Report on
Patient Privacy

Volume 11, Number 4 • April 2011

Practical News and Strategies for Complying With HIPAA

Contents

3 CEs and BAs Should Make Encryption Part of Overall Security Program

5 OCR Regional Staff Is Compiling Small Breaches For Future Action

6 *Patient Privacy Court Case*

7 OCR Is 'Hopeful' Audits Will Start in 2011; Experts Offer Strategies

8 *Privacy Briefs*

11 *Breaches in Brief*

Editor
Eve Collins
ecollins@aishealth.com

Executive Editor
Jill Brown

OCR Pushes 'Culture of Compliance,' Shares Data on Breaches, Investigations

The HHS Office for Civil Rights has a "clear message" for covered entities and business associates, in case the $5.3 million in penalties it assessed less than two months ago wasn't strong enough. "We are serious about enforcement," said the new OCR hire who actually has "enforcement" in her title — Valerie Morgan-Alston, OCR's new deputy director for enforcement and regional operations.

But Morgan-Alston said the "most important message" is that covered entities (CEs) and business associates (BAs) need to create what she termed a "culture of compliance."

Other OCR officials who joined Morgan-Alston at the recent 19th National HIPAA Summit in Washington, D.C., echoed those sentiments. They also shared OCR's "lessons learned" from the privacy and security incidents and complaints the agency has been handling, and provided some compliance tips.

Morgan-Alston was recently "elevated" to her new job after serving as a regional OCR director based in Chicago, said Sue McAndrew, OCR deputy director for health information privacy.

continued on p. 9

CEs Should Expect More State Enforcement As OCR Begins to Train Attorneys General

For years, HIPAA experts have warned that the states were becoming a hotbed of privacy and security enforcement and a limited number of covered entities did feel the brunt of aggressive attorneys general, including Health Net Inc., which actually paid the state of Connecticut twice for the same infraction.

A few creative AGs and insurance commissioners have taken action even without federal authority, and in the case of North Dakota, even a state law to go on *(RPP 12/10, p. 1).* Health Net was the first CE to be fined under new state enforcement authority the HITECH Act conveyed to state attorneys general. And with the announcement by the Office for Civil Rights that it is beginning to train state AGs on privacy and security enforcement, it most definitely won't be the last.

"We are happy to welcome the state AGs' offices into the enforcement scheme," Sue McAndrew, OCR deputy director for health information privacy, said at the recent 19th National HIPAA Summit in Washington, D.C., at which the training was announced. "I think they hopefully will play a very important role…on these matters of such importance about the privacy and security protections of their health information."

"I think it's a savvy move on the part of OCR and I'm impressed that they are funding it," says John Nicholson, counsel with Pillsbury Winthrop Shaw Pittman LLP, in Washington, D.C., who specializes in privacy. "The AGs benefit from the fact that CEs and BAs are now required to report breaches to HHS and/or the Federal Trade Commission. AGs can wait for people to tell on themselves, go investigate and settle accordingly. HHS can just come in behind them, take the results of the AGs' actions and follow up with their own investigation and settlement. HHS expends less money on

enforcement and reaps the benefit of the AGs' investigative work."

When the HITECH Act passed in 2009, it contained a surprise provision that gave state AGs the authority, within certain limits, to pursue HIPAA cases from the state level. At the time, some said AGs were not well-equipped to take on such a task. The training will change that perception.

Starting this month, OCR begins a series of four in-person training sessions for AGs and their staffs around the country. OCR is even paying their way to attend the meetings.

The first such session was scheduled for April 4-5 in Dallas, to be followed by sessions in Atlanta, Washington and San Francisco.

Training In Person, Online

"Each office is being invited to send two people that would be our expense to come and receive training on HIPAA privacy and security rules so the AGs will be better prepared to effectuate their new authorities under the HITECH Act," McAndrew explained, "and to also get involved with enforcement of HIPAA."

She added that OCR also expected to provide an online training module sometime afterward. "Once the in-person training is completed we will have computer-based training available for these offices as well as for other training purposes," she said.

Later, in a question-and-answer session at the same meeting, McAndrew did little to allay fears that if OCR went after a scofflaw, an AG wouldn't (and vice versa). But she noted that HITECH bars "concurrent actions," meaning the state and federal governments couldn't pursue a CE or BA at the same time.

OCR, AGs Can Both Investigate

Yet, "curiously, there is not a prohibition on sequential investigation of the same activities," McAndrew said. "So if the state AG goes first, their enforcement action does not preclude my office from also pursuing the same activity following that, or vice versa."

In fact, according to the notice on OCR's website about the training, the agency plans to share information with state AGs so they can, presumably, take action themselves. "OCR will provide information upon request about pending or concluded OCR actions against covered entities or business associates related to state attorneys general investigations," the website says.

So what exactly will OCR be teaching the AGs? For one thing, how to fund such efforts, responding perhaps to the widespread fiscal crises afflicting state budgets. Listed on OCR's website among the topics to be covered is "Resources for state attorneys general in pursuing alleged HIPAA violations."

A general introduction of the rules will also be covered, in addition to the following:

- ***An explanation*** of how HITECH changed HIPAA,
- ***"Investigative techniques*** for identifying and prosecuting potential violations,"
- ***How state laws work*** together with HIPAA,
- ***OCR's role*** versus state AGs' "roles and responsibilities," and
- ***"HIPAA enforcement*** support and results."

CEs and BAs Better Get Ready

Nicholson says the new training should put CEs and BAs on greater watch against non-compliant employees and send a message to beef up training.

"Companies that handle [PHI] need to focus on policies and training that reach down to the lowest levels of the organization," says Nicholson. "The cost of data breaches keeps going up, and it only takes one employee or contractor to place the entire enterprise at risk. On the other hand, trained, observant members of the cleaning staff could save companies if they realize [for example] what is in the trash before it's put out."

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

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** (**$454 bill me; $424 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Nicholson predicts that "the concept of multiple enforcement actions is something that is likely to continue and increase with this training."

"At a time when people are unhappy with government and corporations, in general, these kinds of actions enable state AGs to show they are protecting the citizens of their state by going after companies who fail to appropriately protect personal information," he says.

Contact Nicholson at john.nicholson@pillsburylaw.com. ✧

CEs and BAs Should Make Encryption Part of Overall Security Program

There was one term that kept making its way into sessions during the recent 19th National HIPAA Summit: encryption. With electronic health records becoming a part of the everyday lives of covered entities (CEs), encryption will become a more natural part of the industry, one source tells *RPP*.

More than 60% of HIPAA covered entities that experienced a data breach said encryption would have been a mitigating factor had they used it, according to a recent study by the Ponemon Institute. "So these organizations might have gone through an addressable analysis and concluded that encryption was not reasonable and appropriate in their environments, but they sure had a different feeling about that after experiencing a breach," Dan Steinberg, lead associate at Booz Allen Hamilton, said at the summit.

Complacency Plays a Major Role

Some of the concerns CEs have about encryption are cost, usability and interoperability, Steinberg told *RPP* in an interview after the summit. But complacency also plays a role, and CEs need to snap out of that with OCR audits coming soon. "It also has to be said that the perception of the ability to stay under the radar has probably played a factor as well.…In last few years, CEs have become complacent," he said. "I worked with OCR on the audit methodologies, and that's part of the groundwork….Compliance is on the upswing."

Covered entities have some very good reasons to be concerned. "Organizations are under relentless attacks. Every 1.5 seconds, there is an attack on an organizational infrastructure," said Ali Pabrai, chairman and CEO of ecfirst, who also spoke at the summit. Pabrai, who has traveled extensively in India, added that there are many Indian companies becoming business associates with U.S. covered entities.

They are "providing services related to processing PHI. They may do it in different ways: coding, billing transcription services, chart reviews, what have you…. The bottom line is that they're all coming into contact with PHI that originates at a CE, flows through a health care organization somewhere in the U.S., and then is contracted through an agreement with the Indian entity," Pabrai said. "Those are the kinds of parameters we have to take into account as we try to determine how we can make our organization more secure.…There is no such thing as a 100% secure environment, but what we can try to do is deliver a resilient enterprise," he added.

U.S. law does not apply to offshore business associates and cannot be enforced, but the BAs have a strong incentive to comply with U.S. regulations to maintain a good reputation among American health care organizations *(RPP 2/10, p. 3).*

Four Key Things to Consider

Steinberg said covered entities should consider four things when contemplating encryption:

(1) The size, complexity and capabilities of the covered entity. In researching encryption, CEs will have to take into account their needs, data flows, etc. "You need to implement it in a way that doesn't impede the overall operations of your information systems," Steinberg said. This is where interoperability comes in, he said, "which is going to be a big focus — forever. We have meaningful use going through 2015, and the idea behind meaningful use is to increase communication between health care entities. There are formats of encryption that don't work especially well together," he said.

(2) The technical infrastructure, hardware and software. There are small providers that don't have the infrastructure with the computing power, speed and memory for encryption, he said. "If that's so, it's time to reassess your technical infrastructure. There are a lot of products out now, including Windows products, where the encryption capabilities can be built right into the application or hardware."

(3) Cost. Steinberg uses the Learned Hand equation. "You are comparing the cost of investing in the protection versus the cost of mitigating the resulting harm, multiplied by the probability of that harm. If you go through that analysis, you're likely to have a pretty large [cost] for encryption," he told *RPP*. "Some of the things you would need to consider in getting the size of that cost down is how many records there are, how sensitive the data are, how large the penalties would be if OCR or an attorney general sought to impose a penalty, and how likely you think it is that someone would be interested in your health care information."

(4) Criticality. Steinberg pointed out that health data now have value beyond what they had in the past with medical identity theft and black market value.

continued

Security is all about layers of controls, Pabrai told summit attendees, and "typically the first layer of defense is your firewall system. That's your DMZ. If the hacker or the attacker penetrates all layers of security you have put in place, but you have encrypted that device or information appropriately — because there are different grades of encryption, different encryption algorithms, protocols — that would be a deterrent," he said. "You can afford to lose the laptop. You cannot afford to lose the PHI on the laptop. So that's where this becomes really important."

Encryption Is Part of Larger Program

Steinberg stressed that encryption should be part of an overall security program. "There are those who think we rely too heavily on encryption at the expense of other security controls," he said at the summit. "Organizations view encryption as a powerful security control, but it needs to be integrated. HIPAA tells us to have a robust, multifaceted security program. So the fact that you're using one powerful control does not mitigate the need for a security program," he added in an interview.

For example, certainly encrypt mobile devices, but also use good access controls. "Make sure you know who has them, and that individual employees are training on their proper care," he said. With networks, "you don't want anyone setting up connections to the system admins or the IT departments," he said. And with media disposal or reuse, make sure no one is able to recover the information on the device.

But just having encryption isn't going to trump common sense. One attendee asked during another session if a CE loses a laptop, and the key to the encryption is contained on that laptop, is the CE safe? "I think it's pretty obvious in that situation that you have not rendered the information indecipherable — you've [provided] the exact tool that's needed to render the information decipherable," Steinberg said.

Encryption was one of the methods cited in HHS's April 2009 guidance on rendering PHI unusable, unreadable or indecipherable. "OCR and HHS are very circumspect about the language that they use," Steinberg said at the summit. "Nowhere in that language do they actually use the term 'safe harbor,' but they put quotes around it. So that illustrates how powerful encryption can be and how much it actually can mitigate your risk," he said.

Sue McAndrew, OCR's deputy director for privacy, also spoke at the summit and indicated OCR's thoughts on this security measure. She said the large breaches involving theft and loss of data continue to be huge problems because CEs don't use encryption.

"Do you know how simple it is to avoid this problem by simply encrypting your portable media? Then you are just faced with the loss of property, and don't have to face the loss of the data," said McAndrew. "This is such an easy problem to solve….We can't stop people from breaking into your homes or your cars or wherever you leave your laptops. That's beyond our control. But it's not beyond our control, and it's not beyond your control, to make sure the data are safe, and that's a simple matter of encryption. So I've given you my encryption lecture."

Citation to NIST Is 'Significant'

The fact that HHS's guidance directs CEs to the National Institute of Standards and Technology's special publications on encryption is "significant," Steinberg told the summit. "In the past, while HHS has made reference to NIST as a possibly helpful source of guidance for individuals seeking help, seeking to learn about security, this is the first time it's actually been included in guidance."

Encryption is emerging as a staple at many covered entities, says Bill Moran, senior vice president of Strategic

Management, an Alexandria, Va.-based consulting firm. "We have some clients that have had EHRs for over 10 years, and have seen the importance of encryption because things have been lost in the past, so they have seen the value of it," he tells *RPP*.

"The covered entities that are progressing with EHRs will come to understand the value….Some are just not there yet in terms of their systems," says Moran. Other CEs have had encryption in certain parts of the facility, but have not expanded it to the others.

But the price tag on encryption should not be the deciding factor, Pabrai contended. "I think in 2011, if an organization is not budgeting for laptop encryption, for backup media encryption, for removable media encryption, that is a significant risk to the organization. There is no reason for [executives] not to authorize that for backup media."

Contact Steinberg at steinberg_daniel@bah.com and Moran at wmoran@strategicm.com. Visit www.hipaasummit.com. ✧

OCR Regional Staff Is Compiling Small Breaches for Future Action

As all covered entities know by now, those unfortunate enough to suffer a breach of unsecured protected health information (PHI) that affects 500 or more individuals must report this to the media and to the HHS Office for Civil Rights as soon as possible, and then suffer the consequences of having the news appear everywhere.

OCR posts the information about these so-called "big breaches"on its website for all to see and launches an immediate investigation into the incident once it receives word.

So far, since the new notification rules went into effect, OCR has posted more than 240 such reports that affect more than 6 million individuals.

But what isn't as widely known is what OCR does with the reports of breaches affecting fewer than 500 individuals, which also must be reported to OCR, although this report can wait until an entity files its annual tally. CEs and BAs are required to submit a single report for each of these smaller breaches, and there have been far more of these — 29,000 reported to OCR from September 2009, when the mandate began, through Feb. 28, 2011.

At the recent HIPAA Summit in Washington, D.C., a high-ranking federal privacy officer revealed that those "small" breach reports are being sent to OCR's regional investigative offices. While OCR may not investigate each breach, it is, in effect, building a "permanent record" of a CE or BA's misdeeds at the regional office level, for future use in enforcement proceedings.

Breach reports involving fewer than 500 individuals "are sent out to the respective regional offices and they are available to the investigators for use either when they have a big breach at an entity or any other investigation that may be ongoing with the entity," said Sue McAndrew, deputy director for health information privacy for the Office for Civil Rights.

She added that "the nature of the small breach itself may call for an opening of an investigation, on its face."

One Report Per Breach

As she has before, McAndrew noted that "the bulk" of the small reported breaches involve errors with paper records, including e-mailing or faxing PHI to the wrong recipients *(RPP 3/10, p. 1).* (For more details on large breaches, and other OCR statistics, see story, p. 1)

McAndrew noted that CEs are required, on an annual basis, to send OCR reports of breaches during the prior calendar year, pointing out that the first such report was due last February. She said OCR is "only on our second cycle of smaller breach reports," with the most recent deadline March 1 for 2010 breaches.

Breach reports, which must each be filed singly — one per incident — are also going to OCR regional offices. When regional staff look over the reports, "I would expect OCR to be more concerned about entities that have multiple breaches," says health care attorney Kirk Nahra, a partner in the Washington, D.C., office Wiley Rein LLP.

Knowing what is happening to these small breach reports "does focus attention on the need for good mitigation, whether a breach is large, small or requires no notice at all. It is critical to fix problems and think broadly about preventing future breaches," Nahra adds.

OCR: 'Tell Us Everything'

OCR officials disclosed this process during a question-and-answer session at the HIPAA Summit, in response to a question about how OCR goes about conducting an investigation, and how much information the target of the investigation should reveal on its own.

An unidentified male questioner at the meeting said his organization had received an "investigation questionnaire," related to a breach. This was most likely a "large" breach, as OCR does not routinely investigate small breaches.

The man was wondering if more information should be disclosed than was required by the ques-

tionnaire. Specifically, the questioner wondered what OCR examines during an investigation.

"When you open a breach investigation, will you commonly look at unreported breaches that have occurred historically, either ones that were under 500 and therefore hadn't been reported to you yet, or incidents that might have been investigated where there was a determination that…it didn't exceed the threshold for harm and therefore it did not need to be reported to you?" he asked.

While she didn't directly answer the question, McAndrew described how the small breach reports were being sent to the regional offices. David Holtzman, OCR's health information privacy specialist, who also spoke at the meeting, gave a second response that spoke more directly to the man's concern.

"If the CE's goal is to cooperate with OCR in resolving an indication of a violation or a compliance review or investigation through informal resolution, through voluntary compliance, it is always better for the CE to be forthcoming and disclose all prior security incidents or unreported breaches or issues involving the unauthorized disclosure or use, as opposed to OCR having to come upon it and find it later on in its investigation," Holzman said. "[That] builds trust and creates a better atmosphere for information resolution and it's to the advantage of the CE."

As far as going beyond the questionnaire itself, "It's better to disclose and ask forgiveness than for us to find out and have to ask you for an explanation," Holtzman said.

Be Helpful, Yet Selective, Lawyer Advises

While OCR has recently imposed big fines *(RPP 3/11, p. 1),* it seems that its overall approach is still to seek voluntary compliance, Nahra tells *RPP*.

"That means that the primary goals are still to fix problems and encourage appropriate behavior. That means that, *generally,* it will be of benefit to entities under investigation to cooperate and communicate as much as reasonably possible," he says. "Accepting responsibility and agreeing to make suggested changes also has been useful in closing investigations in the past."

But, adds Nahra, "that doesn't mean that it's always the right thing to turn over everything all the time" while still being "cooperative and responsible."

PATIENT PRIVACY COURT CASE

This monthly column is written by Rebecca Fayed of the Washington, D.C., office of SNR Denton. It is designed to provide RPP *readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Fayed at rcfayed@snrdenton.com.*

◆ **The U.S. Court of Appeals for the Sixth Circuit found on Feb. 23 that requiring employees to disclose the nature of their illness is not a violation of the Rehabilitation Act.** Current and former employees of the City of Columbus, Division of Police, brought a class action against the city challenging a directive that required employees returning to work from sick leave, injury leave or restricted leave to provide a physician's note stating the nature of the employee's or family member's illness to the employee's immediate supervisor. The employees alleged that the directive violated the federal Rehabilitation Act and sought an injunction prohibiting its enforcement. Although the district court found in favor of the plaintiffs and entered a permanent injunction prohibiting enforcement of the directive, the Sixth Circuit Court of Appeals disagreed and vacated the injunction. In finding for the plaintiffs, the district court found that the directive violated the Rehabilitation Act because "supervisory personnel in the chain of command are not authorized by the statute to have unfettered access to confidential medical information." Moreover, the district court found the directive to be "overly intrusive and improperly provided supervisors with confidential medical information even when they had no reason to possess such knowledge, particularly in light of the fact that the city had a human resources department which presumably could be used to create a 'confidentiality barrier between these personnel whose jobs consist of handling medical information, and supervisors.'" The Sixth Circuit Court of Appeals, however, found that the directive is a "universal sick-leave policy applicable across the board to all division employees, disabled or not, who use contractual sick leave for a personal illness…and constitutes a valid and acceptable inquiry under" the Rehabilitation Act and the Americans with Disabilities Act. (*Lee v. City of Columbus, Ohio)*

Reflecting on Holtzman's comments about disclosure, Nahra says that, "On the large versus small breach situation, if a covered entity will be submitting a report shortly about small breaches, and it hasn't disclosed that during the course of an investigation, it is quite likely that OCR will be much more aggressive the next time, or won't be as quick to accept reports of responsibility."

Contact Nahra at KNahra@wileyrein.com. ✧

OCR Is 'Hopeful' Audits Will Start in 2011; Experts Offer Strategies

Privacy and security audits mandated by the HITECH Act are supposed to start in 2011, and representatives of covered entities who attended the recent 19th National HIPAA Summit in Washington D.C. seemed eager for news of the audits. But very little is known about what form the audits will take, and where and when they will start.

While officials from the HHS Office for Civil Rights spoke at the summit, they barely mentioned the audits in their talks and gave little away in answering the audience's questions about them.

A panel of OCR officials was asked about the status of the compliance audit program. Sue McAndrew, OCR's deputy director for privacy, said OCR is still working out how the program will take shape, but hopes it will be operational sometime in 2011.

"We have pursued, through contract, an analysis and evaluation for potential models for bringing up an audit program and we are looking, again through contract vehicles, to do some piloting on one of those audit models," she said. "It's not an inconsiderable effort to put resources into an audit-type program and to have that be a sufficiently robust program to play a meaningful role — a role in enforcing the privacy and security rules….How you manage all of that in the current environment is challenging," she added. "But we are doing our best to take a very deliberative approach to make sure that what we engage in and commit resources to will be effective, as well as the most efficient use of those resources."

While another summit speaker had little information on when the audits will begin, she — and other experts *RPP* interviewed — provided lots of advice on how to prepare. "I left my crystal ball in the taxi on the way to the conference," Phyllis Patrick, of the Purchase, N.Y.-based consulting firm Phyllis Patrick & Assoc. LLC, joked with the audience. "It was encrypted, but it didn't have any PHI on it," she added.

The HITECH Act directed OCR to develop an audit program for checking HIPAA compliance at covered entities and business associates and provided funding for a study to find the best means of performing the audits and to form audit protocols. OCR contracted with Booz Allen Hamilton to conduct the study, which has been completed, but it is not publicly available. Additional funding will be released to begin the audits in 2011, according to OCR's budget request for FY 2011.

"They're also looking to have the audit process really augment the existing processes that are ongoing: the reviews, the investigations, the complaint remediation," Patrick said. "As we know from some of the past auditing efforts from CMS — from Piedmont — we never got too much feedback from those. So in terms of lessons learned, it wasn't clear what the average CE could do with that, [because] we just heard general information," she added. "With Piedmont, the letter and checklist that they were given was geared more towards the technical aspects of the security rule. [But] remember that the OCR audits are to cover privacy and security in their entirety," Patrick pointed out.

The Universe of Auditees Is Humungous

The agency has its work cut out for it, Patrick said. "OCR has limited resources, limited staffing, yet…the universe of auditees is humungous because now they have business associates, and the new business associate categories that have been added under HITECH."

"They have been giving [the audit process] a great deal of thought, a great deal of time. I know some of us are impatient and saying, 'When will we have some guidance?' But I say, just jump in the water."

Some clues may exist. Patrick said audits may not be completely random — auditors could show up following "sentinel events" like a major breach or complaint, or even a compliance deadline. The audit process could be linked to the meaningful use process, for example. "Entities have been able to enter the registration process and will be able to attest that they have the risk assessment and to other factors required for meaningful use to receive incentive funding," she pointed out.

"One of the things that has become clear in my discussions with OCR…is the consistent theme that OCR really wants these audits to be educational; they're not looking that the primary purpose be punitive; and that the auditing will complement the existing processes," she said.

Patrick provided the following checklist to help prepare for OCR audits:

"Can you say you are in compliance with the security rule evaluations standard," which is not the

same as the risk assessment standard, Patrick says. "When I ask CEs if they've performed an evaluation, a lot of times I'll get a blank stare….Very often, they don't really know what the standard is. You should be doing an evaluation initially based upon the standards and implementation specifications in the rule, but also in response to changes: a new system, new executive team, new approaches, new physician acquisitions."

"Can you demonstrate that your policies, procedures and practices enable a patient's individual rights?" Also, can you prove that you have upheld these policies? "Have you audited in this area? If I were a patient, how do I access my record? What is the process like? Walk me through it. What are the barriers, and did I get what I asked for? Did I get it timely? Did you meet those things you have in your notice of privacy practices?"

"Do you meet the security rule standards for risk analysis and risk management?" The rule requires an "accurate and thorough" evaluation. Patrick's hospital-clients tell her "Yes, we're doing enterprise-wide risk assessment." But she asks them to show her the profile, "and you don't see anything on it about privacy or security. So how are you doing enterprise-wide risk analysis if you're not integrating privacy and security?"

Have you completed the required risk analysis for meaningful use, which has also been required by the security rule since 2005? Have you implemented remediation? "Have you, in fact, made modifications and changes based upon your risk assessment? Or is it a document that you've done and it's on the shelf and you can go back and look at it and it has seven recommendations that nobody ever touched?" Do they go beyond the security rule's technical requirements? "While the technical requirements are very important, they are one aspect of the security rule. Having done penetration testing every year or every other year does not qualify as having completed a risk assessment."

"How often do you perform risk analyses?" she asked. "It probably should be at least annually, but it depends upon your organization," Patrick said. "How do you document them so that a surveyor — or in doing your own internal audit — you can go in and find out that risk analyses were done since the security rule was put into effect." Take into account how training has changed over the years, for example. "Are you still using the online training modules—the mind-numbing online modules that you were using in the beginning?" Patrick asked, with a focus on good passwords and other vintage HIPAA concerns. Today's concerns are "How do you report a breach? Who do I call? What do I do? Do I wait? Do I just hope it goes away?" she said.

Are your security and privacy analyses integrated with the CE's enterprise-wide risk analysis process? The security rule requires administrative, technical and physical safeguards, and Patrick says encryption, training, documentation of policies and procedures, auditing, designating a privacy and security officer are essential. "If I had a limited budget and I were a privacy and security officer today, I would fight really, really hard for the encryption [see story, p. 3] and for the training because if you do those two things and you do them as well as you can given the resource constraints that you have, at least you'll be going a long way towards protecting" patient privacy and security.

Do you engage in ongoing auditing and monitoring for privacy and security? "People think of auditing in terms of access, and that is an important component, that you have a way of auditing access to who has looked at which records, when, why….But the audit process goes way beyond that, and the ideal is that you have to have an audit plan." That should include who is responsible (privacy or security officer, internal audit department), what your corrective action plans are and how do you document that, and how findings are reported to the board or senior leaders.

In addition to these suggestions, consultant and former HHS Office of Inspector General official Bill

PRIVACY BRIEFS

◆ **The Office of National Coordinator for Health Information Technology (ONC) is asking for public comments on the government's recently updated health information technology strategic plan. A goal of the plan is to improve trust in health IT by focusing "**on government efforts to update its approach to privacy and security issues related to health IT and to build greater confidence and trust in EHRs and health information exchange among providers and the public." To read more and post a comment, visit http://www.healthit.gov/buzz-blog.

◆ **HHS is co-hosting a conference on health information security May 10 and 11 with the National Institute of Standards and Technology. The event is called "Safeguarding Health Information: Building Assurance Through HIPAA Security."** Visit www.nist.gov/itl/csd/hipaasec.cfm for registration information.

Moran suggests to his clients that they keep reviewing their business associate agreements. "Go down the line and make sure things are in place…that you know you can rely on the business associates you have and that they'll carry out the things they say they are going to do." A good recent example is the New York City Health and Hospitals Corporation, which is suing the firm that it was using to transport and store PHI after data tapes were stolen from the vendor's unlocked vehicle *(RPP 3/11, p. 3).*

Also, don't underestimate the nosy staff member, says Moran, who is now with the Alexandria, Va.-based consulting firm Strategic Management. "There are different software programs that [check whether] individuals should have accessed this record or not, then you can query their supervisors on whether that person had a reason to access it," he says. Every community has celebrities and newsworthy incidents that happen. "If you are in a tight community, then people are wondering how someone is doing, or someone knows someone else….There is some good monitoring going on, and some people have been fired."

The problem is that breaches don't happen in the privacy office, notes attorney and consultant Cindy Stamer. "Every one of those covered entities that has been sanctioned [by the feds] had a policy in place," she says. "OCR is going to look at how you've operationalized things….When your risk analysis was done, did you just have some consultant come in and say you're HIPAA compliant, and fill out a checklist for you, but then you haven't redone it since?"

Moran says a good place to start is with the resolution agreements HHS has done so far with covered entities. "People get penalized, and everyone looks to see what did the penalty involve, and it'll tell them what they have to do. There will be more agreements as time goes on and the pattern will become clear about what is required and what OCR will demand, and that will help the facilities to understand what they will need to focus on."

Stamer agrees. "Start with what they're already telling us. They're giving us a heads-up. After the settlements with Providence and Mass General, if you don't understand that any PHI outside of your environment needs to be controlled, they're not going to have a lot of sympathy for you."

Contact Stamer at cstamer@solutionslawyer.com and Moran at wmoran@strategicm.com. Visit www.hipaasummit.com. ✧

OCR Promotes Compliance Culture

continued from p. 1

"In light of OCR's clearly articulated intention to aggressively enforce the HIPAA privacy and security rules, covered entities and their business associates should review their current HIPAA compliance programs," Morgan-Alston said at the HIPAA Summit.

She noted that a "robust compliance program" includes employee training, vigilant implementation of policies and procedures, regular internal audits and an action plan to respond to incidents.

Security Corrective Actions Are Rising

"CEs should be training their employees that compliance is as essential as patient safety," she said. "Policies and procedures can't be something just sitting in notebooks on shelves gathering dust. They must be an everyday part of an organization's culture."

Alston tried to hammer home the need for audits, saying "CEs must conduct regular internal audits to find noncompliance themselves rather than waiting for complaints and OCR to come in."

At the conference, McAndrew gave an overview of recent corrective actions by OCR *(RPP 3/11, p. 1).* She noted that since 2003, OCR has investigated a total of 19,460 privacy complaints and obtained "corrective action" in 12,781.

But the public is still apparently confused about what is and isn't covered by HIPAA. OCR statistics indicate that "two out of every three cases" that OCR gets to

HHS Security Case Results 2006 - 2010

	Corrective action obtained	No violation found	Closed without investigation
2006 (partial data)	15%	10%	75%
2007	31%	18%	51%
2008	12%	30%	58%
2009	10%	48%	42%
2010	55%	13%	32%

SOURCE: HHS Office for Civil Rights

add to its "resolved" side of the ledger are closed because they were simply ineligible for federal action, involving circumstances over which OCR has no "jurisdiction," McAndrew said.

As with privacy complaints, OCR investigates each security complaint it receives, but also has a policy of opening a case, called a "compliance review," each time an entity reports to OCR that it has suffered a security breach affecting more than 500 individuals.

In 2010, OCR counted a total of 243 security cases opened, reflecting both complaints and compliance reviews. Prior years' case volume data are not comparable because the breach notification rule was not in effect until September 2009, and OCR did not take over enforcement of the security rule from CMS until July 2009 *(RPP 8/08, p. 1).*

McAndrew was followed at the summit by David Holtzman, OCR's health information privacy specialist, who provided more details about security enforcement. Holtzman explained that the purpose of the automatic compliance review is "to attempt to determine the root cause of the breach and to assure that corrective action has been taken to not just address the root cause, but that there is appropriate compliance action taken to prevent similar breaches or security incidents in the future."

Holtzman shared a chart showing approximate percentages for the number of security cases CMS and OCR handled from 2006 to 2010, and the disposition of the cases (see table, p. 9).

According to the data, it would appear that since OCR took over, it has been more successful in obtaining corrective action than CMS; still, at least 30% of cases fall outside OCR's jurisdiction or do not address a security issue under HIPAA. While this percentage is less than OCR's experience with privacy, it is still significant.

Reasons for Breach Notification	
Theft	51%
Unauthorized access, disclosure	21%
Loss	16%
Hacking/information technology incident	6%
Improper disposal	5%
"Other"	1%

Where Large Breaches Occur	
Laptops	24%
Paper records	21%
Desktop computer	16%
Portable electronic device	14%
Network server	10%
Other	10%
E-mail	3%
Electronic medical record	2%

Administrative Violations Outnumber IT

Holtzman revealed the "most frequent" issues arising in security rule violations and complaints over the course of the past five years. Surprisingly, "technical" comes in a distant second, accounting for 141 cases, versus 449 for "administrative," meaning policies and procedures either don't exist or were violated. "Physical" safeguards were an issue in 84 cases and all were categorized as failings in "work station security."

Regarding "administrative," the most frequent issues involved (and their regulatory sections) are:

- ***Response and reporting*** (CFR164.308(a)(6)(ii)),
- ***Awareness and training*** (CFR164.308(a)(5)(i)), and
- ***Information access management*** (CFR164.308(a)(4)(i)).

Holtzman also described the reasons CEs and BAs have had to issue breach notifications for those affecting more than 500 people, and where the large breaches occurred (see tables below). For information on small breaches, see story, p. 5.

Compliance Solutions Include Network Storage

The fact that 50% of the breaches involved electronic PHI came as a surprise to Holtzman, he says. "[T]his is astounding. This is a no-brainer. We have to reduce the risk of data being lost or stolen through these portable devices," Holtzman says. "We can do that by adopting network or enterprise storage as an alternative to storing electronic PHI on the hard drive of a laptop, or the hard drive of a desktop computer."

Another "lesson learned," Holtzman says, is to encrypt. "That seems to be the most effective mechanism to avoid the loss of electronic PHI," he said. (See story, p. 3.)

Holtzman, like Morgan-Alston, stressed the need for a workplace environment that supports compliance. In businesses that have a "culture of compliance, you will be less likely to be subject to these types of security incidents that result in breaches," he said.

Policies and procedures need to be "indoctrinated through a culture of compliance through our organizations, from top to bottom," Holtzman said.

He suggested that a way to build such a culture is through raising worker awareness and using "security reminders." As an example, Holtzman said that the cafeteria of the U.S. House of Representatives has information security messages stuck on napkin holders.

Such activities "keep the message" present for the workers who are more likely than higher-ups to be

involved in possible privacy and security violations, Holtzman said.

"It's not the chief executive officer or the board of directors who are going to determine if a laptop is left in an airport, if paper files are left on a subway train, or your thumb drive is left in the back of a cab," he said. "So it's really important that we reach [workers], that we teach a message of the culture of compliance to the folks who work with electronic PHI and other PHI on a daily basis."

Visit www.hipaasummit.com ✧

BREACHES IN BRIEF

◆ **Health Net Inc. said March 14 that it is missing several server drives from its data center operation in Rancho Cordova, Calif.** IBM, which is responsible for managing Health Net's information technology infrastructure, told the insurer it could not locate the devices. Health Net has determined that the personal information of current and former members, employees and health care providers is on the drives. The data may include names, addresses, health information, Social Security numbers and/or financial information. News reports say the breach affects about 2 million individuals. Since Health Net announced its investigation of this breach, officials in at least three states have asked the insurer for more information on the incident. Connecticut Attorney General George Jepsen has asked the company about the status of the breach and also for identity theft and credit card protection for the 25,000 residents affected in his state, where Health Net also operates. Officials in Oregon and California also have said they are conducting their own inquiries of the incident. A Health Net spokesperson did not respond to *RPP*'s request for further comment. Visit www.healthnet.com and click on "Newsroom."

◆ **Blue Cross and Blue Shield of Florida said March 7 it notified more than 7,000 members that it inadvertently mailed some of their information to incorrect addresses.** The health plan said the incident was caused by a "system error," but that it fixed the issue the same day it was discovered. During a conversion to a new mailing system that tracks both new and old addresses, some of the old mailing addresses were identified as current addresses, the Blues plan explains. Explanation of benefits forms were mailed to about 7,400 members' former mailing addresses over a three-month period, but there were no Social Security numbers or birth dates on the forms, it says. Visit www3.bcbsfl.com, click on "About Us," and then "Media Room."

◆ **The Cord Blood Registry (CBR), in San Bruno, Calif., is notifying customers that computer equipment and backup tapes stolen from a locked car contained personal client data,** a CBR spokeswoman tells *RPP*. CBR has a bank to store cord blood in case stem cells are needed for transplants and other therapies. The theft affects about 300,000 CBR clients, media reports have said. No health data were on the devices, but they did include Social Security numbers and credit card numbers, according to Kathy Engle, CBR's director of corporate communications. The theft occurred in early December and CBR has been working with consultants to determine the potential risks to the data, Engle says. Visit www.cordblood.com.

◆ **The Adult Industry Medical Health Care Foundation (AIM) is investigating a possible "criminal breach" of the medical record database at its medical clinic in Sherman Oaks, Calif.,** it said March 31. Media reports say a wiki-leaks-type website posted names, birth dates and other information of actors in the adult film industry and other sex workers, which AIM specializes in treating. AIM was not positive it was the only breach victim based on the information released, however. "Substantial amounts of information posted on the site in question could not come from the AIM database because we do not possess that information," including home address and identification documents, it said in a statement. "AIM is utilizing every available resource to conduct a thorough forensic investigation to confirm if a breach of security occurred here….Accessing a database for improper purposes, violating medical privacy and extortion are all crimes in California. There is preliminary information indicating that criminal behavior by persons or entities may have occurred," it adds. Visit www.aim-med.org.

◆ **The Henry Ford Health System said March 18 it is ramping up its privacy and security program after a flash drive containing PHI on nearly 2,800 patients went missing.** The unencrypted flash drive contained data on patients who had been tested for urinary tract infections, including name, medical record number, test ordered, test result, test date and location. No SSNs or health insurer identification numbers were on the device, the provider

BREACHES IN BRIEF (continued)

says. In the next 90 to 120 days, the health system plans to (1) implement a zero-tolerance policy for situations in which personal health information is left unsecured on devices such as computers, smart phones or flash drives (to include suspension or termination for violations), (2) eliminate use of unencrypted devices throughout the health system, and (3) retrain staff on the proper way to store equipment for work purposes and safely protect health information on paper, computers and other devices. Visit www.henryford.com.

◆ **The University of Massachusetts Amherst (UMass) on March 7 told patients that malware may have allowed unauthorized intrusions into one of its workstation computers between June 30, 2010, and Sept. 29, 2010.** The desktop computer's user account contained patients' names, health plan names, medical record numbers, and information about prescription drugs, including medications prescribed, their pharmacists and physician names. UMass corrected the issue Oct. 28, 2010, it says in a letter to patients. At that time, the computer's disk drive was removed and sent to the university's IT department for analysis. "The university has completed its investigation and located no evidence suggesting or indicating that any data was copied from the…workstation," it adds. The "risk of theft of this information is low and it cannot be determined with certainty that any of the PHI was exfiltrated." To stop similar incidents from occurring in the future, UMass says it has (1) increased security training for system administrators, (2) implemented software to detect malicious activity, (3) retrained staff on security practices, and (4) implemented more monitoring of staff adherence to security policies. Visit www.umass.edu/uhs.

◆ **A laptop computer stolen from the Rancho Los Amigos National Rehabilitation Center contained information on more than 650 patients,** the Los Angeles County Department of Health Services (DHS) said March 29. The missing laptop contains patient name, birth date, physician name, history of the illness treated, recommendation and a report on an electromyography test the patient received at the county-run facility. The data cover patients treated between July 2007 and Feb. 17, 2011. While there were no Social Security numbers or financial information, the data were not encrypted, DHS say. Staff noticed the laptop was missing from a diagnostic area of the facility on Feb. 23, and law enforcement officials classified it as a theft on Feb. 24. "In response to the incident, DHS implemented enhanced security measures, retrained staff, initiated a campus-wide privacy and security risk assessment and verified all inventoried laptops are encrypted in compliance with county policy," the DHS statement says. Visit www.rancho.org.

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

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

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

3. Call Customer Service at 800-521-4323

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

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