Report on PATIENT PRIVACY

Scroll down to read the current issue of *Report on Patient Privacy* — or access it at your subscriber-only Web page, http://aishealth.com/newsletters/reportonpatientprivacy

Report on
Patient Privacy

Volume 15, Number 7 • July 2015

Practical News and Strategies for Complying With HIPAA

Contents

3 Regs, OCR Are Mostly Mum on Subcontractors

5 To Report or Not to Report: When Should an Incident Be Disclosed?

6 What Is a 'Breach'?

7 Q&A: IT Expert Explains How CEs Can Build Effective Cybersecurity

8 New OCR Deputy Director Has Great 'Wealth of Experience'

9 Patient Privacy Court Case

11 Privacy Briefs

Thanks to Whistle-Blowing Employee, UC Irvine Notifies Nearly 5,000 of Breach

In the last few months, the protected health information (PHI) of a staggering number of patients has been accessed, thanks to "sophisticated cyber attacks" perpetrated by hackers, perhaps working for the Chinese government. First, Anthem, Inc. gave notice on Feb. 5 that some 80 million records had been breached *(RPP 3/15, p. 1)*. Premera Blue Cross followed suit on March 17, with 11 million records at issue *(RPP 4/15, p. 1)*. Then, on May 20, CareFirst BlueCross BlueShield added another 1.1 million to the pot *(RPP 6/15, p. 1)*.

In June, the hits kept on coming. The Office of Personnel Management reported databases with records for up to 14 million federal workers, including medical and other information collected for security clearances and background investigations, had been breached, a situation so alarming it merited four hearings on Capitol Hill, of which one was conducted for members of Congress privately.

But lest covered entities (CEs) and business associates (BAs) get the impression that only mountains of electronic information are at risk and begin to ignore the more commonplace breaches, they can look to a new breach reported by the University of California Irvine (UCI) Medical Center to remind them, once again, that employees with legitimate access to PHI are often the weakest link in the security chain.

The other lesson from the UCI breach is the converse — that compliance-minded employees can be a CE's strongest safeguard against data loss.

continued on p. 10

CEs Should Take Steps to Assure Business Associates Oversee Their Subcontractors

No covered entity is an island.

Covered entities (CEs) collect and share protected health information (PHI) thousands if not millions of times a day, depending on their size. PHI is constantly flowing among CEs and their partners in health care, namely business associates (BAs) and subcontractors.

But for most CEs, figuring out whether all the BAs and subcontractors are properly safeguarding PHI and complying with the relevant HIPAA requirements can be a near-impossible task. Yet it's one they ignore at their peril.

The use of subcontractors seems to be growing, particularly among large projects that may involve many BAs, such as an upgrade to an electronic medical records system. These complicated situations can cause a CE to feel like a part of "Who's on First?" the old Abbott and Costello routine about the confusing names of players on a baseball team, says Phyllis Patrick, president of Phyllis A. Patrick & Associates.

The Office for Civil Rights has not addressed the issue of subcontractors and its regulations do not say much about them, which may add to the confusion (see story, p. 3). Patrick spoke about subcontractors at the recent 21st Annual HIPAA Summit and in an interview with *RPP*.

continued

As she explains, business associates may use any number of workers who technically fall into the category of subcontractors by virtue of their relationship to the BAs. These organizations and individuals may be called various other names, including vendors, consultants, independent contractors, temps and advisors. They might be nurses, pharmacists, home health workers or IT professionals.

Some of these folks may be "lone rangers" who work in one place only for a short period of time or perhaps a few years at a stretch, Patrick notes. Small firms, of course, may also work for BAs as subcontractors.

Not All Requirements Apply

But CEs may be pleasantly surprised; Patrick says that, on occasion, she has actually found a subcontractor to be more HIPAA "savvy" and sophisticated about privacy and security than the BA it is working for.

She also sees a lot of confusion over who is a BA versus who is a subcontractor, and says this is more than a distinction without a difference. Although all must comply with HIPAA generally, not all requirements are applicable, and CEs need to understand where to focus their oversight.

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, Theresa Defino; Executive Editor, Jill Brown; Associate Editor, Lauren Clason; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Tracey Filar Atwood; Production Director, Andrea Gudeon

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.AISHealth.com that include a searchable database of *RPP* content and archives of past issues.

To order an annual subscription to **Report on Patient Privacy** ($524 bill me; $494 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Subscribers to *RPP* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

"You have to go through every standard and document why it does or does not apply" to a particular subcontractor, she says. For example, a subcontractor that doesn't hold any information electronically wouldn't necessarily have a process for reporting security incidents.

Sometimes the BA's subcontractor actually becomes more like a member of the CE's workforce than the BA itself, by virtue of working at the CE's location. This situation raises the stakes considerably for CEs.

IT firms may use a number of subcontractors, especially because specialized skills are in short supply and the personnel can sometimes make more money as contractors than employees. Many may dislike the idea of being an employee, even though as a contractor they might be on a job for a CE for two years at a stretch, especially if they are assigned to a large project.

Some may not have a health care background and could be working for a HIPAA CE for the first time in their careers.

CEs should be working with their BAs and asking them a series of questions to learn what they can about their use of subcontractors, to better assure that BAs are keeping tabs on their subcontractors. Patrick adds that she doesn't "know of any CEs that are talking to subcontractors" directly.

Armed with this information, CEs can focus their oversight of BAs on subcontractor areas of concern, which include training, risk analysis, access management and use of equipment.

Business Associates May Have Many Subs

CEs need to be clear about "the subcontractor's role in the compliance chain." They often are "lumped" in with BAs but they are not the same, she adds.

"Basically, everybody is using subcontractors to some extent," says Patrick. "It's not unusual to go into, especially a large health system today...and find a number of individuals who are, in fact, subcontractors."

Patrick recommends that CEs, if possible, obtain a list of the BA's subcontractors and that they forbid the blanket use of off-shore subcontractors. Instead, CEs should require the BA to submit any potential off-shore subcontractors for approval.

Although subcontractors are required to conduct a risk assessment, as are BAs, Patrick does not think CEs should ask to see either. These are proprietary documents, she says, and assuming they reveal vulnerabilities, must be safeguarded.

It may be sufficient to request subcontractors' policies on risk assessments, to understand how often these are done and their scope, as well as the date of the most

recent one. Policies should also identify how the findings of assessments will be corrected.

Because so many breaches occur when laptops and other mobile devices are lost or stolen, addressing how subcontractors handle equipment is essential, says Patrick.

Patrick was recently involved in advising a BA that was insisting subcontractors use their own equipment, which she thought was a bad idea that was only pursued as a cost-saving measure. But the loss of a subcontractor's private laptop that leads to a reportable breach would likely be more costly, she points out.

Instead, she advises subcontractors to have a "virtual machine," such as a tablet or Chromebook with no hard drive for storage and no ability to download or print. The purpose is to allow contractors access to the system, but all work they do is within the system. And if that device is lost, "there shouldn't be anything on it," Patrick adds.

CEs also need to be prepared to react to circumstances that arise with subcontractors. What happens, she asks, when a subcontractor "is showing up with a laptop that's not properly configured, or it's not the one that's supposed to be used?"

BAs, of course, have business associate agreements (BAAs) with CEs. But what do they have with subcontractors? Patrick says they can use a version of their BAA, which she argues really should not be a stand-alone document but an addendum to a contract that describes the scope of work and other duties the subcontractor will perform in addition to its HIPAA obligations.

The BAA with the subcontract must address notifications in the event of a breach or other incident. The breach notification regulation requires CEs to notify affected patients, OCR and the media (if more than 500 individuals are involved) within 60 days of discovery of a breach.

continued

Regs, OCR Are Mostly Mum on Subcontractors

To a HIPAA covered entity (CE), subcontractors are individuals or firms that work for business associates (BAs), who, in turn, are working for the CE.

The HHS Office for Civil Rights (OCR) first introduced the concept of HIPAA compliance by subcontractors in proposed regulations issued in 2010 to comply with the 2009 HITECH Act. This was a surprising move at the time *(RPP 8/10, p. 1)*.

Not only did OCR not stray from this concept on Jan. 25, 2013, when it issued a quartet of final regulations, the agency actually expanded the definition of "business associate" to include cloud and other storage companies previously not under HIPAA.

The regulations say little about subcontractors, however, and OCR has not opined about them since 2013. As a result, HIPAA organizations are on their own when it comes to corralling subcontractors, some of whom operate as a "lone wolf," says Phyllis Patrick, president of Phyllis A. Patrick & Associates, a longtime HIPAA consulting firm.

Final Reg Modified Definitions

Subcontractors (and BAs) have been required to comply with relevant parts of the privacy, security and breach notification regulations since the regulations went into effect in September 2013. They are both addressed in Section 160.103 of the final regulations.

Under the proposed regulations, a "business associate" was defined as a "person" who "on behalf" of a CE but not as a member of its workforce, "performs or assists in the performance of a function or activity involving the use or disclosure of PHI."

The proposed rules offered examples of functions, such as "claims processing or administration, data analysis, processing or administration, utilization review, quality assurance," etc.

OCR modified the definition in the final regulations, dropping the words "performs" and "assists" and stating instead "creates, receives, maintains or transmits" PHI "for a function or activity regulated by this subchapter." It then restates the examples of functions.

The agency also revised the definition of "subcontractor" in the final regulation. Under the proposed rules, it was "a person who acts on behalf of a business associate" and is not a member of the BA's workforce."

The final rules define a "subcontractor" as "a person to whom a business associate delegates a function, activity or service," and as before, is not a workforce member.

In the preamble to final omnibus regulations, OCR states that officials "believe that making subcontractors directly liable for violations of the applicable provisions of the HIPAA Rules will help to alleviate concern on the part of covered entities that protected health information is not adequately protected when provided to subcontractors."

continued

BAs that experience a breach must report it earlier than 60 days so the CE can make the notification on time. This must flow down to the subcontractor, who will have its own deadline to notify the BA.

The time prior to reporting a breach is used to investigate the situation, implement mediation strategies if possible, assemble a package of services and a notification letter and related activities. CEs, which typically make the public announcement of a breach, need to learn about a breach as early as possible to set this in motion.

Because there are two layers to go through, some BAs require contractors to notify BAs within 24 or 48 hours of learning of a breach, Patrick says.

She adds that subcontractor agreements also need to spell out how the costs will be covered if there is a breach.

One area that CEs might easily overlook is training for subcontractors. These organizations are required to train their workers, but whether that training is adequate — or comports with what the CE thinks is important — might be pure conjecture.

In Patrick's view, subcontractors need to be trained in policies and procedures of both the BA and the CE. The latter is especially necessary when the subcontractor is working on site at the CE's location.

Regs, OCR Are Mostly Mum on Subcontractors (continued)

Further, OCR clarified that "under the final rule, covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far 'down the chain' the information flows."

Sample BAA Barely Mentions Subcontractors

When the regulations were published, Lisa Sotto, who heads the privacy and information management practice for the New York-based law firm of Hunton & Williams, LLP, predicted that this "downstream application of HIPAA, particularly with regard to subcontractors," would be "an unmitigated disaster" *(RPP 2/13, p. 1)*.

It was hoped that OCR would help the situation, and the agency promised to issue guidance that would assist BAs and subcontractors, who are often small and new to HIPAA. That has not happened. OCR made four brief mentions of subcontractors among the "Sample Business Associate Agreement (BAA) Provisions" posted on its website when the regulations were published in 2013.

Business associate agreements are forged between CEs and BAs to establish their roles and responsibilities when it comes to HIPAA compliance. OCR stipulates 10 "musts" to be included, such as "(2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law."

Subcontractors come in at (9) and (10). These state that the BAA must "require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information" and "authorize termination of the contract by the covered entity if the business associate violates a material term of the contract." OCR adds that "Contracts between business associates and business associates that are subcontractors are subject to these same requirements."

In providing sample language, OCR says the BAA may state the following:

"In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information."

Finally, OCR notes, in brackets as if an afterthought: "The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors."

Ensuring compliance with some of the requirements also hinges on whether the BA or subcontractor has too much PHI and is using it for purposes that go beyond the BAA, which would be a violation of the long-standing minimum necessary standard, among others.

But OCR hasn't shed light on the oft-misunderstood concept of "minimum necessary," failing to issue the guidance Congress required it to publish five years ago.

Of significance is assuring that subcontractors know how to recognize a violation of policies, including how to report a suspicious incident.

CEs may even want to include subcontractors in training sessions or, if available, make online programs accessible to them.

When the final regulations mentioning subcontractors were published, Lisa Sotto, who heads the privacy and information management practice for the New York-based law firm of Hunton & Williams, LLP, predicted that this "downstream application of HIPAA, particularly with regard to subcontractors" would be "an unmitigated disaster" *(RPP 2/13, p. 1)*.

She tells *RPP* now that it's been "years" since any clients asked her about subcontractors, and says lack of enforcement by OCR regarding BAs and subcontractors could cause CEs to take the path of "business as usual."

Sotto cautions that CEs and BAs "have a legal obligation to be in compliance now" regardless of whether OCR has come down on them. CEs and BAs, in particular, need to be engaged in "due diligence" when it comes to subcontractors, Sotto says.

While it is difficult to assess the level of compliance among subcontractors, Sotto suggests it is at least greater than before the final regulations went into effect.

If BAAs are revised as required to address subcontractors, their duties get "baked in," Sotto says. "Frankly, there's less angst over [subcontractors] as time has gone on, and in the absence of OCR actions."

Particularly large CEs "definitely don't know and they can't know" every time a BA places a subcontractor on site. CEs "have to rely on BAs" to assure compliance by their subcontractors, which makes it all the more important that CEs keep tabs on their BAs, says Sotto.

Contact phyllis@phyllispatrick.com and Sotto at lsotto@hunton.com. ✧

To Report or Not to Report: When Should an Incident Be Disclosed?

"To report or not to report?" can be a tricky question for covered entities (CEs) when they're faced with a potential security incident involving protected health information (PHI). While HIPAA provides a four-step assessment to determine whether or not a suspected breach should be reported to the Office for Civil Rights (see box, p. 6), that doesn't mean each incident comes stamped with a clear-cut answer.

In May 2013, Idaho State University (ISU) settled with OCR for $400,000 after discovering a firewall protecting a cache of more than 17,000 patient records at several of its clinics had been down for 10 months. ISU determined in August 2011 that IT workers had failed to reactivate the server's firewall following routine maintenance on the system. Even though a forensic analysis by an outside firm determined that no PHI had been accessed, university officials alerted HHS anyway, a case in which an abundance of caution may have led to more discipline than the CE expected. The ensuing federal investigation alleged a string of shortcomings in ISU's data security practices, including:

(1) A failure to conduct an appropriate risk analysis from April 1, 2007, to Nov. 26, 2012;

(2) A failure to implement sufficient security measures to reduce risk in the same time period; and

(3) A failure to review PHI activity on a regular basis from April 1, 2007, to June 6, 2012.

Failure to Report Can Have Bad Consequences

The violations could have cost ISU $3.9 million had the university not settled, according to Bob Chaput, CEO and founder of the Tennessee-based consultancy Clearwater Compliance. But, Chaput tells *RPP*, when in doubt, report. The charges OCR would bring forth otherwise are "absolutely, unequivocally" harsher.

"If you screw up and don't follow what's required under the breach notification rule, you may have a series of other issues that they get you for: not having done a risk analysis, not having security officials in place, not having good policies and procedures, boom boom boom boom boom," Chaput says. "But additionally, you're going to get dinged for not taking the action you were supposed to under the breach notification rule."

Of course, there is the chance OCR won't discover an unreported data breach, as many privacy experts point out. But there's also the chance it will. For one company still under investigation, a cyberattack affecting 200,000 records resulted in 21 alleged violations of the three HIPAA rules: 15 security rule violations, three privacy rule problems, and three breach notification rule violations. But even in instances such as these, Kirk Nahra, a privacy lawyer and partner at Washington, D.C.-based Wiley Rein LLP, contends that too little data exist to predict OCR's behavior, for a number of reasons.

OCR Is 'Appropriately Reasonable'

"One is that OCR is appropriately reasonable in all situations," Nahra says. "So whether it's a breach or it's something else, if you made a good-faith decision to do or not do something and they don't end up agreeing, as long as you were thoughtful about it and it wasn't the 92nd time it happened, they're generally pretty good about that."

Determining whether to report a breach can involve more than just technical factors; reporting could also

potentially bring more harm to the affected individuals. A county in North Carolina recently was faced with a tough decision after finding a breach of a section in its Medicaid database devoted to pregnant women with sexually transmitted diseases. Because the breach had occurred three years prior to its discovery, and because the county had no evidence the information had been accessed, reporting the breach could have further jeopardized the privacy of the beneficiaries, especially since HIPAA requires the CE to alert local media outlets.

The unknown factors of a data breach are oftentimes what cause CEs to pause in evaluating the situation under the terms of the four-step assessment. "Any kind of lost or missing information is a toss-up," Nahra says. "If someone leaves a document on the subway, the most likely scenario is that maintenance picked it up and threw it out." But because that can't be proven, the CE is left to make a judgment call.

Assessments Provide CEs With Guidance

At least one expert, David Holtzman, vice president of compliance for the audit firm CynergisTek, Inc., believes the assessment provides all the necessary guidance CEs need. If an employee temporarily loses an unencrypted laptop but recovers it shortly thereafter, for instance, the situation could indeed qualify as a reportable breach.

"The definitions of terms that are used in the breach notification rule are derived from those that apply to the privacy rule," Holtzman says. "For purposes of the privacy rule, 'access' is the loss of control of the information or in this case, the unencrypted device on which the information is disclosed. The fact that the covered entity believed they lost control of the unencrypted laptop would constitute access under the privacy rule."

But other experts say there's a lack of clarity in some of those definitions and how CEs are meant to use them in their evaluations.

"How do you actually quantifiably review those four factors?" asks Adam Greene, a privacy lawyer and partner at D.C.-based David Wright Tremaine LLP. "Do each of them get the same weight? Is there a potential that three factors could be high risk, but the fourth factor could be so strong that it overall leads to a low probability of compromise?"

Document Your Review of the Four Factors

The best solution, regardless of a CE's decision, is to document all the reasons behind it. Greene cites former OCR Director Leon Rodriguez's mantra that HIPAA compliance is similar to fifth-grade math. You don't get credit for a correct answer so much as you do for showing your work.

"What's most important is that you have strong documentation that you addressed at least the four factors and that you apply your methodology as consistently and as objectively as you can," Greene says.

Contact Chaput at bob.chaput@clearwatercompliance.com, Greene at adamgreene@dwt.com, Holtzman at david.holtzman@cynergistek.com and Nahra at knahra@wileyrein.com. ✧

What Is a 'Breach'?

According to 45 CFR §164.402, a "breach" is defined as follows:

"[A]n acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

"(1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

"(2) The unauthorized person who used the protected health information or to whom the disclosure was made;

"(3) Whether the protected health information was actually acquired or viewed; and

"(4) The extent to which the risk to the protected health information has been mitigated."

Three Exceptions Are Provided

But the unauthorized use or disclosure is not a "breach" if the PHI is properly secured or the breach falls into one of these exceptions:

(1) Unintentional acquisition, access, or use of PHI by a workforce member as long as the disclosure was made in good faith and within the scope of authority and does not result in further unauthorized use or disclosure.

(2) Inadvertent disclosure by one person at a covered entity or business associate who is not a member of the workforce but is authorized to access PHI (e.g., a physician) to another person authorized to access different PHI at the same covered entity, as long as the PHI is not again used or disclosed without authorization.

(3) A good faith belief that the unauthorized recipient of the information would not have reasonably been able to retain the information.

Q&A: IT Expert Explains How CEs Can Build Effective Cybersecurity

In the game of cybersecurity, "sophisticated" hackers — as scores of compromised companies have called them — seem to have the upper hand on health care companies that often underfund security and relegate their security strategies to the back burner. But as costly data breaches continue to make headlines, the industry is slowly realizing that cyber-monitoring is a full-time job. Fred Cox, CEO and managing director of the Florida-based IT security firm FDC Associates, answered for RPP *some of the technical questions related to a covered entity's cybersecurity policies and practices.*

RPP: What is the difference between HIPAA compliance and protecting your organization from a cyberattack?

Cox: HIPAA compliance tends to be the least you can do to protect your firm from a cyberattack. For instance, HIPAA requires you to authenticate your users, and you can satisfy this requirement with single-factor authentication — "something you know" — such as a user ID and password. However, two-factor authentication is a far stronger method of ensuring that the person is who they say they are. Two-factor is not a requirement for HIPAA, at least not yet, but it is a much more robust method of authenticating someone and it will prevent a breach in many instances, because the attacker may have obtained someone's user ID and password but does not have the token or cellular phone — the "something you have" — required as the second factor.

RPP: Do you expect two-factor authentication to be a requirement in the foreseeable future? What other security enhancements do you expect eventually will be mandated?

Cox: Two-factor authentication is very likely to be a requirement in the next five years, particularly for systems that handle financial or health care data. It is already a requirement in financial systems when funds are transferred. Two-factor authentication won't prevent the theft of credentials, but it will go a long way in preventing the fraudulent re-use of those credentials. For instance, the Target and Anthem breaches would not have occurred if those firms had used two-factor authentication. The other technology that is very likely to be required in the next five years is "true" data leak prevention (DLP) software — meaning those software tools that can identify electronic protected health information (ePHI) in data packets that are outbound from the client's infrastructure and stop, or at least suspend, the outbound data flow until reviewed by a human being.

RPP: What authentication strategies do you recommend for confirming your users are who they say they are?

Cox: In today's high-risk environment, I strongly recommend using an out-of-band (OOB) two-factor authentication approach and tool. For instance, Microsoft's Azure Multi-Factor Authentication (MFA) uses the user's cell phone as the "something you have" two-factor. First, you input your user's phone numbers. Then, when they try to log on with their user ID and password, their phone rings. Azure expects a prearranged response, like the user keying the "#" key within 20 seconds of the ring. This means that even with a workstation that has a keyboard logger virus or compromised Internet browser, an OOB solution can still be used to authenticate the user, and the hacker still cannot log on because they do not have the user's cell phone. As an additional benefit, the OOB cell phone approach tells the user when it is time to change a password; when their phone rings as part of an attempted log-on and the owner did not initiate the log-on, then the owner knows that someone else knows their password.

RPP: What data leak prevention tools would you recommend?

Cox: DLP tools that are recommended are those tools that can "fingerprint" data elements, which you can then use to identify when ePHI data are stored on your infrastructure, or when they are being transported off your network. Typically, a data leak provider like Code Green offers a hashing algorithm software tool that you can point at the file or database that stores your ePHI, and, by using two data elements (you can use more if you wish), like a patient's name and their medical record number, you can create hash values, or numerical representations, of these data elements. Then, you can scan your network and workstation hard drives (I scan the backup copies of these hard drives) and create hash values of any patient name/medical record number that you find, comparing the hash values to the hashes you know represent ePHI. When these two hash values are equal, you know you have discovered ePHI data. This hash value can be used by your DLP provider to scan the outbound data packets for ePHI. Again, when you find hash values that are outbound, you know that ePHI data is leaving your network and you can then stop the outbound data flow, thus detecting and stopping a breach in progress.

RPP: What tactics will help recognize an atypical workflow?

Cox: Early on, a firm called Fair Warning created an activity log parser software tool to help see who has accessed someone's ePHI. However, several other firms, as well as Fair Warning, like Securonix or Iatric, have created software that creates or defines what a normal workflow is for a user's access role category, and then can tell us when this ID is not acting in the "normal" workflow. This is very helpful because all data breach events are the

result of an atypical work flow. This behavioral approach is a much faster and cost-effective way to find the needle in the haystack.

RPP: What is a layered security strategy and how can it prevent a single control point of failure?

Cox: Each security layer is there not only to protect but also to compensate in the event another layer or control fails. For instance, when you deploy a DLP data egress scanner control — which scans outbound data packets for ePHI and verifies the person sending and receiving it — you are creating a second layer of control. Your first layer of controls is the firewall that hopefully only permits authorized parties to have access to your infrastructure. However, if your firewall fails, or if your antivirus fails, then the second layer, your DLP egress filter, stops the data from leaving your network. Upon examination of the suspense bucket — where the filter will hold potentially invalid or dangerous transactions — and warning messages, you discover that one of your control layers has failed and must be repaired. But because of your layered control design, a data breach has not occurred.

RPP: How does one deploy real-time telecom perimeter software to assure firewall integrity?

Cox: When you deploy real-time telecom perimeter software to evaluate each addition or change to your telecom perimeter, you are in effect creating a real-time Internet vulnerability test when any change is made. This greatly increases the integrity of your protection since, should your network telecom or firewall engineer make a change and not be aware that their new firewall rule creates an opening that a hacker could use to gain access, the telecom perimeter analysis software would very likely detect that this change opens the firewall up to attack and would let the engineer know that the change creates a vulnerability. This vulnerability can then be corrected for and eliminated at that moment in time, rather than waiting until your next vulnerability test.

Contact Cox at fcox@fdcassociates.com. ✧

New OCR Deputy Director Has Great 'Wealth of Experience'

Deven McGraw is so closely identified with HIPAA that her handle on Twitter is simply @HealthPrivacy. It was through Twitter the world learned that McGraw, an attorney with a masters of public health who later developed a specialty in health IT and security, would be joining the HHS Office for Civil Rights (OCR) as its new deputy director for health information privacy.

Like the speed that characterizes Twitter, McGraw was on the job at HHS just a week after OCR Director Jocelyn Samuels announced her appointment, and McGraw went straight from her position as a partner with Manatt, Phelps & Phillips, LLP on a Friday and began her new job on Monday, June 29.

"That's the kind of person she is," says John Halamka, chief information security officer for Beth Israel Deaconess Medical Center, who calls McGraw's selection "a great appointment." McGraw "wants to make a difference; she wants to make an impact. She is not a person who seeks fame and fortune," he tells *RPP*.

And it may come as good news to some that McGraw was among the biggest opponents of OCR's much-maligned accounting of disclosures regulation, published in proposed form in May 2011 but never finalized.

Halamka knows McGraw well, having served beside her on government advisory committees, collaborated with her on papers, and, as he puts it, "shared the podium" with McGraw as both are frequent public speakers. He called her "a great thinker" whose greatest asset is that she understands the balance that needs to be struck when ensuring both patient privacy and patient access to protected health information (PHI) amid the practicalities of health care operations.

While the move to OCR makes perfect sense for McGraw, Halamka was surprised to learn of it. He tells *RPP* the two of them had just finished coauthoring a paper reviewing 20 years under HIPAA when her appointment was announced, and McGraw hadn't mentioned her impending move.

Post Brings Stability, Energy

In naming McGraw, OCR Director Jocelyn Samuels puts in place her No. 1 privacy person in a post that has been vacant, and she does so with a known quantity. Samuels herself was new to health care and the HIPAA community when she started last July, having come from the Department of Justice's Office for Civil Rights.

McGraw joined Manatt in April 2014 as co-chair of the firm's privacy and data security practice. Previously she was director of the Health Privacy Project at the Center for Democracy and Technology.

When Samuels was named, McGraw told *RPP* she knew Samuels because she had been chief operating officer of the National Partnership for Women & Families when Samuels was at the National Women's Law Center. At the time, McGraw called Samuels "smart, savvy and hardworking" *(RPP 8/14, p. 5)*.

The post McGraw fills has been vacant since the May 2, 2014, retirement of longtime OCR official Sue McAndrew *(RPP 5/14, p. 1)*, whose departure came amid a period of tumult at the top of OCR and at HHS itself. In January 2014, then director Leon Rodriguez was tapped as director of the United States Citizenship and Immigration Services and confirmed by the Senate on June 24. During this time, the rocky implementation of Healthcare.gov and the maiden open enrollment period concluded, with the resignation of HHS Secretary Kathleen Sebelius.

In announcing McGraw's selection, OCR said she "will spearhead OCR's policy, enforcement, and outreach efforts on the HIPAA Privacy, Security, and Breach Notification Rules." The statement noted she is a "well-respected privacy expert" who "comes to OCR with a wealth of experience in both the private sector and the nonprofit advocacy world."

McGraw could also be a reenergizing force at OCR. Samuels, who came to OCR admittedly new to HIPAA and the health care community, has not proven to be a dynamic public speaker, but, in her defense, there hasn't been much to be dynamic about. OCR has not issued regulations or substantive guidance in some time, and makes only a few enforcement settlement agreements per year.

Rodriguez "did a lot of presentations," Halamka says. "When Leon was the director, I felt there was great activism [at OCR]. Since he left I haven't seen as much."

OCR Audits Should Resume Soon

The most significant project at OCR, from the perspective of HIPAA CEs, is resumption of the audit program. Phase II was initially planned to be onsite and was expected to include business associates (BAs) for the first time. OCR officials have been saying the audits were going to begin "soon" for the past two years, a statement that Samuels herself recently repeated to *RPP* recently *(RPP 4/15, p. 5)*.

The audits have been scaled back to "desk audits," which generally involve a paper review of policies and procedures. The audit program was supposed to start in 2013 but, to date, OCR has contacted only some CEs and BAs to confirm their names of officers and how they may be reached and complete a survey to collect basic information *(RPP 5/15, p. 1)*.

continued

PATIENT PRIVACY COURT CASE

This monthly column is written by Tamara Senikidze of Morgan, Lewis & Bockius LLP in Washington, D.C. 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 Tamara at tsenikidze@morganlewis.com.*

◆ **Kentucky Supreme Court permits *ex parte* physician interviews but limits disclosure of patient health information.** On June 11, the Kentucky Supreme Court opined that the state's privacy law does not limit a defendant from conducting *ex parte* interviews with a plaintiff's treating physician as part of the discovery process. However, the state Supreme Court emphasized that the physician may not disclose a patient's protected health information unless authorized by a court order in compliance with federal law. The question arose out of a medical malpractice suit in which the trial court allowed the physician's counsel to conduct *ex parte* interviews with plaintiff's physicians. According to the trial court's order, the physician's participation in the interviews was voluntary. The order also expressly directed the physicians not to disclose PHI. Caldwell, the patient and an appellant in this case, appealed the order. As a result, the state Supreme Court allowed the interviews to proceed, reiterating the ban on the physician's disclosure of PHI. As to the analysis of the federal law, the court briefly noted that among the permissible disclosures under HIPAA is the litigation exception. This exception allows for the disclosure of PHI "in the course of any judicial or administrative proceeding," either in response to a court order or in response to a subpoena, discovery request "or other lawful process." HIPAA does not expressly mention *ex parte* interviews. Therefore, the court concluded that "HIPAA doesn't forbid *ex parte* interviews, but the doctors participating in such interviews may not disclose the plaintiff's PHI unless ordered to do so by the court or pursuant to a subpoena, discovery request or other lawful process." The opinion in *Caldwell v. Chauvin*, No. 2014-SC-000390-MR, 6/11/15, is available at http://cases.justia.com/kentucky/supreme-court/2015-2014-sc-000390-mr.pdf?ts=1434031276.

Because of the tight time schedule, McGraw told *RPP* she was unable to comment on her new position. However, *RPP* has interviewed McGraw on numerous topics over the years that provide insights into her perspective on privacy and HIPAA compliance.

As co-chair of HHS's Health IT Policy Committee, McGraw pushed for recommendations that the government back off the requirement in the proposed regulation for "access reports" until it had conducted a successful pilot showing that electronic records systems had the capacity to create these reports and that they proved meaningful to patients *(RRC 12/13, p. 1)*. The committee studied the issue for several months and heard testimony from stakeholders over a two-day period.

The 2010 HITECH Act required OCR to expand existing accounting of disclosures reports to include protected health information that is used for treatment, payment and health care operations (TPO) — if the PHI resides in an electronic health record (EHR).

OCR additionally required a new access report that would give a patient a list of workforce members who had accessed PHI contained in a designated record set, a move roundly criticized as unnecessary, since few patients ever asked for an accounting; onerous, because presumably such reports needed to be created in advance of a patient request; and possibly not technologically feasible *(RPP 6/11, p. 1)*.

In addition, the policy committee recommended HHS require a "report of external disclosures," which it believed will get more to the heart of what patients really want to know about how their PHI is used, and to inform patients of their "right to an investigation of accesses inside the entity."

OCR has moved the accounting of disclosures regulation to the "long term actions" in its most recent semiannual list of regulations under development, which was published in May.

Plea to Not Overwhelm Covered Entities

When asked what advice he would give McGraw, Halamka says he urged her to consider the "entire ecosystem." He says he wrote to her that, "As you create new regulations and enforce old regulations, keep in mind the collective burden of everything that is happening."

Halamka ticks off the conversion to the ICD-10 claims system, implementation of meaningful use measurements for electronic medical records and the myriad changes and adjustments to treatment and payment required under the Affordable Care Act as among the challenges CEs face today.

David Holtzman, vice president of compliance for CynergisTek, Inc., an information security consulting firm, worked at OCR for eight years until October 2013, most recently as senior privacy and security advisor. Holtzman called McGraw "a tremendous pick and a true thought leader." His only lament was "how long it took to get her into the position."

But he points out that while Samuels, as a political appointee, will be expected to step aside when President Obama's term concludes, McGraw is under no such time constraints and "can make a real and lasting impact."

Contact Halamka at jhalamka@bidmc.harvard.edu and Holtzman at david.holtzman@cynergistek.com. ✧

UC Irvine Med Center Is Breached

continued from p. 1

The medical center's breach of nearly 5,000 records occurred because an employee "whose job required access to some patient records...looked at additional records without a job-related purpose between June 2011 and March 2015," UCI announced on June 17.

UCI reported the breach to the HHS Office for Civil Rights (OCR) on the same day as its public announcement. Under the breach rule, notification is generally required to be made to patients within 60 days of a breach being discovered.

Notification Was Delayed to Help Investigation

"The law enforcement agency investigating this breach asked us not to immediately provide patient and public notification as that may affect their investigation," John Murray, the medical center's spokesman, tells *RPP*. "In early June, they gave us the go-ahead to proceed with notification. The appropriate state and federal privacy laws permit a delay under these circumstances."

The employee, according to UCI, "may have viewed some protected health information of our patients including names, dates of birth, gender, medical record numbers, height, weight, medical center account numbers, allergy information, home address, medical documentation, diagnoses, test orders and results, medications, employment status, and the names of patient's health plans and employers."

According to the OCR website that lists breaches affecting over 500 individuals, the UCI breach involved 4,859 patients. UCI, which offered individuals one year of credit monitoring, said the employee "did not access or electronically distribute Social Security numbers, driver's licenses or state ID card numbers, or credit or debit card information," at least "as far as it is possible to determine."

In response, UCI "[r]emoved the employee's access to medical center's computer systems and imposed disciplinary actions" in March, its statement said. Murray tells

RPP the employee "no longer works for the university." He added that the UC Irvine Police Department has an open investigation into the breach.

Coworker Used Whistleblower Process

Asked how UCI learned of the breach, Murray tells *RPP* tells the snooping came to UCI's attention through another employee who reported suspicious activity through the university system's whistleblower process (see http://www.ucop.edu/uc-whistleblower).

Murray says he doesn't know "whether the staff member called the whistleblower hotline or spoke to the Locally Designated Official." UCI provides multiple avenues for employees to report "inappropriate behavior" by co-workers, he adds.

Experts recommend that covered entities have a compliance hotline so that employees can report concerns. One advantage is a hotline can be used by any employee, regardless of location *(RPP 2/08, p. 5)*.

It is not clear what the worker's motives were. UCI's outside computer forensics experts analyzed the worker's hard drive and email account but "found no evidence that this employee removed any patient information."

Investigating allegations of HIPAA violations among a CE's workforce is among the trickiest activities for compliance officials, and they must ensure inquiries are conducted objectively *(RPP 8/11, p. 4)*.

The UCI breach also underscores the value of strong access controls and the need to actively monitor employee access through audit logs. CEs also benefit from special policies that tighten access to certain kinds of patients, including celebrities, local or national politicians, accident victims and others whose treatment might prompt curious workers to snoop *(RPP 1/13, p. 1)*.

At UCI, the compliance office "maintains access logs along with the ability to track which information is viewed and by whom," Murray says. "The compliance office is strengthening its auditing of employee access to records, including more reviews of access permissions when employees move between departments or their job responsibilities change."

Contact Murray at jdmurray@uci.edu. ✧

PRIVACY BRIEFS

◆ **Maryland-based Meritus Medical Center discovered unauthorized activity by one of its vendor's employees in a routine audit,** the health system said on June 26. Meritus suspended the employee's access, but did not disclose whether an ensuing investigation resulted in the employee's termination. Accessed information included names, dates of birth, age, gender, medical record numbers, health insurance information and clinical data such as diagnoses and treatments. Visit http://tinyurl.com/pdzx2qd.

◆ **Eighty-four percent of Americans want to be notified immediately following a data breach,** according to a study released June 25 by email security vendor Zix Corp. A survey of 500 people between the ages of 18 and 75 found that the best ways for a company to regain a consumer's trust following a data loss incident are immediate notification and a "high level of contact." The study also found that 92% of respondents feel companies should be required to report all breaches to their entire customer base, rather than notifying only affected individuals. Visit http://tinyurl.com/oo7qk2q.

◆ **The information of approximately 6,600 Medicaid beneficiaries was inadvertently posted online at the Texas Department of Aging and Disability Services (DADS),** the agency said on June 11. On April 21, the department was alerted that an internal web application was accessible via the Internet. Compromised PHI included names, dates of birth, addresses, Social Security numbers, Medicaid numbers, diagnoses and treatments. DADS said it had no reason to believe the information had been misused. Visit http://tinyurl.com/qeory7u.

◆ **Blue Shield of California revealed a glitch that resulted in a data breach affecting 843 members,** *The Desert Sun* reported on June 11. Members who logged into their accounts at the same time between May 9 and May 18 were able to access each other's information. Blue Shield of California discovered the discrepancy May 18, and took the site offline in order to correct the problem. Compromised information included names, dates of birth, addresses and ID numbers. Visit http://tinyurl.com/pu572qv.

◆ **Rep. Doris Matsui (D-Calif.) on June 9 introduced legislation to clarify HIPAA rules in dealing with patients with mental illness and their caretakers and family members.** The bill would allow health care providers to share information about treatments and side effects with the patient's relatives or caregivers, but would also provide consider-

PRIVACY BRIEFS (continued)

ation for when a patient objects. The measure would also establish a model training program to teach providers how to judge when it is appropriate to share information. Visit http://tinyurl.com/orxx239.

◆ **The more than 100 pending class actions against Anthem, Inc. will be heard in the Northern District of California,** *The National Law Journal* reported on June 9. Anthem had petitioned the judicial panel to move the cases to its home in Indianapolis, where the company said it could be closer to its resources. The panel chose California based on the insurer's large presence there, and also assigned the case to U.S. District Judge Lucy Koh, who ruled in favor of data breach victims in one case last year. Visit http://tinyurl.com/q8pvspf.

◆ **Rep. Joe Wilson (R-S.C.) on June 9 introduced a bill to develop a standard measurement of cyberattacks.** The Cyberattack Standards Study Act would require the Director of National Intelligence, FBI Director, Secretary of Defense and Secretary of Homeland Security to "define a method for quantifying a cyber incident." Wilson's office in a statement said the legislation would help officials more quickly coordinate an appropriate response to cyberattacks. Visit http://tinyurl.com/oqwl9om.

◆ **Female privacy experts make $5,000 less than their male counterparts,** according to a June 9 report from the International Association of Privacy Professionals. Men were paid an average salary of $130,000, while women were paid an average salary of $125,000. That difference shrunk when comparing privacy professionals with certifications: men were paid $135,000 on average while women were paid $132,500. Women, however, were 33% more likely to occupy the C-suite than men. Visit http://tinyurl.com/ntgfeo5.

◆ **A Richmond, Ky.-based storage company inadvertently tossed thousands of medical records from a closed radiology clinic that abandoned a unit,** WTVQ reported on June 1. A man found 65 boxes of medical records from Richmond Radiology in a dumpster behind a storage facility, where the records were placed after making room for the unit's new tenant. The records, which included Social Security numbers and credit card information, were being held at Baptist Health until the clinic's former owners could be reached. Visit http://tinyurl.com/q8vxzoj.

◆ **A Metropolitan Hospital Center employee broke protocol when he sent an email to his personal account that contained PHI for nearly 4,000 patients,** New York City Health and Hospitals Corp. (HHC) said on June 1. The email was sent on Jan. 15 and discovered by the hospital on March 31. The employee's reason for the email and the type of information it contained were not disclosed. HHC said it installed software that blocks the transmission of PHI and terminated the employee. Visit http://tinyurl.com/obp4gc2.

◆ **A "sophisticated" cyberattack compromised more than 300,000 patient records at Beacon Health System,** the hospital said on May 22. Beacon discovered the attack on March 25, determining that employee email inboxes had been phished as early as November 2013 and as late as January 2015. The majority of affected information included patient names, physician names, patient ID numbers and whether the patient was active or inactive, but in some cases also included dates of birth, Social Security numbers, driver's license numbers and medical information such as diagnoses and treatments. Visit http://tinyurl.com/p3eoxsx.

◆ **Looters in the Baltimore riots compromised PHI when they stole prescriptions from various Rite Aid and CVS stores,** *The Baltimore Sun* reported on June 3. Types of medication, as well as names and addresses on the labels, were exposed in the robberies. Rite Aid reported the breach of 2,345 records to the Office for Civil Rights on June 3. CVS Health, who also told the *Sun* it would be notifying customers of a potential breach, on June 26 notified OCR of a stolen desktop computer containing nearly 13,000 records, but it's unclear if this was connected to the riots. Visit http://tinyurl.com/p2hdd5j.

◆ **Two-thirds of health care organizations have experienced a "significant" security event,** according to a June 30 survey from HIMSS. The organization polled nearly 300 health information security professionals, reporting that they use an average of 11 different technologies in their security practice. More than half confirmed they had created a specialized data management position within their organization. Visit http://tinyurl.com/ncset2l.

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 provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — 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.)