Report on
PATIENT PRIVACY

Volume 7, Number 9 • September 2007

Practical News and Strategies for Complying With HIPAA Rules

Contents

New Health Information Privacy and Security Legislation Is Called 'HIPAA on Steroids'

The Health Information Privacy and Security Act (S. 1814) includes several provisions that would make privacy protections much stronger, prompting industry experts to say that it is giving HIPAA some teeth. Although this bill may not pass soon, its privacy provisions are so momentous that privacy and compliance professionals would be well-advised to begin paying serious attention.

The bill, introduced in late July by Sens. Patrick Leahy (D-Vt.) and Edward Kennedy (D-Mass.), would establish a National Office of Health Information Privacy within HHS that would be led by a director appointed by the HHS secretary *(RPP 8/07, p. 12).* It also would require that patients be notified of health data breaches within 15 days of the breach occurring, among other provisions.

But what sets this bill apart from the dozen or so proposed health care information privacy and security laws that Congress sees in a year? For example, the Healthcare Information Management and Systems Society (HIMSS) says there are now 11 bills pending that have emphasis on health care IT. About half of those have privacy and security requirements.

"It's HIPAA on steroids," says Dallas attorney Cynthia Stamer. "This bill, on every level, expands the people who would be subject to the requirements — business associates, employees and employers would be subject," she says.

continued on p. 9

Concord Hospital Took a Series of Effective Steps to Weather Recent Data Breach

The brief, innocuous-seeming e-mail arrived at 5 p.m. on May 30, just at the end of the business day. A company that had been hosting an online bill-pay Web site for Concord Hospital in New Hampshire without apparent problems for the previous 10 months had a big goof — patient data had been left unsecured on the Web, the company said in the e-mail. But we've corrected the problem, so don't worry, the e-mail said.

The folks at Concord, whose slogans include "We heal through technology," were shocked and upset over this news, as anyone receiving this kind of information would be. But they immediately took steps to deal with the situation and, today, say they believe they did most things right and weathered the breach (including a front-page story in the local paper) quite well.

The actions Concord took — including issuing a press release, setting up a phone number for people to call with questions, posting a Q&A page on its Web site and offering a free credit monitoring service — can serve as a real-life example for hospital privacy and security compliance officials to follow, should they ever find themselves in this unfortunate situation. At issue is not only how to meet HIPAA requirements as well as state laws, but also how to minimize the possible harm to a hospital's reputation (see story, p. 4).

continued

Published by Atlantic Information Services, Inc., Washington, DC • 800-521-4323 • www.AISHealth.com
An independent publication not affiliated with hospitals, government agencies, consultants or associations

Exposure Involved Bill-Pay Feature

The hospital is the second largest in the state. Licensed for 295 beds, it now staffs 209 of those. It is among the 100 "most wired" hospitals as ranked by a journal published by the American Hospital Association. It began offering a Web-based "My Bill" feature about 10 months ago to permit patients to check their accounts and make payments electronically.

The company selected to offer the service, Verus Inc., was based in Washington state. The firm has since gone out of business after it was revealed that the same breach that ensnared Concord had also affected four or five other hospitals. Bruce Burns, Concord's chief financial officer, told *RPP* that his hospital was notified in early June by Verus that it was ceasing operations. *RPP* was unsuccessful in repeated attempts to contact the firm.

The first hint of a problem came in the May 30 e-mail that was received by Concord's patient accounts director. "A phone call would have been nice," Burns pointed out. *(Hint to vendors: When something like this happens, pick up the phone!)*

"They told us that they had been doing maintenance on April 11, 2007," and that a firewall had been turned off, exposing patient data. "The next day it had been cached by the Google bots....It sat out there for six weeks," Burns said, referring to the automated system that the search engine uses to collate data. Verus said it had not become aware of the breach until May 22.

What was exposed was "an archived file of old account information," which included names, addresses, birthdates and Social Security numbers, Burns said. "Unfortunately, this was human error in the upgrade process," Burns said. "They had policies and procedures, but they weren't followed."

The first thing Concord had to do after getting the e-mail was call Verus and attempt to determine the size of the breach — Burns said the original e-mail didn't even say how many patient accounts had been exposed.

Concord discovered on its own that there were "a little over 9,000" patients whose data were involved — even though only 2,000 or so had signed up to use the bill-pay feature. "[Verus] must have assumed it was an insignificant amount [of patients]," Burns said. "It was a significant amount for us."

Team Met to Plan Strategy

Burns then met with other top officials from Concord, including a representative of its information technology (IT) security group and the privacy compliance officer. The same group of individuals met for several days and throughout that weekend, Burns said.

"On Monday morning [June 4], we met with public affairs folks and notified legal counsel. The [public affairs] folks started to work on a communications matrix," which included notifying affected patients. In addition, Concord continued to probe with Verus what had happened, Burns said, and it even hired a forensic data company that visited Verus on site in Washington state to verify events and to ensure that no data would be released again.

Verus agreed to this visit. In fact, the hospital's business associate (BA) agreement specified that Verus would cooperate in the event of a breach. The hospital also terminated its relationship with Verus. "We basically felt that the relationship had been damaged, regardless of our ability to recover," he said. Burns added that, technically speaking, the firm lived up to the terms of its BA contract.

The team produced a patient notification letter (see p. 3), and it was ready to be mailed by Thursday afternoon to 9,300 individuals. The letter explained what had happened and listed three credit-watch companies that patients could contact. Each of the firms offers a free, three-month credit-watch product.

Part of the communications plan also included posting a Q&A document on the hospital's Web site, and Concord also made dedicated phone lines available for

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, Eve Collins; Contributing Editor, Nina Youngstrom; Executive Editor, James Gutman; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Russell Roberts

Call Eve Collins at 1-800-521-4323 with story ideas for future issues of *RPP*.

Subscriptions to *RPP* include free e-mail delivery in addition to the print copy. To sign up, call AIS at 800-521-4323. E-mail recipients should whitelist **aisalert@aispub.com** to ensure delivery.

To order **Report on Patient Privacy**:

(1) Call 1-800-521-4323 (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* ❑ $363

Bill Me ❑ $388

*Make checks payable to Atlantic Information Services, Inc.
D.C. residents add 5.75% sales tax.

callers with questions (including a toll-free line). The patient letter indicated the lines would be operational beginning Sunday, between 10 a.m. and 3 p.m.

The letter was posted by a mailing house on Friday, June 8. At around the same time, the hospital also notified the state attorney general of the breach.

The hospital prepared a press release about the breach and the notification letters, which it intended to issue on Monday, June 12. But due to the swiftness of the U.S. mail, some patients got the letters the day after they were mailed, and started calling the hospital nursing staff.

Hospital's Letter to Patients Explains Data Breach Incident

Concord Hospital in Concord, N.H., sent the following letter to more than 9,000 of its patients after an incident in which one of its vendors left patient data unsecured on the Web. Contact Bruce Burns, Concord's chief financial officer, at keastman@crch.org.

Dear Concord Hospital Patient:

I am writing to you because we have learned of a serious data security incident that has occurred involving some of your personal information. On May 30, 2007, Verus Inc., the company that Concord Hospital subcontracts with to enable patients to view and pay their bills online, notified us of a lapse that unintentionally occurred in their data security procedures on April 12, 2007. As a result of this lapse, some of Concord Hospital's patient files were left unprotected when the company turned off the firewall, or security device, for maintenance purposes. Data from several other hospitals across the United States was also compromised.

The security breach involved a number of files that included 9,297 Concord Hospital patients and/or guarantors' personal information, including name, date of birth, address and Social Security number. Regrettably, your personal information was included in the data that was at risk. However, **no credit card information was exposed and to the best of our knowledge, no one could access personal health information.**

The personal information was exposed and unprotected on the Internet for over a month before it was discovered, upon which the problem was rectified and the information was immediately secured. We feel it is essential that we notify you of the potential risk.

Concord Hospital takes its responsibility to protect our patients' personal information very seriously. Since being notified of the security breach, we have taken all necessary actions to assure our patients' data is secure and we'll do everything we can to prevent this type of breach from occurring again. In addition we have contacted the New Hampshire Attorney General's Office to alert them of this issue.

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert tells creditors to contact you before they open any new accounts or make changes to your existing accounts. You may activate a fraud alert by contacting any one of the three major credit bureaus below. Once one company has been contacted, the other companies are also notified. You may also consider requesting a free credit report from any of the three companies.

Equifax
1-800-685-1111
http://www.equifax.com
Experian
1-888-397-3742
http://www.experian.com
Trans Union
1-800-888-4213
http://www.transunion.com

If any unusual or suspicious activity is noticed, the FTC recommends you contact the local authorities immediately and file a police report. Additionally, if that should happen, you may also file a report with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338).

Should you have additional questions or concerns, please contact us. We have established a special telephone line at 603-230-7399 and have dedicated staff available to respond to your needs. You can also check our website, www.concordhospital.org for updated information.

I am truly sorry for any distress that this situation may cause you and all of us at Concord Hospital stand ready to assist in any way that we can.

Sincerely,

Michael B. Green, President/CEO

Burns got a call from the staff at home and took steps to get the press release out early. He also gave interviews to reporters, as did the hospital's chief executive officer, who had signed the patient letter.

The story appeared on the front page of the *Concord Monitor* that Sunday, June 11. Sunday newspapers are the most read of any day of the week, so the story likely reached a readership greater than would have happened on a weekday. The story also got picked up by the wires and started appearing in other papers.

Concord also took steps to notify its employees, sending them an e-mail on Friday, before the letter was mailed.

The phone lines proved to be a good way to communicate with patients; Burns said more than 1,500 calls were received. The hospital did a second mailing after some letters came back undeliverable.

What Lessons Were Learned?

In some sense, the hospital had to make it up as it went along, adapting to issues that arose. For example, on June 26, the hospital announced it was offering free one-year credit monitoring to all affected individuals who requested it. (Patients request a coupon to cover the cost.)

This is a package of services that Concord purchased beyond the three-month monitoring, Burns said. Thus far, fewer than 100 people have selected this service. Burns said he contacted one of the other hospitals affected by the Verus breach to find out which company might be good to use for this.

All in all, Burns felt that his hospital had done a good job in dealing with the breach, but he and others at Concord recognized that, next time (heaven forbid), they might do things a little differently. The phones should have been available earlier, he said, and the hospital would offer the year-long credit service from the start.

"I think most people said we got right on it, that we were out in front, that we had responded quickly and hopefully allayed some people's fears," Burns said.

The local newspaper, however, wrote an editorial criticizing the hospital for not acknowledging the breach sooner. Burns said the hospital "was trying to be quick" and needed time to figure out what had happened and to notify employees before the public. "Could we have done [the letter] two-to-three days faster? Maybe," he said.

But he noted a St. Vincent Health hospital in Indiana, one of the other hospitals that also suffered a Verus-related breach, did not issue a notification until nearly two months had passed.

Could Concord have prevented this? Was Verus a good choice? In hindsight, Burns said that, although his hospital did appropriate due diligence when Verus was hired, no one from Concord ever visited the Verus offices — Verus officials came to Concord. That was probably a mistake, and next time Concord officials will personally visit any similar companies themselves, he said.

The hospital is also now reviewing the procedures and contracts of all third parties that must maintain patient data in a secure way to see if all is well with them. In addition, Concord intends to formalize an "incident response" procedure to deal specifically with breaches of this type, in the same way that it handles disasters, Burns said.

In addition, "we will establish a privacy and security oversight group to assess new IT projects when they come forward. It will be more of a coordinated effort," Burns added.

It seems unlikely that Concord will be able to recover any of the costs associated with the breach, but Burns said they were not significant.

Contact Burns at keastman@crch.org. ✧

Damage Control After Breach: Six Steps Will Limit Your Risks

The worst has happened. A privacy and security breach has occurred, exposing Social Security numbers and other information about thousands of patients to anyone with Internet access (see story, p. 1). Or maybe a laptop computer containing patient data is missing. You hear the news; you catch your breath. Then what?

What steps should you take to minimize the possible damage — to ensure that your patients do not become victims of identity theft?

RPP asked Jeffery P. Drummond, a partner in the health care section of Jackson Walker, a Texas law firm, to provide tips and strategies for damage control in the event of a breach. Drummond frequently speaks on privacy and security issues and HIPAA, and operates a popular blog at http://hipaablog.blogspot.com.

The steps to responding to a breach, he said, include a reality check, assembling the right people, telling your story, disciplining those responsible, accounting for the disclosure and learning from the experience.

(1) Reality check. You may have a small, non-newsworthy event on your hands or a big event that could make the front page. The first thing you need to do after learning of a breach or possible breach is "a reality check" to discover what really happened, what is missing, how it happened, and, finally, how great is the risk that the data could be misused.

This helps you determine whether to notify patients. Secondarily, you do an assessment to ponder if more harm could result from notification.

(2) Assemble the right people. After an incident occurs, you need to quickly rally the troops and bring together all your personnel who are going to help you respond to it. "Your IT people, your lawyer, your c-level executives" (chief executive officer, chief operating officer, chief information officer, etc.), Drummond said.

Don't forget your public relations staff and outside individuals who might also be essential, including disaster recovery specialists if you have lost data and a credit monitoring service to offer to affected patients.

"PR people and lawyers, I think, will have the biggest impact" on how well you handle the breach, Drummond said.

(3) Tell your story (if necessary). Once your team is in place, it will determine the steps you will take, including whether to notify patients and the public. Pay attention to state laws as well. For example, Texas state regulatory and licensing authorities have the right to randomly review patient files, and an organization must document in patient files whether any data has been disclosed without authorization.

Similarly, state laws may require notification to affected patients. "You need to know what your legal duty is," Drummond said. Under HIPAA, he added, "you have to mitigate any known harmful effects."

But you may not want to stop there. Drummond cautioned that, particularly in a field where patient trust and your public reputation are so important, "you also have an ethical duty to do what you think is right for your patients."

If You Notify, Offer Specifics Promptly

If you decide that notification is required, "tell people as soon as possible in a way that does not create panic," Drummond said. "You can't run out and yell fire." He recommends offering specifics about what happened and steps you are taking to mitigate the breach, including whether you are offering any credit monitoring.

How you notify affected individuals will depend on how many are involved. "If the data is on 100,000 people, you might not be able to locate them all," Drummond said. "If the data was on 50 people, it might be feasible to contact everyone." Do so "as soon as you can without jeopardizing the investigation."

Drummond represents a group of physicians who had a break-in at their office and had several laptops stolen. After reporting the theft to the police, they learned that a number of buildings in the area — that did not involve health care businesses — had recently also been burglarized, with computer hardware missing.

The authorities told the physicians they were certain the thieves were after only the computers, that they would probably be "scrubbed" clean and then resold. The police, Drummond said, were convinced that the thieves were not stealing the data to engage in identify theft. "It appeared to be a crime wave that involved buildings in the area," Drummond said. Given this, Drummond advised the physicians that they did not have to notify patients of the theft.

Drummond noted that in Texas, the law strictly defines what a breach is, which ties into whether notification must be given. If the Texas physicians had believed this was necessary, they would have been hampered in doing more than a global announcement of a theft because they were not sure which patient data were actually on the computer. "They did think there was some protected health information on the laptops, but they were not really sure what was on them," Drummond said.

(4) Discipline those responsible. If you can pinpoint blame in the incident, you need to take action to punish them, Drummond said. You should follow your own policies in this regard, such as those you have specified for unauthorized uses and disclosures, or for HIPAA compliance in general.

'Heads Need to Roll' if Someone's Responsible

But Drummond said he believes strongly that individuals responsible should be terminated whenever possible, bearing in mind whether the person is in a union or may have rights to a grievance procedure. "If there is someone responsible, heads need to roll," he said. "That person needs to be fired and marched out of the building by security."

This will send a message to other employees that infractions will be treated seriously, especially if you don't have instances like this happen very often. "It will scare everyone, and fear is a good motivator," he said. If a third party or a vendor is responsible, you may also want to terminate your contractual relationship.

(5) Account for the disclosure. According to Drummond, a breach or data loss is required to be logged as an unauthorized disclosure. He noted that the documentation must specify what happened and what was done to meet the mandated obligation to "mitigate any known harmful effects" of the disclosure.

So in the case of the physician group, they needed to note that "they knew, with a high degree of confidence, that these were going to be sold for their hardware value; the police were backing them up that this was a hardware theft. They had no reason to suspect there were any known harmful effects," Drummond said.

In addition, if you know the actual patients affected, you must note the loss in each of their charts.

(6) Learn from the experience. Do you have a flaw in your privacy and security compliance policies and procedures? What changes are necessary to prevent a similar occurrence?

In the case of the physicians, the data on the laptops were not encrypted or password protected — measures the physicians realized were necessary, and they put these in place for their other computers, Drummond said. "If this is truly a data breach, if data is core to the incident...if you have someone hacking in or a firewall breach, you need to be much more intensive in your dealings with it," Drummond said.

Drummond warns against falling into the "bad boxer" trap. A bad boxer covers the spot he was last hit, but doesn't think about how to protect other vulnerable spots that haven't been attacked (yet). "Do a specific review of your whole system, and look for areas where you could have similar problems," he said. "Then, be creative, and figure out where your other weaknesses might be."

Part of your analysis should include whether you missed any red flags if the breach was caused by a vendor. Was your business associate agreement airtight? Did you do appropriate due diligence before you selected them? "Tech companies bloom and die daily," Drummond cautioned.

"Sometimes [a firm] is just a bunch of guys from brand X who form brand Y. They might be all the smart guys, but they might be all the stupid guys. There is a lot of risk out there. You have to be very cautious."

And finally, remember what is at stake in all of this. "I am a believer that the PHI is of little value beyond the Social Security numbers. Unless you are a celebrity, no one cares about Aunt Edna's gallbladder" or other medical information, Drummond said. But he adds, that "even though the great likelihood is that individuals are not going to be harmed, your reputation and your good name are toast if you don't react appropriately."

Contact Drummond at jdrummond@jw.com. ✧

E-mail Is Still Big Privacy Risk; CEs Turn to Scanning Technology

E-mail has become an indispensable tool in every industry, and health care is no exception, as busy professionals use the technology to quickly communicate with colleagues and patients. But for those who deal with protected health information (PHI), pressing the "send" button can be fraught with compliance dangers. As hospitals and covered entities (CEs) see their peers victimized by damaging electronic PHI breaches, more and more are installing filtering technologies that not only scan outgoing e-mails for PHI, but also can encrypt the messages.

Ensuring appropriate use of e-mail is a top HIPAA concern, say compliance and information officers. "E-mail is so prevalent in society and has become such a casual occurrence," says Michael Apfel, chief privacy officer at Truman Medical Centers in Kansas City, Mo. "It has integrated itself into our professional and personal lives. It's very important to us that we provide consistent and constant education and monitoring of those communications."

One slip-up can become a whopper. For example, a Palm Beach County, Fla., health department statistician and epidemiologist mistakenly attached a list containing more than 6,000 names of HIV/AIDS patients to an e-mail in 2005. The message was sent to 800 of the department's 900 employees *(RPP 3/05, p. 4)*.

Such a disaster is unlikely to happen at Truman Medical. The organization's internal e-mail system is encrypted, Apfel tells *RPP*. "E-mail that contains PHI that is business appropriate is permitted within our internal e-mail system," he explains. "Absolutely no PHI may be released or shared with any systems external to our e-mail system."

To ensure this doesn't happen, the hospital monitors outgoing e-mails with technology that searches for specific language or strings that could identify a patient account number or medical record number, Apfel says. While he declined to discuss any examples of the technology catching PHI before it was sent, Apfel says one area of e-mail concern involves the influx of new residents who work at the research institution every year.

New residents are required to go through HIPAA and privacy training before they are given access to any of the computer systems, he says. But mistakes can happen, Apfel acknowledges. One example might involve an intern sending PHI to his or her own personal e-mail account for later documentation in an educational paper. "In those scenarios, it's not so much patient names but enough identifying information that you could run afoul of the identification requirement within the privacy rule," Apfel says.

Some CEs Are Slow to Adopt Technology

Despite the obvious pitfalls of e-mail, some health systems have been slow to adopt technology that can ward off HIPAA violations, according to the head of information security company Workshare, Inc.

"I'm aware of very large health…providers in the country that have done nothing yet," says Joe Fantuzzi, CEO of Workshare. One of the challenges with HIPAA is that the costs of noncompliance are not particularly high, he contends.

"What is happening is that because the actual penalties are not very strong, a lot of people are moving very

slowly," Fantuzzi says. "That doesn't make it right. We see companies move — even if they haven't had any sort of leak or gaffe — because they are very focused on their ethics and reputation. We see people who are moving slower, but who have the same sort of risk profile."

Workshare analyzes e-mail content and then remediates potential risks by blocking or quarantining the message. Workshare also partners with tech firm Cryptzone (formerly Secured eMail), which provides the application to encrypt data. "That's the best standard of care," Fantuzzi says of the detection and encryption capabilities. This standard is important from a legal aspect, in that case law tends to require that an organization be "at the midpoint or above what is available," he adds.

Policies Are Built Into Technology

Messaging security vendor Proofpoint, Inc. also offers various e-mail scanning and encryption products. On a basic level, its software will scan outbound communications for PHI and personal identifiers, and then quarantine the message, explains Keith Crosley, director of market development at Proofpoint.

"The more advanced case — where people are not just trying to block stuff but are trying to facilitate e-communications — they will have a policy that says if you detect what would be a HIPAA violation, then encrypt the message before the transmission and send it in an encrypted way," he tells *RPP*.

Because CEs may not have policies regarding e-mail usage, Proofpoint comes with preconfigured policies, he says. "It's literally as simple as the administrator saying, 'Turn on the HIPAA protection policy,'" Crosley says. "It gives you the basics: Find PHI containing e-mail and do something with it, whether that is quarantine or encrypt, depending on what modules you buy."

Crosley says Proofpoint has worked with organizations in which hundreds of privacy violations a day are occurring. "It's not necessarily something bad going on — especially in the HIPAA case — it is someone sending protected health information in an e-mail and it's not being encrypted." This may occur through the use of personal Web-based e-mails, especially when nurses change shifts. "You would have the shift nurse on duty using her or his Yahoo or G-mail account to send information about the patient to the next shift nurse," he says. "That's a violation of HIPAA."

MedCentral Health System uses Proofpoint to identify and filter e-mail messages containing PHI, says Mike Mistretta, chief information officer at the hospital system in Mansfield, Ohio. The filters are updated regularly, and MedCentral has the ability to fine-tune them as appropriate, he tells *RPP*. "Currently we block messages containing PHI, and a copy is forwarded to myself and our compliance officer to contact the individual attempting to send the message in order to provide education and provide an alternative way of sending the information if appropriate," Mistretta says.

Ideally, Mistretta says, MedCentral would like to identify messages containing PHI, automatically encrypt them, and then send them out in a transparent fashion. "Proofpoint has this capability with an additional module for an additional fee," he notes. "However, it has been cost prohibitive for us to purchase this additional engine."

More Doctors Use E-mail With Patients

While hospitals grapple with the e-mails of thousands of employees, more and more doctors, even in small practices, also are using this method. In 2007, 31% of physicians reported using e-mail to communicate with patients, up from 24% in 2005, according to a survey released this spring by health care research firm Manhattan Research, LLC.

David Ermer, managing partner at Washington, D.C.-based Gordon & Ermer, says there are two major problems with e-mail: misaddressing and forwarding. "E-mail is very convenient, but address errors can occur and the problems associated with address errors are magnified if protected health information is included in the message," he says. "Internal controls can address this problem," Ermer adds. "My concern about using e-mail for legally privileged discussions is that they are so easy to forward to others, and forwarding can destroy the privilege."

Jasmine Moghissi, M.D., a physician with a solo practice in Fairfax, Va., is one physician who has embraced e-mail. She sends roughly 20 e-mails to patients per week. But she first gets their permission in writing. "I will not send out e-mails unless they have signed a consent form," she tells *RPP*.

Among other things, the consent document informs patients that e-mails are not encrypted and could be observed en route by a third party. It also states that Moghissi tries not to put sensitive information in e-mails — for instance HIV results are not reported in e-mail — "but there may be information contained in an e-mail that you consider sensitive."

Moghissi says that realistically she's not looking up everyone to make sure they have a consent form before sending an e-mail. But their name doesn't go into a contact list unless they have a consent form, she adds. Moghissi also does not write the patient's name in the e-mail.

In the past five years, Moghissi acknowledges that she has sent two or three e-mails to the wrong patient. "They knew they had some blood drawn, but they didn't know whose results they were." She says that she would prefer to send encrypted e-mails, but adds that

dealing with the software is difficult. "My e-mail address is on my Web site, people e-mail me about all sorts of stuff, and my patients e-mail me. If they had to go through some sort of encryption process, it would really shut things down."

Contact Apfel at michael.apfel@tmcmed.org, Crosley at kcrosley@proofpoint.com, Ermer at (202) 833-3400, ext. 3009, Fantuzzi through Mary Van Zandt at mvanzandt@trainercomm.com and Mistretta through Cindy Jakubick at cindy@medcentral.org. ✧

State Cites Privacy Issues at Facility; Hospital Has Easy Fixes

Washington state inspectors found problems with patient confidentiality at a facility that is part of the Swedish Medical Center system, according to the state's reports, which were completed in May. The system put a corrective action plan in place and says the tools mentioned in the report were brand new and have been updated to protect privacy.

Swedish is the largest nonprofit provider in the Seattle area. It consists of three hospitals, a stand-alone emergency department, 12 primary care clinics and home health care services.

According to the report:

◆ ***"During observational rounds conducted on May 15, 2007 in the emergency department nursing station area,*** it was noted that the full surname of the patient was located on the 'electronic white board' and was readable from a distance of 15 feet. This allowed any person either walking by or standing near the workroom to observe and read the names of the patients currently being seen in the emergency department. This observation was confirmed by administrative staff present at the time;" and

◆ "***During observational rounds conducted on May 15, 2007 on the medical and surgical telemetry units,*** cardiac rhythm monitors including the patient's full surname were noted to be located in the public hallways of the units. This allowed any person either walking by or standing near the monitors to observe and read the names of the patients currently being monitored on the telemetry units. This observation was confirmed by administrative staff present at the time."

"The hospital has submitted a corrective plan of action, and we have accepted it," says Donn Moyer, media relations manager for the state's Department of Health. "The hospital must assure us that the corrective actions are implemented and [also] will provide progress reports…on that work. We have the option to go back to check and verify that it's happening. We'll also review progress in the next licensing inspection," he tells *RPP*.

State auditors conducted a re-licensing survey of Swedish's Cherry Hill campus (formerly known as the Providence facility) and the First Hill, Ballard and Issaquah campuses in May, but spotted the confidentiality issues only at the Cherry Hill location.

Marianne Klaas, director of accreditation and safety for Swedish, explains that both of the devices cited in the report were "brand new…only about 24 hours old." State inspectors came for the regularly scheduled licensing survey just after they had been installed. "If we had had a chance to sit back and look at them, we would have noticed it," she says. The reader board in the emergency department was placed in a nursing station alcove with the intent to shelter it from direct view, but they state surveyor felt that others could still see patients' names too easily, she explains.

It was easy enough to fix, Klaas says: Instead of using patients' full names, they now use initials. "We need to see what patient is where because people are moved around. We need to have some sort of patient identifiers to track care and communication. There is no link to the patient's name and other protected information," she says. These devices will be installed at other Swedish facilities, but with the corrections already in place, she adds.

Swedish has its own internal audits and checklists that include privacy, Klaas says, but state inspections also are a good opportunity to have more expert eyes look things over. "It's a balancing act. We have to make sure we are not displaying confidential information, but are still using the tools for patient safety and good workflow."

Visit www.doh.wa.gov and www.swedish.org. Contact Klaas at marianne.klaas@swedish.org. ✧

Most Popular Stories on AISHealth.com (August 2007)

1. Will HIPAA 'Business Associates' Survive Implementation of Electronic Records?
2. Insurers, Employers Must Disarm HSA Landmines Before Fall Enrollment
3. Specialty Pharmacy Spending Still Increasing, As New Drugs Make Big Splash
4. Former Compliance Officer Alleges Hospital Chain Paid for Referrals
5. Part D Plan Sponsors Must Now Prepare for CMS Audits

Read these stories at www.AISHealth.com/Top5.html.

Bill Would Toughen Protections

continued from p. 1

According to the bill, the requirements apply to any 'person' "that is a government, governmental subdivision of an executive branch agency or authority, corporation, company, association, firm, partnership, society, estate, trust, joint venture, individual, individual representative, tribal government, and any other legal entity. Such term also includes the employees, contractors, agents, and affiliates of all legal entities described in the preceding sentence, whether or not they are acting in the capacity of their employment, contract, agency, or affiliation," it says.

HIPAA violations carry civil monetary penalties and criminal penalties. The U.S. Code section dealing with criminal penalties for "wrongful disclosure of individually identifiable health information" (42 U.S.C. 1320d-6) refers to "a 'person' who knowingly [violates the law]." A "person" in HIPAA means organizations as well as individuals.

But the Department of Justice (DOJ) released a memo in June 2005, saying that rank-and-file covered entity (CE) employees probably wouldn't be prosecuted for HIPAA violations. Only CEs would be prosecuted, the memo indicated.

"The Department of Justice said it generally wouldn't go after employees, and then almost immediately went after an employee," Stamer points out, referring to the September 2006 prosecution of a former scheduler in a Florida facility owned by the Cleveland Clinic for HIPAA violations *(RPP 10/06, p. 1).* Since then, "we have been scratching our heads, but we have not lobbied for change," says Stamer, who is with the Glast, Phillips & Murray law firm.

"That the CE [could be] held liable criminally if an employee does something wrong, but that person isn't also held liable is troublesome," Stamer continues. "Under many agreements, the remedy is basically [to fire them]. It's not a very effective remedy for somebody who is violating the law or selling services, but the government is not making a conscientious effort to control them. I think CEs are resentful that these associates can [provide] their services but not be held accountable."

"There are a number of pluses and minuses here, depending on which side of the industry you're coming from," says Susan A. Miller, J.D., a Boston attorney. "I think it puts teeth in HIPAA enforcement….that's part of the goal. The industry has been asking [lawmakers] for a long time to enlarge the scope, and this does that. It puts everybody in the CE pool. I think the current CEs would think that's a plus, but others would not," she says.

Many organizations that are not CEs have been claiming that they are living up to HIPAA privacy and security regulations, and "some are already community members. For others, this would be the first time that they would have to live up to the same regulations," says Miller, who has her own legal practice.

Patients Could Delete Info From Files

Patients have had the power to make amendments to their medical files, but the Health Information Privacy and Security Act also would give them the power to delete information. "It clearly states that a patient can delete information from their medical records," Miller says. "In most states, they can't do that. They can say, 'This is wrong and here is the new information'…They can mark it," she says. But they cannot delete it.

Another new power that patients would be given is to opt out of health information networks. "Individuals who are the subject of protected health information have the right to…exercise nondisclosure and nonuse rights (referred to in this act as 'opt-out') with respect to their protected health information, including the right to opt out of any local, regional, or nationwide health information network or system that is used by the person," the legislation says.

The advancement of electronic health records is a goal of federal and state legislators, and the requirement to get permission from every patient to participate in them is onerous, Pam Atkins, divisional director of IT and HIPAA security at Children's Health System in Birmingham, Ala., tells *RPP*.

"One of the biggest things for us from an IT standpoint is interoperability — having the data available in a timely manner, no matter where the patient goes," she says. "We share our patient population back and forth [with other facilities] now. Physicians at the receiving

facility do not always have timely access to the patient's information. That's something we are going to have to dig into," she contends. "The concern is that the process is going to slow down if we have to get permission first. I think that may take away some of the benefits of interoperability," she says.

Kathleen Street, director of corporate compliance and HIPAA privacy at Children's, says the bill's opt-out clause could open a new debate on an old topic. "We discussed in 2002 [the need for] patient authorization for treatment or payments. Now it is presented to us again five years later, and we can evaluate that again, based on what we currently know about HIPAA. It is something that we definitely need to look at, something worth re-exploring," she tells *RPP*.

So What Are Its Chances?

The bill is still in committee and had not yet been scheduled for hearings as of *RPP*'s press time. "We're probably not going to see any discussion of it over the next couple of months. Since it's not scheduled, the odds that they are going to do anything on it fast are small," says Stamer.

Street is more optimistic. "Looking at what the legislative and regulatory environment has been in 2007, and the bills the House and Senate have put out there [i.e., the Wired for Health Care Act, a bill that Kennedy also sponsors, and others]…I think this one sits quite well within the context of how we are seeing privacy and security meshed more together as we proceed more toward protecting health information in the electronic age."

However, as Miller points out, "it took us 10 years to get HIPAA with all the administrative simplification rules. But I think that this won't take as long," she adds.

Stamer says the debate has been whether lawmakers would enact health-specific legislation or whether they will come up with more generic standards for protection of information. "There is an overall federal and state recognition that the protection of information…is a critical issue," says Stamer. "And there's a recognition by many members of Congress and the enforcement arm that the mechanism for addressing that problem is to state it up front. That is the theme. I think at some point we're going to see expanding standards for privacy — what we have to do, how we have to protect it — become more consistent and become more regularized."

For more information, contact Stamer at cstamer@gpm-law.com, Street at kathleen.street@chsys.org and Miller at tmsam@aol.com. ✧

Proposed Health Privacy Bill Includes Major Changes

S. 1814's provisions would mean major changes to health information privacy and security (see story, p. 1), including the following:

◆ ***It would establish a National Office of Health Information Privacy within HHS that would be led by a director appointed by the HHS secretary.*** The office would (1) provide individuals with access to health information to which they are subject, and give them the opportunity to challenge the accuracy of that information; and (2) provide "strong and effective mechanisms" to protect against unauthorized use of PHI, among other things.

◆ ***It would require that patients be notified of health data breaches within 15 days of the breach occurring or earlier if the HHS says it is appropriate.*** Also, "the person required to provide notification under this section shall have the burden of demonstrating that all notifications were made as required under this subtitle, including evidence demonstrating the necessity of any delay."

◆ ***It would include criminal and civil penalties.*** A person could be fined up to $500,000 and sentenced to 10 years in prison if charged with selling or using protected health information (PHI) for commercial advantage or personal gain. If enacted, the law would allow the feds to establish procedures to exclude providers, researchers, insurers, employers, and schools or universities from federal health care programs if they illegally disclose PHI.

◆ ***It would require the establishment of safeguards*** to "ensure that (1) [PHI] is used or disclosed only with informed consent; (2) the categories of personnel who will have access to [PHI] are identified; (3) the feasibility of limiting access to [PHI] is considered; (4) the privacy, security and confidentiality of protected health information is maintained; (5) [PHI] is protected against any anticipated vulnerabilities to the privacy, security, or integrity of such information; and (6) [PHI] is protected against unauthorized access, use, or misuse of such information."

PRIVACY BRIEFS

◆ **Security services provider SecureWorks says it has seen a 57% increase in the number of attempted attacks on its health care clients by online hackers in the first half of 2007.** The company studied 40 of its health care clients (out of 70 total) over one year and found that attacks increased from an average of 5,900 per client per day in the last half of 2006 to 9,300 per client per day in the first half of 2007. "While the financial industry has been audited for many years to ensure that appropriate security practices were in place, the health care community has not been subjected to the same regulatory inspection," says Wayne Haber, director of development for SecurWorks, in a prepared statement. "While it isn't clear whether there will be a trend of audits, it is clear that the health care organizations need to raise the bar to ensure that they can defend themselves against increased attack volumes and more lethal attack types," says Haber, who is also the Healthcare Information and Management Systems Society (HIMSS) security special interest group chairman. Read more at www.secureworks.com.

◆ **Boxes of research study records from the Walter Reed Army Institute of Research (WRAIR) that should have been shredded were found in a trash bin,** the *Washington Post* reported on Aug. 21. Officials are investigating what information the documents actually contained and why they were found in the trash, says the Post. No foul play is suspected. The records were from the late 1990s and were found by a resident, according to the newspaper. WRAIR is a Department of Defense biomedical research facility located in Maryland. A WRAIR spokesman could not be reached before the *RPP* deadline. Visit www.washingtonpost.com.

◆ **Privacy Rights Clearinghouse (PRC), a nonprofit consumer advocacy group, is suing Albertsons, the owner of supermarkets and pharmacies in 33 states, because PRC says the company violates consumers' privacy,** PRC announced July 30. Albertsons became part of SuperValu Inc. in 2006, according to the company's Web site. The company allegedly converts prescription information into a database and "does not inform the customer's doctor about what it is doing," PRC says in a statement. "The database allows [the company] to personally identify you by name, telephone number, address and drugs prescribed," PRC says. "This allows communications to be sent based on your medical condition as implied by the information in your prescription. [The company] developed a highly profitable business this way, filling more than 100 million prescriptions a year, based on your confidential information combined with your name and address," it adds. A spokesperson for SuperValu could not be reached for comment. Visit www.privacyrights.org.

◆ **Small- to medium-sized hospitals can achieve advancement in information technology capabilities just as well as complex academic medical centers,** says a new report by HIMSS Analytics, HIMSS's health IT market research firm. HIMSS studied six hospitals that have implemented fully automated electronic medical records (EMRs) and looked at their governance, investment, staffing and accomplishments, HIMSS says. All of the hospitals, which are of varying sizes, have been given Stage 6 status on HIMSS's Electronic Medical Records Adoption Model (EMRAM), meaning that they are able to handle HIPAA claims attachments, pay for performance and government quality reporting programs, HIMSS says. Read "Stage 6 Hospitals, The Journey and the Accomplishments," at www.himssanalytics.org.

◆ **HIMSS's Office of Government Relations has updated its Federal Legislation Crosswalk, which gives details on health care legislation pending in Congress,** the organization said on Aug. 16. "With 11 pieces of health care IT legislation now under consideration by the 110th Congress, HIMSS evaluates the specifics of each bill in the Crosswalk," HIMSS says. The Crosswalk's tracking tool can compare and contrast aspects of provisions of different bills, the organization says. Visit www.himss.org/advocacy/FedCrosswalk.htm.

◆ **The North Carolina Healthcare Information and Communications Alliance (NCHICA) released a security policy template for managing sensitive information on portable devices,** it said on Aug. 14. It includes policies, standards and procedures for protecting information when using devices such as PDAs, USB drives and laptops outside of an entity's "fixed security and firewall protections." NCHICA is a nonprofit consortium of health care, research and information technology organizations. Read the template at www.nchica.org.

PRIVACY BRIEFS (continued)

◆ **Park Nicollet Clinic in Minneapolis has suspended more than 100 employees this year for peeking at electronic records of their friends or relatives, among other patient privacy concerns,** according to a report in the *Star Tribune*. The facility told its 8,300 employees about the suspensions in July to remind them about its zero-tolerance policy, the newspaper reports. "Already, twice as many employees have been disciplined for privacy violations in 2007 than in all of 2006," Park Nicollet officials told the paper. Employees are suspended for three days without pay for violations. The majority of breaches were employees checking on friends or family, according to the Star Tribune. None of the breaches involved celebrities. In one case, someone looked at a co-worker's file, and in another, the employee altered his/her own record, the newspaper reports. A Park Nicollet spokesman would not discuss the suspensions with *RPP*. Visit www.startribune.com.

◆ **State Medicaid agencies have made progress developing health information technology (HIT) and health information exchanges (HIEs), but the HHS Office of Inspector General (OIG) says in a new report (OEI-02-06-00270) that privacy and security should still be a priority**. Through surveys and interviews of the 52 Medicaid agencies, OIG learned that 12 have implemented a variety of HIT initiatives, including e-prescribing, remote disease monitoring and personal health records. Many of the other states are in the process of developing these programs, OIG says. Also, 25 state agencies are now planning and developing statewide HIE networks that will create infrastructures so most providers and payers in a state can exchange clinical information. Finally, 13 states have included the Medicaid Information Technology Architecture (MITA) as part of their HIT planning. CMS developed MITA to help states modernize their Medicaid information systems, OIG explains. The report says CMS should (1) continue to support MITA to facilitate states' HIT and HIE initiatives, (2) work with other federal agencies to assist states in developing privacy and security policies, and (3) continue to ensure the states' programs are in line with national goals. CMS agreed with all of the recommendations. Visit AIS's Government Resources at the Compliance Channel at www.AISHealth.com; click on "OIG Office of Evaluation and Inspections."

◆ **Highmark Blue Cross Blue Shield says it has added more security to its Web site as protection for members' online health information.** Highmark members now need a personal identification number (PIN) in order to access their information, the company says. New members will choose their user identification and password to log in to the member portal, but they will only be able to see "non-personal content" about cost and quality, the insurer says. Visit www.highmarkbcbs.com.

Are You Now Reading a Photocopy, Fax or Unauthorized E-mail?

On an *occasional* basis, it is okay for you to copy, fax or e-mail an article or two from *Report on Patient Privacy.* But it violates federal law to make copies of or fax an entire issue, post newsletter content on any Web site or intranet, or transmit it by e-mail without our permission, whether it is for internal use, other offices, clients or meetings. It's also illegal to *regularly* copy, post on the Web or otherwise distribute portions of *Report on Patient Privacy,* or republish, repackage or summarize its contents.

CCC Digital Participation Discontinued. AIS no longer participates in the Copyright Clearance Center's digital program, which means that CCC users who renew their annual CCC contracts after October 2006 are no longer permitted to redistribute portions of AIS newsletters electronically.

If you need to make a few copies of *Report on Patient Privacy* (or get a few back issues) at no charge, or you'd like to review our *very* reasonable rates for bulk subscriptions, site licenses or electronic delivery, please call AIS's Bailey Sterrett at 800-521-4323.

Federal copyright laws provide for statutory damages of up to $150,000 for *each* issue infringed, plus legal fees. Several recent newsletter copyright cases have involved *very* large settlements and court awards, and AIS itself has recently settled several significant infringement cases.

AIS will pay a $10,000 reward to persons with evidence of illegal copying, e-mail transmittal or Web posting of *Report on Patient Privacy* that leads to a satisfactory prosecution or settlement. Confidentiality will be ensured. Information on potential violations should be reported in strict confidence to Richard Biehl, AIS publisher, at 800-521-4323, or AIS's copyright counsel Tom Curley at 202- 508-1125.

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

(1) Call us at **800-521-4323**

(2) Fax the order form on page 2 to **202-331-9542**

(3) Visit **www.AISHealth.com** and click on "Shop at the AIS MarketPlace"

If You Are a Subscriber And Want to Routinely Forward this E-mail Edition 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 e-mail editions without prior authorization from AIS, since strict copyright restrictions apply.)