, for example, malware, open ports, etc., and conducting a security impact analysis, examining whether new or modified security safeguards and procedures beyond what is already in place should be established based upon information such as security logs, security incident tracking, etc.," Kim says.

Following the assessment, recommendations would be made for security controls, and the whole process would be documented, she adds.

"Privacy and security people need to realize there are all kinds of things that can store data whether they are portable or not, and the best practices include some really strong encryption so that no one unauthorized gets a hold of it, or can't crack the code to access the confidential information," says Kim.

If policies are changed to comply with the new definition, re-training may be a good idea. For some, however, it wouldn't be *re*-training. "In terms of the climate I am seeing, there are a lot of BAs and CEs that haven't even gotten to the initial level of training, or comprehensive training," she says.

Contact Kim at lkim@tuckerlaw.com, Parmigiani at jcparmigiani@comcast.net and Govindaswamy at kamal@rnc2.com. ✧

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.*

◆ **A federal district court allowed a hospital to pursue claims against a contractor under the computer fraud and abuse laws.** On July 28, 2010, the U.S. District Court for the District of New Hampshire determined that two pathologists — owners and employees of a pathology practice group that provided professional services to Wentworth-Douglass Hospital under a series of contracts — were not entitled to a dismissal of the claims brought against them by the hospital under the Computer Fraud and Abuse Act (CFAA) (18 U.S.C. § 1030). The CFAA provides a private right of action for compensatory damages and equitable relief to any person who suffers damage or loss because another "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains…information from any protected computer." In late 2009, the hospital informed the defendants that their contracts, scheduled to expire on Feb. 28, 2010, would not be renewed. The hospital alleges that between Feb. 1 and Feb. 28, 2010, the defendants downloaded electronic data — including specimen/slide photos; autopsy images; individual employee subfolders; patient charts; documents, templates, and forms used by the pathology department to process specimens; and records relating to complaints against the defendants — from the hospital's computer network, using two desktop computers, one laptop computer in the hospital's pathology department and a removable storage device. Wentworth-Douglass further alleges that on Feb. 28, 2010, the defendants installed software on the pathology department's computers that deleted data from the hard drives of those computers and from the hospital's network, and that as a result of this action, the hospital and its employees were unable to access the data stored on the network for approximately one week. The hospital's theory is that the defendants' actions implicate the CFAA because the defendants obtained information from the hospital's computers in a manner that exceeded their authorized access, as the hospital policy prohibited them from connecting external hardware to its computers. The defendants argue, in part, that their right of access to the hospital's computer is governed by their contract with the hospital, not by hospital policy, and that they had a right to access the data on the computers and the network. The court, however, refused to dismiss the case, reasoning that even individuals with the authority to access a computer can violate the CFAA. (*Wentworth-Douglass Hosp. v. Young & Novis Professional Association*)

◆ **The U.S. Court of Appeals for the First Circuit ruled that a Maine law protecting prescribers' data privacy is constitutional.** On Aug. 4, 2010, the appeals court issued an opinion stating that 22 Me. Rev. Stat. Ann. tit. 22, § 1711-E(2-A) is constitutional, thereby reversing a 2007 trial court ruling. Section 1711-E(2-A) allows physicians and other prescribers licensed in Maine to choose not to make prescribing data — that is, information regarding a physician's prescribing habits, including choice of particular brand-name drugs versus their generic equivalents — available to companies that collect and aggregate such data for use in marketing prescription drugs. The statute does not directly prohibit any marketing practices, but rather, prohibits certain entities from licensing, using, selling, transferring or exchanging this information for a marketing purpose if the prescriber has opted to protect the confidentiality of his or her prescribing data. The plaintiffs contended, in part, that the restrictions provided by the statute were an unconstitutional limit on protected speech under the First Amendment. The plaintiffs also argued that the restrictions were unconstitutionally vague and overbroad under the First and Fourteenth Amendments. The First Circuit rejected all of the plaintiffs' constitutional challenges, finding that the statute regulates conduct, not speech. The court also stated that even if the statute were to regulate speech, such regulation would satisfy constitutional standards. Section 1711-E(2-A) was enacted in 2008 but has never been implemented, due to a preliminary injunction issued by the trial court. The First Circuit rejected the plaintiffs' claim that the court should leave the injunction in place and remanded the case for further proceedings. (*IMS Health Inc. v. Mills*)

PRIVACY BRIEFS

◆ **Connecticut Attorney General Richard Blumenthal (D) announced Aug. 18 he is investigating a data breach at Yale School of Medicine that may have affected as many as 1,000 individuals.** According to a statement from the AG's office, the school reported the theft of a laptop containing personal health information. Blumenthal is looking into whether state or federal laws have been violated and is seeking privacy protections for affected individuals. In an e-mail response, Yale told *RPP* that the computer did not contain Social Security, financial or insurance numbers. "The computer was owned by Yale and stolen from the office of a data analyst at the Yale School of Medicine," the university stated. "While access to the stolen laptop was protected by a password, the laptop was not encrypted." The school said it is notifying affected individuals by mail. See the AG's statement at http://tinyurl.com/2wrbd7q.

◆ **A *Boston Globe* photographer found thousands of intact patient records from four Massachusetts community hospitals at a dump, reports the Globe.** The files, which contained patients' names, medical diagnoses and Social Security numbers, came from Milford Hospital, Holyoke Medical Center, Caritas Carney Hospital and Milton Hospital. According to the Globe, executives at two of the hospitals said a medical billing company used by their pathologists had the records dumped at the Georgetown Transfer Station. The Massachusetts AG is reviewing whether a breach occurred. See the article at http://tinyurl.com/2cmquyt.

◆ **Privacy watchdog Patient Privacy Rights released a white paper contending that patients should have control over their personal health information and that health information technology can enable that to happen.** The 21-page document, "The Case for Informed Consent: Why it is Critical to Honor What Patients Expect — For Health Care, Health IT and Privacy," says that a majority of Americans believes their medical data should not be shared without their permission. It argues for the creation of "patient-centric" IT systems, which clinicians, rather than patients, need permission to access. The paper states that consent technologies can lower costs and simplify data exchange. See the white paper at http://tinyurl.com/339vkh3.

◆ **The Massachusetts Supreme Judicial Court ruled Sept. 2 that patient privacy laws prohibit a medical board from subpoenaing the confidential records of a psychotherapist for a physician misconduct investigation,** reports the *Boston Herald*. In 2007, a doctor reported a psychotherapist to the Board of Registration in Medicine for allegedly prescribing pain medication improperly. The board subpoenaed the psychotherapist's records, but the physician refused to turn them over citing patient privacy laws. The court sided with the physician, rejecting the board's assertion that the investigation into misconduct was a valid exception to state privacy laws, according to the newspaper. The court also rejected the board's argument that the psychotherapist should not be considered a psychotherapist because he specializes in pain management. See the article at http://tinyurl.com/37xzybe.

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.)