Report on
PATIENT PRIVACY

Volume 9, Number 12 • December 2009

Practical News and Strategies for Complying With HIPAA

Contents

Go to www.AISHealth.com *for summaries of the latest House and Senate health reform bills.*

Five narrative sections at www.AISHIPAA.com *have now been updated to reflect new requirements contained in the HITECH Act, and a brand-new section on Security Breach Notification has been added. If you don't have a Web site password, call 800-521-4323 or e-mail customerserv@aispub.com. Please whitelist* aishipaa@aispub.com *to ensure e-mail delivery.*

Two Breaches Give State Attorneys General A Chance to Exercise New HIPAA Powers

In a sign that state attorneys general may be flexing the HIPAA enforcement muscle granted by the HITECH Act provisions in the Recovery Act, the Connecticut and Arizona attorneys general are investigating health plans that recently experienced data breaches that they failed to disclose for several months.

Typically, state attorneys general prosecute only violations of state laws, but they now have authority to investigate and levy fines for violations of HIPAA and the HITECH Act, which requires mandatory notifications within two months of knowledge of a breach *(RPP 4/09, p. 1).*

Connecticut Attorney General Richard Blumenthal (D) has emerged as possibly the first AG to take on a HIPAA investigation, and Arizona's AG may also be pursuing a similar course. The larger of the two breaches that have come to the AGs' attention was experienced by Health Net, Inc., which lost a portable external hard drive containing seven years of data for 446,000 Connecticut residents. The lost data came from 1.5 million individuals in total, who also hailed from New Jersey and New York.

Health Net reported the loss to the Connecticut AG on Nov. 19, and on the same day Blumenthal issued a scathing statement demanding answers and promising action. He specifically said he was investigating whether Health Net may have violated "federal laws," as well as his state's own data protection laws.

continued on p. 9

Social Networking Sites Are Creating a Flood of New Patient Privacy Challenges

Loud conversations about patients between clinicians in hallways and elevators, or Dr. Smith blabbing to her husband about the knee reconstruction she performed on a New York Yankee, were typical worries in the good old days of HIPAA.

But it's a whole new ballgame with social networking, which has significantly increased the risk of privacy violations and made them harder to monitor. When employees post pictures they have taken with hospital patients on their Facebook wall, potentially hundreds of people they have "friended" could be viewing PHI. If a physician tweets about surgical triumphs on VIPs, it's exponentially more dangerous and more expensive to address through breach notification. Employees may even stream unauthorized video of a procedure on YouTube.

"There are many opportunities for violating privacy" through social networking and blogging, says Jerry Seager, chief compliance officer for Inova Health System of Falls Church, Va. As the threat becomes more apparent, health systems are starting to take action, whether it's blocking employee access to the Internet or through restrictive policies and intensive training.

Until recently, "no one had social networking on their radar. But with all the BlackBerrys and iPhones and all this capability in everyone's hand, you have to think, where are the avenues that could be risks for us?" says Inova Privacy Officer Neschla McCall.

continued

"People are talking about patients they cared for on a private site with people who have no right to know. The same way you can't go home and tell your spouse about the patients you cared for today, you can't tell everyone on your Facebook page."

There's data bearing out the privacy risks of blogs and social networking in health care. Eighty deans from medical schools that are members of the Assn. of American Medical Colleges were recently surveyed about medical students' behavior on social networking sites and blogs. Results were reported in the Sept. 23 issue of the *Journal of the American Medical Assn.* According to a summary of the survey, 60% of medical schools in the U.S. responded, and 60% of them "reported incidents of students posting unprofessional online content." Thirteen percent of the deans cited violations of patient confidentiality. The lead author of the survey was Dr. Katherine Chretien from the Veterans Administration Hospital in Washington, D.C.

Social networking seems to cause a sort of selective amnesia. Some employees, medical students and physicians may forget their fundamental oath to protect patient confidentiality, not to mention their HIPAA training. "When people get into social networking sites, they become very comfortable with the people they are talking to. They lose perspective and the lines blur, and they want to talk about what they do and they want it to sound exciting, so they often go a little too far," Seager says. Instead of just updating their status on their Facebook page — "I'm a pediatric nurse and I took care of 12 patients today" — individuals may name their hospital and talk about some interesting cases. "An egregious example is for someone to have a picture of the clinical area of the hospital on their Facebook page," he says, because a patient could be identified. Or maybe they'll post "Susan is still awestruck from treating Ben Affleck at her hospital today." (Facebook updates are written in third person.)

Work and Private Life Are Blurred

At the heart of the problem is the artificial division, magnified by the Internet, between work life and private life, said Orrie Dinstein, chief privacy leader for GE Capital. "People think, 'when I am at home in my pajamas, you can't tell me what I can say on Facebook,'" said Dinstein, who spoke at a recent social-networking audioconference co-sponsored by the Health Care Compliance Assn. and Society of Corporate Compliance and Ethics. But certain rules are enforced — whether it's HIPAA or sexual harassment prohibitions — and "there is not much of a difference" whether the abuses take place on work or home computers, between 9 a.m. and 5 p.m. or at midnight, he contends. "The line has been erased as a practical matter," Dinstein says.

There's nothing new in that, according to Dinstein. It's analogous to insider-trading violations of the securities law, whether whispered over the phone at work or over wine at dinner. "What's new is the form of interaction and the biggest challenge is that most employees don't understand that many workplace policies can continue to apply to their activities at home," he says. "Social networking is creating a new space for people to say things, which creates a higher risk, so you need new guidelines to remind [them] that just because they are at home on Facebook doesn't mean that none of the workplace policies apply to them."

Inova Restricts Web Access

Inova has responded to the privacy perils of social networking by blocking most employee access to social networking Web sites and implementing relevant policies and training, Seager and McCall say.

With technical support from its information systems security department, Inova prevents most employees from accessing social networking and other inappropriate Web sites at their work computers. "We want to

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, James Gutman; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Russell Roberts

Call Liana Heitin at 800-521-4323, ext. 3066 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.

minimize what employees are doing on computers for personal reasons," Seager says. If they're shopping on eBay, "friending" people through Facebook or entering other Internet worlds, "it's not a business use," he says. Plus the Web site may be inappropriate (e.g., gambling, porn). And, of course, Inova wants to "minimize the potential for security and privacy violations."

Some Inova managers maintain access to blocked Internet sites because they need it for their jobs. For example, marketing people need to surf the Web as part of their job, and McCall has access for HIPAA compliance oversight purposes. "If I hear a rumor" of PHI disclosures on a Web site or blog, "I can check it out," she says. "But it's not as easy as it sounds. If you are trying to find a Facebook page for [nurse] Anne Smith, you get 40 gazillion hits. How do you know what to look for? And if they do it on a friends' basis, they might invite other hospital employees in, but not the privacy officer."

The Internet is too vast a world to monitor in the absence of a specific complaint. Like other compliance violations, inappropriate use of Facebook, blogging and Tweets (and other social networking abuses) will probably be identified only when reported to the privacy officer. "This will be a self-policing thing," McCall says. Sometimes, she says, the complaints come in from good friends of hospital employees who see PHI spilled on social networking sites. They can't abide the danger to the patient and the hospital, and turn in their friend or colleague.

General Ethics and Standards Apply

Inova also approaches social networking risks through its general ethics and compliance standards. "The place we start is our code of conduct and standards of behavior that include professionalism and appropriate communication, and we expect all of our employees to abide by those standards," Seager says. Employees are reminded that they are privy to patients' most confidential information — Social Security number, address, medical information, maybe financials — and that's a sacred trust. "We try to impress upon our employees that they need to protect all that information and the identity of patients and imagine themselves in the same situation," Seager says. "We talk about examples like videos and pictures and sharing patient information and social networking, and that it's not appropriate to share any patient information on social networking sites or blogs." For example, employees are reminded not to take pictures or post pictures on Web sites, McCall adds.

Inova policies also state that employees can't photograph clinical areas unless there are business purposes (e.g., producing training videos) and management has preapproved the project. "We don't want employees taking pictures of patients and treatment areas that have not been authorized," McCall says. The policy also states that clinicians can photograph pictures of wounds for the medical records, "but employees can't take pictures of something weird or gross involving a patient just because [it's novel or interesting]."

Seager says there have been incidents of employees using their cell phones to take pictures of semi-public areas and inadvertently including a patient. A manager happened to witness such events and required the employees to immediately delete the photo from their cellphones.

At times, caregivers and their patients connect on Facebook, according to reports Seager and McCall have received. "This raises an issue of professional boundaries," Seager says. "There are boundaries that clinicians are not supposed to go beyond and it's not appropriate to have a personal relationship with your physician." He says it's a good idea to inform staff that it's not a proper interaction, and at some point Inova might formalize a policy banning such interaction.

Professional Boundaries Are Crossed

Questionable employee behavior prompted Virginia Commonwealth University Health System in Richmond to fast-track more restrictive policies and additional training on the use of social networking sites. "We discovered that employees thought it was sometimes justifiable to post photographs because patients or families asked employees to be in the photos or take photos of the patient. Employees thought that was a form of consent," Compliance Manager Jacqueline Kniska said at the HCCA/SCCE audioconference. Comments about the photos were also a big concern. "That triggered our taking a closer look," she said.

Kniska also found that employees sometimes responded on Web sites to patient comments on the care they received while in the hospital. They meant well and didn't think this violated HIPAA. "We had to remind them it was not the right way to do business and was not justifiable under HIPAA," Kniska said. "Our best approach is to stick to the theme of protecting patient privacy. This is respectful of patient privacy despite what patients may comment about it." She says it's been hard for some employees to grasp this perspective. "It has taken a substantive effort to continually remind them."

Health-care-specific social networking sites used by relatives of sick people to update their virtual community also sounded alarm bells. She urges employees to use caution in what they share about patients they encounter at VCU Health System. "It's almost like people don't associate their virtual world with the real world," Kniska said. For example, some employees couldn't distinguish

between filming that VCU Health System sometimes permits for teaching purposes (after obtaining appropriate consents) and live stream video put on Internet sites. "The risks are not always as clear to everyone as they are to people in compliance," she said.

VCU Health System implemented "very clear guidelines and education," she said. Cell phone pictures were already barred in the hospital, so VCU took it from there. There would be no videography and photography in the hospital by employees. "We grant employees the right to refuse taking photos, even if requested by the family," she said. And VCU took other restrictions further. Even when photos and videos are approved, they can't be posted on the Internet. According to the revamped VCU policy, no information about patients or staff members can be displayed through non-electronic or electronic means, including blogs and tweets.

"Our future challenge is to factor in these technological changes," Kniska says. "There are generational differences in communication styles. The fact is that organizations are using social media tools to further their brands. The challenges are endless and so are the opportunities."

Contact Seager at jerry.seager@inova.org, McCall at Neschla.mccall@inova.org, and Dinstein at orrie.dinstein@ge.com. ✧

Experts Advise the Rewriting of Business Associate Agreements

Covered entities should be revising their business associate agreements (BAAs) to ensure that the CE is not responsible if the BA violates HIPAA or the new provisions under the HITECH Act, according to a task force of the American Bar Association. But CEs may have to get ready to do battle over apportioning liability.

The bar association established a task force to create tools and documents, such as business associate agreements, for CEs and BAs to use that will be compliant with the new enforcement and breach notification requirements included in the HITECH Act of the American Recovery and Reinvestment Act of 2009.

A committee of the task force developed a draft BAA that requires business associates to indemnify the CE, and also mandates that business associates purchase insurance to cover the cost of claims and other expenses that could arise as a result of violations of the BAA.

The draft, currently 10 pages, will be reviewed and revised as appropriate whenever the Office for Civil Rights issues guidance or new regulations, John Christiansen, a health care attorney in Seattle and task force chair, tells *RPP*.

But the indemnification provision is unlikely to change, he says. "This is not something that has been a required part of a BAA before," Christiansen says, "but it is something we think ought to be seriously considered in light of increasing risks for both parties under the new regulatory regime that HITECH mandates."

ABA Addresses HITECH Act

Specific sections of the draft that deal with new HITECH Act requirements and the indemnity clauses are as follows:

◆ "Business Associate shall implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Covered Entity. Business Associate covenants that as of February 17, 2010, such safeguards shall include, without limitation, implementing written policies and procedures in compliance with HIPAA and ARRA, conducting a security risk assessment, and training Business Associate employees who will have access to Protected Health Information with respect to the policies and procedures required by HIPAA and ARRA."

◆ "Business Associate shall indemnify, defend and hold harmless Covered Entity and its directors, officers, subcontractors, employees, affiliates, agents, and representatives from and against any and all third party liabilities, costs, claims, suits, actions, proceedings, demands, losses and liabilities of any kind (including court costs and reasonable attorneys' fees) brought by a third party, arising from or relating to the acts or omissions of Business Associate or any of its directors, officers, subcontractors, employees, affiliates, agents, and representatives in connection with the Business Associate's performance under this Agreement or Service Agreement, without regard to any limitation or exclusion of damages provision otherwise set forth in the Agreement. The indemnification provisions of this Section…shall survive the termination of this Agreement."

◆ "Business Associate shall obtain no later than one (1) month from Effective Date of this Agreement and maintain during the term of this Agreement liability insurance covering claims based on a violation of the Privacy Rule or any applicable law or regulation concerning the privacy of patient information and claims based on its obligations pursuant to this Section in an amount not less than $1,000,000 per claim. Such insurance shall be in the form of occurrence-based coverage and shall name Covered Entity as an additional named insured. A copy of such policy or certificate evidencing the policy shall be provided to Covered Entity upon written notice."

Some CEs might already have included similar provisions in their BAAs or the underlying services agree-

ments with their BAs. But if not, CEs should think about adding them, says David Ermer, of Ermer & Brownell, PLLC in Washington, D.C., who serves on the task force's security committee.

Ermer points out another area of change in a revised BAA, and a possible source of friction between CEs and BAs that deals with when whistleblowing might be necessary. Kristen Rosati, a partner at Coppersmith Schermer & Brockelman PLC in Phoenix, calls this part of the HITECH Act the "rat rule."

Under HIPAA, CEs are liable for business associate violations of the BAA. If a CE knows of a "pattern or practice" of BAA violations by the BA, the CE must "cure" the violation or terminate the contract if the problem can't be fixed. In addition, the CE must report the business associate to HHS if for some reason the BA cannot be terminated, such as if the BA is a sole-source vendor.

'Rat Rule' Goes Both Ways

Now the rat rule extends both ways — to BAs and CEs and then back again. To address this, the bar association committee added this provision to its draft BAA:

"In the event that either Party has knowledge of a material breach of this Agreement by the other Party, and cure is not possible, the non-breaching Party shall terminate the portion of the Service Agreement that is affected by the breach. When neither cure nor termination is feasible, the non-breaching Party shall report the violation to the Secretary."

However, Rosati notes that the CE or BA isn't looking for violations of HIPAA or the HITECH Act — *just violations of the terms of the BAA itself.* Because of this, she recommends that the CE refrain from listing CE obligations in the BAA, and stick to enumerating the BA's responsibilities. That way, there can be no CE violations of the BAA to report to HHS.

Yet, there is more at stake than a simple violation of a BAA. The HITECH Act gives the Office for Civil Rights the ability to impose higher monetary fines if the CE and the BA had knowledge of violations and did not act. Given this, some CEs and BAs may choose to exercise oversight beyond technical compliance with the BAA.

Christiansen says he recommends that BAs also consider having CEs indemnify them. "I'd recommend using a bit of care in this, too, since indemnification requirements can be fairly technical, and a simple reciprocal indemnification provision might not be appropriate for all risks," he adds.

But BAs will need to protect themselves, given "the extension of HITECH/HIPAA jurisdiction to BAs, which does expose BAs to new risks based on CE failures," he says.

Responsible Party Should Pay

The bar association's draft BAA does not specify, beyond general indemnification, who would bear the cost of a HITECH Act or HIPAA violation. Aside from having to pay fines, the most costly part of any violation is likely to be a breach of unsecured PHI, which now must be

accompanied by notifications to affected individuals as well as HHS and the media, depending on the scope of the breach *(RPP 9/09, p. 1)*.

Some CEs are also being ordered to provide credit monitoring services — for up to two years in some cases. The question of who would bear the costs should be included in a BAA, Christiansen says. "Otherwise, the parties will end up fighting about it after the fact, which is probably not the best time for a non-adversarial negotiation," he says.

He and Rosati agree that the responsible party should absorb expenses related to a breach.

"The party that was in a position to prevent the incident should bear the costs," Christiansen says, adding they can be quite substantial for a large breach. Recent estimates put costs for dealing with a breach at $230 per affected individual, he says, which includes "the cost of gearing up to notify, responding, and providing credit monitoring services."

In addition to addressing who bears the costs, it may also be useful to establish which party might actually be doing the notifications. Typically this would be the CE, even if it was not responsible, but there may be instances in which the BA "has a direct relationship with the patient" and would be the more appropriate party to make notifications, Rosati says.

Ermer says to expect that some vendors may want to push back on the insurance coverage portion of the BAA, and may insist that they be responsible for bearing only costs that total the value of their contract. "These are going to be leverage issues" that BAs and CEs will have to discuss, he says.

It may be possible for the BA to obtain "business malpractice" coverage, which Ermer says is often standard in a contract. Business malpractice coverage may have a provision that covers "errors and omissions," he says. But he advises having the BA demonstrate that its coverage does not exclude HIPAA violations.

BAs May Oppose Some Requirements

How much success a CE will have in getting its BAA accepted is likely to depend on how large the business associate is, Ermer says. "The way I see it is there are really two types of BAs — [one is] sophisticated ones that have a multitude of BAAs. These BAs may even address the issue with the CE and create their own BAA, which they will want to use as the basis for negotiation with the CE," he says.

Then there are the "unsophisticated BAs" that don't do a lot of HIPAA-related work and "just happen to be caught up in the HIPAA web. They are going to be more willing to use the CE's BAA," Ermer says.

Some BAs are already starting to make their own demands, says Frank Ruelas, a HIPAA consultant based in Arizona. He says a "big problem" he's hearing is "the BAs are pushing back and saying if the covered entity is concerned about the breach notifications, then they're taking the position that the data being entrusted to them [should] be encrypted."

Of course, the BA would be responsible "if there should be a breach at the BA level because someone defeated the BA's safeguards in managing the encrypted data," he adds.

He also quips that he would "have better luck climbing Mt. Everest's Southeast Ridge than getting BAs to agree to absorb the costs of the notifications and related expenses."

"This continues to be a significant stumbling block" in CE-BA negotiations, but Ruelas says he "sees some progress being made if the covered entity can show the breach was attributable to the BA."

Contact Christiansen at john@christiansenlaw.net, Ermer at dermer@emerlaw.com, Rosati at krosati@cs-blaw.com and Ruelas at frank@hipaabootcamp.com. ✧

Surveys Say CEs and BAs Are Still Far From Compliant With HITECH

The Healthcare Information and Management Systems Society (HIMSS) released two surveys last month: a survey of HITECH Act compliance by subsidiary HIMSS Analytics, and the 2nd annual HIMSS Security Survey. In general, the surveys found that health care organizations have not made many changes in privacy and security since 2008, business associates (BAs) are generally unprepared to comply with the new security breach rules, and much work remains to achieve compliance with the new HITECH Act provisions.

A less comprehensive benchmark study conducted by Crowe Horwath for the Ponemon Institute echoed the conclusion that health care organizations still fall considerably short of full compliance with the HITECH Act.

The 2009 HIMSS Security Survey, which was administered for the first time last year, collected data via a Web-based questionnaire from information technology executives. With 196 respondents, up from 155 in 2008, the major findings from the security survey, released Nov. 3, included:

◆ 60% of respondents said their organizations spend 3% or less of their IT budget on information security, with 21% spending less than 1%.

◆ One-third have had at least one known case of medical identity theft.

◆ 75% conduct a formal risk analysis, half of which occur yearly or more frequently.

◆ Less than 50% said their organizations have a formally designated Chief Information Security Officer (CISO) or Chief Security Officer.

◆ 50% have a plan in place for responding to threats or incidents of a security breach.

◆ E-mail encryption and single sign-on were identified most frequently as technologies that were not yet installed but planned for future installation.

A separate survey, released on Nov. 17 by HIMSS Analytics, a HIMSS subsidiary, looked more specifically at the HITECH Act's impact on privacy and security. Data came from senior IT executives and security officers at 150 provider organizations and 26 business associates. The numbers differ somewhat from those on the security survey, says Lisa Gallagher, senior director for privacy and security at HIMSS, because the security survey questioned people in IT only, while this survey included compliance officers.

The HIMSS Analytics survey found the following:

◆ 2% of CEs and 12% of BAs were not aware of the new HITECH Act provisions.

◆ One-third of hospitals overall and 52% of large hospitals reported having a data breach in the last 12 months.

◆ 91% of hospitals conducted a risk assessment and took actions to address identified risks and gaps in the last 12 months.

◆ Large hospitals had a higher level of awareness of the new breach requirements than did small hospitals.

◆ Over 30% of business associates did not know they are now accountable for the HIPAA privacy and security requirements.

◆ Nearly half of hospitals would terminate a BA contract for violations.

According to Gallagher, the budget numbers from the security survey indicate that organizations "may be short on resources. They're trying to do a lot with a little," both in terms of finances and administrative support. The results on spending levels are consistent with those from 2008, indicating that little has been done to increase the amount of resources applied to security.

Nothing has changed in terms of the percentage of organizations conducting risk assessments in the last year either — 75% are still conducting them, with 50% of those doing them yearly. Gallagher says these static numbers are also "somewhat concerning. We would've expected them to be trending upward. …This many years post-HIPAA, especially with the security rule, people should know they should be doing security risk assessments." The finding about the use of future technologies remained the same as well, likely indicating that many health care organizations have not yet followed through on their plans to add e-mail encryption and single sign-on.

However, rather than simply raising concern about what isn't being done, Gallagher says, the survey results should serve as "a call to action." Business associates and covered entities need to "pay attention, educate their staff, and put the right procedures in place to be actively complying. …We have a history of a perception of non-enforcement. People ask me, 'Do you really think this time they're going to enforce it?'" Considering that ARRA requires CEs and BAs to put a system of compliance audits in place and report some information directly to Congress, Gallagher says her answer is "yes."

BAs Are Less Aware Than CEs

The Crowe Horwath benchmark study, conducted for the Ponemon Institute, collected data from 42 covered entities and 35 business associates. Larry Ponemon, chairman and founder of the Ponemon Institute, explains that the sample was not scientific but representative, and that each organization had multiple responders answering questions based on their expertise. The key findings of the benchmark study, which was released Nov. 10, included:

◆ 94% of respondents were not in "substantial compliance with HITECH."

◆ Only 1% of organizations are ready to meet the deadlines for near-term effective dates.

◆ 90% of organizations experienced one or more data breaches in the past two years.

◆ 98% of CEs have formally implemented a HIPAA privacy compliance program; 43% of BAs have done the same.

◆ 86% of CEs have formally implemented a HIPAA security compliance program; 26% of BAs have done the same.

◆ 32% said their organizations do not provide adequate staff training for both privacy and security.

◆ 21% said their organizations have not formally implemented a risk-based assessment program.

◆ 30% said their organizations do not conduct a detailed security risk analysis.

◆ 22% have not formally assigned the role of security officer or CISO.

Ponemon calls the results "surprisingly negative." Like Gallagher, he cites the lack of resources as a major source of difficulty, saying many health care organizations "are grossly underfunded for security." In addition, he says, C-level executives are not necessarily supportive of privacy and data security compliance initiatives. "They

tend to focus on things that are revenue related. Their view is when a problem occurs, they'll deal with it."

Compliance is also hindered because the "rank and file" employees handling medical records may not be the best to manage privacy, says Ponemon. "I don't know if it's a cultural issue in these organizations, because when we look at other industries, they have data that are far less sensitive than health care records and people are more diligent and more responsible with it. That's true in CEs, but especially true for business associates." Overall, Ponemon notes, the HIMSS survey and Ponemon benchmark study "show the same pattern: We have a ways to go for [compliance] readiness." Strict enforcement from the government — which he anticipates under the current administration, as it seeks to prove that electronic health records are necessary and secure — is the only thing that will overturn complacency about privacy and security, says Ponemon.

See the HIMSS Security Survey at http://tinyurl.com/ygwudq6, the HIMSS Analytics survey at http://tinyurl.com/yhgumsa and the Crowe Horwath study at www.crowehorwath.com/crowe/. Contact Gallagher at (703) 581-2014 and Ponemon at (231) 357-2007. ✧

Case Tests Privacy of Patient Files, Data in Medical Board Complaints

A Texas attorney, defending two nurses indicted on criminal charges of alleged "misuse of official data" after they anonymously reported a physician to the Texas Medical Board (TMB), has been granted access to HIPAA-protected patient files.

The other HIPAA angle in this case: It hinges on the TMB's seemingly inadvertent disclosure of the nurses' complaint itself. Medical board records are never revealed, except in some exceptions, such as when there is a law enforcement investigation of a physician. But in this case, unbeknownst to the TMB, it was the complainants who were being investigated.

Brian Carney, representing the two nurses who worked for a 15-bed county hospital in Winkler, Texas, told *RRP* he needed access to the patient records to prove the women did not intend to "harm" the physician by their report to the TMB.

Carney says he wants to show that, as the nurses charge, the physician's treatment of the patients in question violated standards of care, which the nurses had a duty to report. The complaint refers to the use of herbal medicines.

District Judge James Rex granted Carney's motion for access to patient files in October; a trial is expected in January, but no date has been set. The district attorney handling the case, Michael Fostel, did not return a call from *RPP.* The Texas Nurses Association supported the motion for access to the patient files.

The case began last spring when the nurses filed a complaint on April 7 to the TMB, in which they referred only to patient record numbers. As is standard procedure, the TMB notified the physician that it was investigating a complaint against him and listed patient names that corresponded to the records noted in the complaint.

In response, the physician complained of harassment to the local sheriff, who began his own investigation. He requested and received from the TMB a copy of the complaint, interviewed the named patients, and gained access to the nurses' computers — all in an attempt to discover who had reported the physician, according to court records.

After identifying the women through a letter found on a hospital computer, the sheriff brought the case to the district attorney. The women were indicted and arrested on charges of violating an obscure 1974 state criminal law that prohibits "misuse of official data." Specifically, the law bars "[a] public servant…in reliance on information to which he has access by virtue of his office or employment and that has not been made public" from using such data "with intent to obtain a benefit or with intent to harm or defraud another" by disclosing or using that information "for a nongovernmental purpose."

Because the women worked for a county hospital, from which they were fired on June 1, they qualified as "public servants."

Requesting Patient Files Not Unusual

But the rest of the charge is nonsensical for a variety of reasons, Carney argues, including the fact that the use of information was for a governmental purpose, given that the TMB is a governmental agency. "That's the real flaw in this case," he says.

Carney's motion for access to the patient files was "not that unusual," he says, and it was not opposed by the prosecution. In granting the access, the judge told Carney to put procedures in place to assure that only those who needed to see the information — such as expert witnesses — would have access to it, according to James Willmann, general counsel and director of governmental affairs for the nurses association.

Willmann, who attended the October court hearing, says the association did not oppose opening patient files under the specific conditions unique to this case. "I think the court can build in patient privacy protections" while granting access, Willmann says.

Carey was starting from scratch in building a defense against the charges, which has been a challenge because alleged violations of the law have been

prosecuted only twice before, and neither instance was health-care-related or resembled this case, he says.

The law was "designed for someone like a police officer that is running background checks" when he or she doesn't need the information for the job, he says.

If convicted of the charges, the women face imprisonment of two to 10 years and a fine of up to $10,000. Free on $5,000 bail, the nurses have been unable to find work with the cloud of indictment over their heads, Carney says.

In August, in response to the criminal charges, Carney filed a civil countersuit in federal court against the hospital, the sheriff and the district attorney.

This suit charges that the case against them violates their right of free speech, the state's whistleblower law, Texas health and safety codes and that it "interfered with the plaintiffs' business relationship and at will employment." He has asked for unspecified monetary damages and a jury trial.

"They had an obligation to be a patient advocate," Carney says. The judge in that case, on Nov. 2, ordered the two sides to mediate. Mediation is set for Dec. 17, Willmann says.

One Privacy Issue Unresolved

For its part, the TMB is hopping mad that the information in its files has been disclosed under false pretenses — the sheriff did not reveal that he was probing to determine the source of the complaint. The TMB only releases information to law enforcement officials if they are investigating an individual who is licensed by the board, its spokeswoman told *RPP.*

Willmann predicts that once the suit against the nurses and the one they filed are resolved, attention will turn to how the sheriff received confidential information from the TMB that led to the charges against the nurses.

Nurses nationwide are concerned that the confidentiality of their reports be maintained. Willmann notes that the nurses' association contributed $20,000 to the women's legal fund and raised another $15,000 from 400 individual nurses in 30 states and from 19 other organizations, including the American Nurses Association.

His wish is that that the nurses are awarded what they seek, as well as punitive damages. "I personally hope there are some additional [monetary] damages to send a message to other people that you do not engage in retaliation," Willmann says. "To be slapped with criminal charges when they had no choice but to report…this is a very important case because of the chilling effect it can have on nurses' reporting."

Contact Carney at (432) 686-8300 and Willmann at jwillmann@texasnurses.org. ✧

State AGs Flex Their HIPAA Muscles

continued from p. 1

"I will vigorously and aggressively seek damages, penalties and other appropriate remedies, if warranted," Blumenthal said. "The company's failure to safeguard such sensitive information and inform consumers of its loss — leaving them naked to identity theft — may have violated state and federal laws."

Blumenthal said he would "seek to establish what happened and why the company kept its customers and the state in the dark for so long." The Connecticut attorney general minced no words, saying he was "outraged and appalled" by Health Net's actions. He added that failure to provide notice sooner was "unconscionable foot-dragging," which he said followed the plan's "inexplicable and inexcusable delay."

The Connecticut AG also said he would "demand identity theft insurance and reimbursement for credit freezes as well as credit monitoring for at least two years for all 446,000 consumers."

Health Net's hard drive, which disappeared from its offices in Shelton, Conn., was described as requiring a special reader to view, but it was not encrypted.

Two Incidents in November Alone

Blumenthal's "outrage" over the delay in notification and size of the breach may have been exacerbated by the fact that this was the second such incident affecting his state's residents in the same month that had belatedly come to his attention.

And Blumenthal had already deemed the first incident — which affected "only" 19,000 health care providers — "one of the most sizable and significant" in the state's history.

That loss involved a laptop that was stolen on Aug. 25 from Anthem Blue Cross Blue Shield that contained names, addresses, Social Security numbers and other information on providers (not patients). The laptop was not encrypted.

Anthem didn't tell Blumenthal about the theft until Nov. 9. In a statement released that day, the AG railed at the health plan, using words as colorful as when he berated Health Net.

"Failing to promptly notify providers of the breach is inexcusable — and a possible violation of state law. Waiting two months left providers severely at risk — needlessly and irresponsibly exposing them to financial mayhem," Blumenthal said. However, he cited only Anthem's possible violation of the state notification law as the subject of his investigation.

Specifically, the HITECH Act states that when an AG "has reason to believe that an interest of one or more

of the residents of that state has been or is threatened or adversely affected by any person who violates a [privacy and security provision], the attorney general of the state…may bring a civil action on behalf of such residents of the state in a district court of the United States of appropriate jurisdiction."

In general, the HITECH Act requires health plans, hospitals and other HIPAA covered entities to disclose any breach of unsecured protected health information that puts individuals at significant risk of harm. CEs must also alert the public, the media and the government of breaches affecting more than 500 individuals. Business associates of a CE are also required to alert the CE so that notifications can occur.

The HITECH Act defines what constitutes a "security breach" and describes what the notices to victims should contain, including a brief description of the breach and the type of information involved. Notification must occur within 60 days of discovery, according to the requirement. An AG could bring an action if any requirement were violated.

Although the HITECH Act, a part of the massive Recovery Act, was signed into law in February, the breach notification provisions did not go into effect until Sept. 23, and they apply to breaches discovered after that date. In August, HHS published interim final regulations spelling out the security breach rules and the tiers of penalties for violations, which are now double what they were pre-HITECH Act and can range up to $1.5 million per year *(RPP 9/09, p. 1).*

At that time, HHS said it was not going to impose sanctions for failure to follow the rule for 180 days — which would bring it to the one-year mark of HITECH passage — to give CEs and BAs time to comply.

But Kristen Rosati, a partner at Coppersmith Schermer & Brockelman PLC in Phoenix, tells *RPP* that while HHS is backing off imposing penalties, "that applies only to enforcement on the federal level, and the state attorneys general are not bound by the HHS decision not to impose penalties during this period. Through an action brought in federal district court, the state attorneys general may seek the penalties that are available to them," she says.

In addition, while the federal breach notification requirement might not apply to the Health Net breach because it occurred in May — earlier than the Septem-

PATIENT PRIVACY COURT CASES

This monthly column is written by Rebecca Fayed 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 Fayed at rcfayed@sonnenschein.com.*

◆ **The Supreme Court of Georgia held that a surviving spouse is a personal representative who is entitled to her husband's medical records under HIPAA.** Mary Miller, the surviving spouse of a deceased Alvista nursing home resident, requested copies of her husband's medical records from the nursing home in connection with a possible wrongful death action against the nursing home. Relying on HIPAA, the nursing home denied the request, alleging that it could only disclose the records to a permanent executor or administrator of the estate, who had not yet been appointed. Miller filed an action against the nursing home seeking an injunction to require the nursing home to disclose the medical records. The Supreme Court of Georgia held that Georgia law "authorizes a surviving spouse to act on behalf of the decedent or his estate in obtaining medical records and, therefore, that the surviving spouse is entitled to access the decedent's protected health information in accordance with" the HIPAA privacy rule. Specifically, the court relied on that provision of the privacy rule that requires a covered entity to treat an individual as the personal representative if the person is an executor, administrator, *or other person who has authority to act on behalf of a deceased individual or the individual's estate* under applicable law. Moreover, relying on the privacy rule and prior case law, the court stated that a covered entity must treat a personal representative as the individual. The court disagreed that the person having the authority to act on behalf of the decedent must intend to use the records in her fiduciary capacity as the personal representative. Rather, the court stated that once the personal representative obtains the medical records, the privacy rule does not further restrict the ways in which those records may be used or disclosed. Therefore, the personal representative may use the medical records to pursue a wrongful death claim against the covered entity from whom she obtained the records. *(Alvista Healthcare Center v. Miller)*

ber effective date — an AG in any state with affected individuals could bring a case on other HIPAA grounds, according to Rosati.

HIPAA includes a requirement (pre-HITECH Act) that CEs take action to mitigate the impact of a HIPAA violation, and by failing to notify affected individuals where identity theft is possible, an AG might make the case that mitigation actions were not acceptable, she says.

Conn. Insurance Dept. Is Also Involved

Health Net's possible violations of state law might be easier to establish, as Connecticut has a data breach notification law that requires entities that own, license or maintain personal information electronically to disclose any security breach to state residents "without unreasonable delay." Violations can bring a penalty of up to $5,000 for each affected resident.

In Connecticut, Health Net came face-to-face with not one but two upset (and powerful) state officials, as Blumenthal tag-teamed with Thomas Sullivan, the state's insurance commissioner. Sullivan issued his own statement the day he learned of the breach — Nov. 18, a day earlier than the AG — and made his own demands to Health Net.

Specifically, Sullivan ordered Health Net to provide two years of "adequate credit monitoring protection" to any person affected and, in an unusual move, actually named the company that he said should provide such protection — Debix, an Austin, Texas, company that describes itself as "a leader in the corporate identity theft market."

Sullivan also said he was requesting "information to ascertain the scope of the breach," and asked Health Net to provide "detailed information," including:

(1) The total number of members and providers affected by this incident;

(2) The circumstances that led to the disc drive disappearing;

(3) Whether there was any medical or protected health information on the missing disc drive;

(4) The date that Health Net, Inc. determined Connecticut consumer data was affected;

(5) Documentation of Health Net's established security procedures;

(6) What security plan changes Health Net will be undertaking as a result of this incident;

(7) The steps being taken to determine how this occurred; and

(8) Why there was a delay in reporting this breach to the insurance department.

The Health Net breach also involved data for 316,000 Arizona residents, and apparently that state received word from Health Net a day after Connecticut did. Within two days, Arizona Attorney General Terry Goddard also expressed his anger at the delay in his learning of the breach and told Health Net to immediately notify state residents.

Calling the six-month delay "inexcusable," Goddard said his office was investigating the incident to determine if Health Net had violated Arizona's notification law, which is similar to Connecticut's.

"Health Net's failure to notify its customers after all this time appears inexcusable," Goddard said. "The breach apparently includes sensitive personal health information as well as financial information that could put people at risk of identity theft. There can be no further delay; the company needs to provide notification as quickly as possible."

Anne Hilby, a spokeswoman for Goddard's office, told *RPP* she "could not comment on the specifics" of the investigation because it is ongoing. But the AG is "concerned about potential violations of the law associated with the apparent failure to notify policyholders of the data breach." Hilby declined to say whether the investigation would encompass only state laws, or would also include HIPAA or the HITECH Act.

"We potentially would be concerned with any violations of the law we found evidence of," she says.

More State Action May Come

With new health care breaches being reported regularly, AGs like Blumenthal and Goddard may have other opportunities should they choose to test out their new HIPAA authority.

In same cases, they may have no choice but to take a very hard — and public — position if circumstances are egregious, says John Christiansen, a health care attorney in Seattle.

"Certainly with a breach of [Health Net's] magnitude, aggravated by the failure to give notice for six months, I'd expect an AG to take a strong public stand and investigate aggressively," he says.

"State AGs also have concurrent penalty jurisdiction with the Federal Trade Commission for e-commerce security failures, and we've seen a couple of states — New York and California, in particular — which have been quite willing to pursue penalty actions in those cases," Christiansen adds. "I wouldn't be at all surprised to see some AGs taking a hard look at how they might use this new authority."

Contact Tara Downes for Blumenthal at Tara.downes@po.state.ct.us, Rosati at krosati@csblaw.com, Hilby at Anne.Hilby@azag.gov and Christiansen at john@christiansenlaw.net. ✧

PRIVACY BRIEFS

◆ **Blue Cross Blue Shield of Tennessee (BCBST) is sending letters to as many as 3.1 million customers following the theft of 57 hard drives containing personally identifiable information.** According to Mary Thompson, a BCBST spokesperson, someone broke into a training facility in Chattanooga on Friday night, Oct. 2 and removed the 3½- by-10-inch hard drives from a data closet. The computer monitoring system sent out an alert that the servers were not functioning properly. On Monday morning, a maintenance employee went to assess the problem and discovered the break-in. BCBST contacted law enforcement immediately, Thompson says. The hard drives contained "voice recordings of eligibility and coordination-of-benefit calls used for training purposes," according to a BCBST press release, which investigators are retrieving and analyzing. BCBST is identifying those individuals most at risk for having their Social Security numbers accessed and is contacting them first. The initial batch of letters was sent out Nov. 30, and letters will continue to go out over the next month, says Thompson. See the press releases at www.bcbst.com/about/news/releases/.

◆ **The vice president for corporate compliance at Mercy Medical Center in Baltimore sent letters to an undisclosed number of patients warning that their records may have been breached,** *The Baltimore Sun* reported Nov. 11. The letters state that a former employee may have accessed records with patient information in order to apply for credit cards and loans. Neither Mercy officials nor the Maryland attorney general's office returned *RPP*'s phone calls for comment. See the article at http://tinyurl.com/ybwukou.

◆ **The National Community Pharmacists Association (NCPA) is joining the consumer and privacy groups Consumer Action, U.S. Public Interest Research Group, Patient Privacy Rights, Private Citizen and Privacy Journal in urging HHS's Office for Civil Rights and the FTC to investigate possible HIPAA violations by CVS Caremark Corp.** NCPA has collected 93 letters documenting CVS Caremark's alleged use of personal medical histories for marketing purposes, such as to encourage patients to switch prescriptions from an independent pharmacy to CVS. The solicitations, which contain sensitive information including the names of specific drug prescriptions and the last date the consumer filled the prescriptions, were sent by mail, which NCPA claims increases "the risk that a neighbor or other unauthorized person might inadvertently learn of a medical condition." A spokesperson for CVS Caremark tells *RPP,* "We have extensive policies and procedures in place to safeguard our customers' sensitive personal and health information, and we follow federal and state laws in handling this information." Read the NCPA press release at http://tinyurl.com/ykgva2c.

◆ **A former patient services coordinator at Johns Hopkins Medicine in Baltimore was sentenced to 18 months in prison for stealing patient information to make credit card purchases and obtain cash,** according to a Nov. 20 Department of Justice announcement. From August 2005 to April 2007, Michelle Courtney Johnson provided co-defendant Shannell Bowser with the names, Social Security numbers and other personal identifying information for more than 100 current and former patients. Bowser used the information to apply for credit, obtain cash from ATMs and make purchases that were delivered to Johnson, Bower and other conspirators' homes. Overall, the defendants stole information from at least 207 individuals to apply for at least 373 credit accounts, of which 125 fraudulent accounts were opened. Johnson will also pay restitution of $203,627. Bowser pleaded guilty as well and was sentenced to five years in prison and will pay the same amount in restitution. See the DOJ press release at http://tinyurl.com/yfvvzsx.

◆ **Officials at Wentworth Douglass Hospital (WDH) in Dover, N.H., were not required to report a patient privacy breach after an employee improperly accessed electronic records more than 1,800 times,** according to *Foster's Daily Democrat.* Between May 2006 and June 2007, a hospital employee, who had been transferred from the pathology lab for poor performance, retrieved and altered patient medical records. Drs. Cheryl Moore and Glenn Littell, who ran the independent pathology clinic based at the hospital, pushed administrators to disclose the security breach, but the hospital denied their requests and subsequently ended their 28-year contract with the hospital. WDH officials claim they were not required to inform patients of the breach under HIPAA or state laws and that they did not renew the pathology contract due to cost factors. HHS confirmed that a disclosure was not mandatory under HIPAA prior to when the HITECH Act became effective. The hospital did inform the patients' doctors about the security breach in July, two months after an internal audit. Read one in a series of articles about the WDH breach at http://tinyurl.com/ykhshw9.

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.)