May 2012 Vol. 12, No. 5

Briefings on HIPAA

• Privacy • Security • Transactions • Training

An $18.5 million HIPAA lesson for healthcare organizations

If healthcare organizations take a lesson from Blue Cross Blue Shield of Tennessee's (BCBST) $1.5 million settlement for its 2009 HIPAA breach, it's that they should wake up and pay attention to where their ePHI is contained and stored, says **Ali Pabrai, MSEE, CISSP, CSCS.**

That's just one message from the corrective action plan (CAP) that BCBST devised with OCR in order to address gaps in its HIPAA compliance program, says Pabrai, chief executive of ecfirst, home of The HIPAA Academy, based in Newport Beach, Calif.

BCBST reported to OCR in the fall of 2009 that 57 unencrypted computer hard drives were stolen from a leased facility in Tennessee. The drives contained the PHI of more than 1 million individuals, including names, Social Security numbers, diagnosis codes, dates of birth, and health plan identification numbers.

> **"That's really something we have not seen before. [OCR is] making [Blue Cross Blue Shield of Tennessee] randomly audit their facilities that house portable devices."**
>
> *—Ali Pabrai, MSEE, CISSP, CSCS*

The breach cost BCBST $18.5 million—the $1.5 million settlement plus an additional $17 million in breach response costs. The company reported the latter figure in a press release.

OCR reached the settlement with BCBST in March. It was the office's first enforcement action resulting from a breach that was reported to the agency per HITECH requirements.

The point of enforcement

Leon Rodriguez, OCR's director who spoke March 26 at the 20th National HIPAA Summit in Washington, D.C., urged healthcare organizations to learn from such enforcement actions.

"Enforcement tells a story," he said—that story is, quite simply, "don't be like this entity."

And Rodriguez made it clear that the stepped-up efforts to enforce HIPAA regulations will continue. The main takeaway from the BCBST incident is that "acceleration in enforcement by OCR will continue, and it will intensify," he said.

A costly breach

The BCBST settlement covers the theft of the insurer's

HCPro

IN THIS ISSUE

hard drives from a data storage closet at a former company call center in Chattanooga, Tenn. The hard drives contained audio and video recordings related to customer service telephone calls from providers and members, and included varying degrees of personal information on more than a million health plan members, according to a BCBST statement.

To date, the health insurer says there has been no indication of any misuse of data housed on the stolen drives. The company's response included the encryption of all its at-rest data as well as investigation, notification, and protection efforts that cost almost $17 million.

"Since the theft, we have worked diligently to restore the trust of our members by demonstrating our full commitment to limiting their risks from this misdeed and making significant investments to ensure their information is safe at all times," **Tena Roberson,** deputy general counsel and chief privacy officer for BCBST, said in a press release.

BCBST's CAP requires the health insurer to:

- Review, revise, and maintain its privacy and security policies and procedures
- Conduct regular and robust training for all BCBST employees that covers employee responsibilities under HIPAA
- Perform and monitor reviews to ensure BCBST's compliance with the CAP

In addition to the above items and the monetary settlement, the agreement also requires BCBST to obtain OCR approval for all policy changes and conduct unannounced random audits of its own employees.

You can access the resolution agreement by visiting *www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_cap.pdf.*

The CAP contains many of the elements seen in previous OCR settlements.

"As with other plans, it emphasizes policies, training, and monitoring," says **Adam Greene, JD, MPH,** partner at Davis Wright & Tremaine, LLP, in Washington, and a former regulator at OCR.

BCBST's revised policies must address risk assessments, a risk management plan, facility access controls, a facility security plan, and physical safeguards that work to govern the storage of the organization's ePHI, Greene says.

"All [of these] are issues that appear directly related to the loss of hard drives from a server whose security may not have been prioritized with respect to a change in facilities," he notes. "The monitoring requirements are slightly more detailed than prior corrective action plans that called for internal monitoring, but are not drastically different."

Briefings on HIPAA (ISSN: 1537-0216 [print]; 1937-7444 [online]) is published monthly by HCPro, Inc., 75 Sylvan St., Suite A-101, Danvers, MA 01923. Subscription rate: $349/year. • **Briefings on HIPAA,** P.O. Box 3049, Peabody, MA 01961-3049. • Copyright © 2012 HCPro, Inc. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro, Inc., or the Copyright Clearance Center at 978-750-8400. Please notify us immediately if you have received an unauthorized copy. • For editorial comments or questions, call 781-639-1872 or fax 781-639-7857. For renewal or subscription information, call customer service at 800-650-6787, fax 800-639-8511, or email: *customerservice@hcpro.com.* • Visit our website at *www.hcpro.com.* • Occasionally, we make our subscriber list available to selected companies/vendors. If you do not wish to be included on this mailing list, please write to the marketing department at the address above. • Opinions expressed are not necessarily those of **BOH.** Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.

A focus on portable devices

But Pabrai says some of the details of the 450-day CAP surprise him. For one, he is intrigued by the provision that BCBST must randomly audit facilities using portable devices.

Specifically, BCBST must conduct unannounced audits of its facilities that house portable devices and audit 25 BCBST workforce members in total who use portable devices. The CAP defines "portable devices" as portable or mobile devices and external hardware that contain, store, or are used to access ePHI.

"That's really something we have not seen before," says Pabrai. "They are making them randomly audit their facilities that house portable devices. The fact they are saying it should be done randomly and unannounced shows they are serious about this. There's a lot the industry can learn; we must all be proactive in enabling a resilient and compliant organization."

That said, here are some lessons healthcare organizations can take from BCBST's CAP:

➤ Update your policies and be sure they address technology you may have added since they were originally written—such as portable devices. Many organizations do not have an updated mobile or portable device policy in place, and if they do, often the policy is not aligned with the organization's actual practice, Pabrai says.

➤ Review the findings from the Office of Inspector General's May 2011 report, Pabrai advises. The report, *Audit of Information Technology Security Included in Health Information Technology Standards,* includes recommendations in the areas of securing wireless networks, adequate system patching, integrated and automated system event logging, minimizing shared user accounts, and controlling excessive user access and administrative rights, he says.

➤ Make sure training is robust. Communicate your policies effectively to your workforce. Document your training and be sure it covers portable devices. Develop meaningful scenarios to help train your workforce members. What happened at BCBST can help educate staff members, Pabrai says.

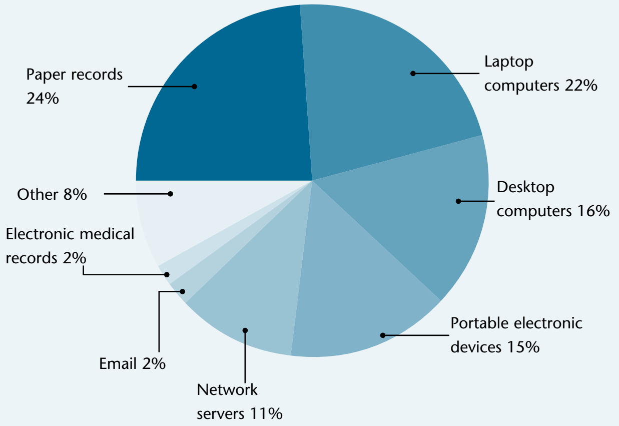
➤ Monitor the use of portable devices. Have an active program in place to do this. Your HIPAA security officer or compliance officer should schedule regular monitoring, Pabrai says. For example, he or she should walk through patient floors every so often—say, every three or six months—and see what is going on. Are physicians using portable devices? If so, are they following your policies? "We don't see evidence of that. In the CAP, OCR shows it is very serious about it," Pabrai says. "Ensure they are reviewed on a regular basis."

An OCR spokeswoman in an interview with BOH reinforced the importance of regular monitoring. She suggested organizations review OCR's *Guidance on Risk Analysis Requirements Under the HIPAA Security Rule*, which addresses the importance of periodic review and facilities updating their risk assessment. You can find the guidance by visiting *www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.*

"There are some very strong statements in this guidance on the importance of a routine, ongoing monitoring to help reduce associated risks to reasonable and appropriate levels," the spokeswoman said.

The causes of unsecured PHI affecting 500 or more individuals

According to OCR, here's how causes of PHI breaches reported to the agency are broken down:



Source: Leon Rodriguez, director of OCR (from a presentation given March 26 at the 20th National HIPAA Summit in Washington, D.C.).

➤ Look at past security incidents. The interim final rule on breach notification went into effect in August of 2009, only months before the BCBST breach. Pabrai says entities should take note that OCR is willing to go back years to investigate breaches.

"Go back and document as much detail as you can on your security incidents," Pabrai says. "Ensure you address all areas as outlined in the breach notification form; go beyond those requirements so such incidents are not repeated in the future. The bottom line as a result of this OCR action is that all organizations—covered entities and business associates—are responsible for establishing and driving a carefully designed, delivered, and monitored HIPAA compliance program." ■

Editor's note: Want to read more about the BCBST settlement? Go to http://tinyurl.com/cy6axsy *to read a Q&A with OCR plus more coverage and commentary from our expert sources.*

HIPAA/HITECH final rules, finally?

Healthcare organizations could see the long-awaited final rules for HIPAA/HITECH before the end of June.

OCR officials, announcing the news at the 20th National HIPAA Summit in March, sent the final rules to the Office of Management and Budget (OMB) March 24 for review.

From that date, OMB has 90 days to complete its review of the new regulations—the final step before OCR releases the modifications to the HIPAA privacy, security, enforcement, and breach notification rules.

Because of the large number of rules from many government departments now awaiting OMB clearance, **Susan McAndrew, JD,** OCR's deputy director for health information privacy, predicted it will take OMB the entire 90 days to get the review done.

"I fully expect 90 days is what it will take to get through OMB," McAndrew said March 26 when she spoke at the summit, held at the Renaissance Hotel in Washington, D.C. That means it will be late June before OCR can publish the final rules.

Because of the long delay on these final rules, some people are taking a wait-and-see approach to their advent. "The final rules may be [released] on or about June 25. I wouldn't bet the farm," said **John C. Parmigiani,** cochair of the summit, in a presentation the day following the OCR announcement. Parmigiani, president of John C. Parmigiani & Associates, LLC, in Ellicott City, Md., is skeptical since OCR has already taken more than 18 months to release final rules to the healthcare industry.

OCR packaged four HIPAA-related rules into a single submission to the OMB, under the title "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules." The final rules will include:

- ➤ Modifications to the HIPAA Privacy and Security Rules, including changes to comply with HITECH—namely making business associates (BA) and subcontractors liable and responsible for Security Rule compliance and the use and disclosures provision of the Privacy Rule
- ➤ Enforcement (new penalty levels)
- ➤ Breach notification
- ➤ Modifications to the HIPAA Privacy Rule as required by section 105 of the Genetic Information Nondiscrimination Act of 2008

OCR also plans to publish guidance to help healthcare organizations comply with the new final rules, said McAndrew. The guidance will include BA contracts, de-identification, and how to conduct a risk assessment to determine whether a breach occurred.

The contents of this guidance suggest that OCR's final rule is preserving a controversial provision of the interim final rule on breach notification: the harm threshold assessment. This threshold allows entities to conduct their own risk assessments on breaches before notifying affected individuals. If the breach is considered to have no financial or reputational harm, entities don't have to notify patients.

Many in the industry—particularly some members of Congress—called for the harm threshold to be removed because, they said, patients should always know when their information may have been breached.

When asked during a question-and-answer period following her presentation, McAndrew did not say whether the harm threshold standard is included in the final breach rule. Organizations will still need to conduct a risk assessment and, if a breach occurred, determine whether the incident compromised the privacy or security of their information, she noted.

Organizations can expect OCR's guidance to include an updated sample contract for BAs to help with contracts they will need to rewrite, McAndrew said. OCR will allow a "generous amount of time" for organizations to rewrite those contracts given the new final rules, she indicated.

HITECH included new privacy requirements allowing for stronger individual rights to access electronic health records (EHR) and restrict the disclosure of certain PHI. Those provisions are addressed in the final rules. According to McAndrew, the final rules will:

- Strengthen protections on the use of PHI for marketing without an individual's authorization. If subsidized by a third party, covered entities (CE) will no longer be allowed to send marketing materials without an individual's authorization. One exception to this provision is prescription reminders.
- Address fundraising, making it easier for patients to opt out of receiving such communications.
- Address the sale of PHI. The final rule will contain a list of exceptions, but in general, CEs will be prohibited from being paid to disclose information.
- Strengthen the provision that gives patients the right to receive a copy of their health records in an electronic format if the CE uses or maintains an EHR. This will make it easier for an individual to obtain PHI from a CE in electronic form, as well as allow patients to request that information be sent electronically to a third party.
- Grant patients the right to request mandatory restrictions on disclosure of PHI for healthcare operations or payment purposes to health plans if they pay for medical costs in full and out of pocket. CEs must honor a patient's request not to share that information with his or her health plan.

One provision that won't be in this package is the accounting of disclosures proposed rule, which is still to come. McAndrew said it was not part of the final rules sent to OMB in March. ■

Initial OCR audits complete; more to come

With 20 initial "trial" audits completed, OCR expects to move forward with another 95 audits to measure HIPAA compliance before year's end, said **Susan McAndrew, JD,** OCR's deputy director for health information privacy. This represents a reduction in the number of audits (150) that were originally planned for 2012.

Additionally, healthcare organizations may soon get a look at the protocol that audit teams are using to conduct the audits, said **Michael D. Ebert,** national HIPAA services leader at KPMG, the company hired by OCR to conduct the HIPAA audits required under the HITECH Act. Both McAndrew and Ebert spoke at the 20th National HIPAA Summit held March 26 in Washington, D.C. Ebert said OCR and KPMG wanted to get through the first 20 audits, which are being used as a test phase, before publishing the audit protocol. Healthcare organizations may be better able to prepare if they know more about the protocol that audit team members follow.

Fewer audits planned

McAndrew said results are still coming in from the initial 20 audits. OCR will try to resolve any problems with the process and, when satisfied, will go forward with 95 more audits. That means OCR will conduct about 115 audits by the end of 2012—significantly less than the 150 it originally planned. OCR is now identifying the covered entities (CE) that KPMG will audit in the next wave, McAndrew said.

KPMG may be able to complete more audits if it is able to streamline the process, Ebert noted. "There will be at least another 95," he said.

Initial findings

So what is OCR discovering so far? "It really is very, very early in the process," McAndrew demurred. "We are on the second step of a path that will go through the end of this year. We are working with the auditors to assess the findings. We're just beginning to do that process. I'm not sure I'm in a position to say much more."

While McAndrew did not offer specifics, as is OCR's practice, she did offer in conversation with **Mac McMillan, CISSM,** CEO of CynergisTek in Austin, Texas, who is working as a consultant with a hospital that underwent one of the initial audits, that many of the initial audits uncovered quite a few compliance problems.

"Nearly all had significant deficiencies," says McMillan.

One organization that did fairly well in its audit was a healthcare clearinghouse that also works in the financial sector—meaning it already has strict requirements and has undergone many audits, he says, which likely contributed to their readiness.

In total, the initial 20 audits investigated eight health plans, 10 healthcare providers, and two healthcare clearinghouses.

Healthcare providers targeted in the audits included three hospitals, three allopathic and osteopathic physicians, a laboratory, a dental practice, a nursing and custodial facility, and a pharmacy.

The initial audits ended March 1, Ebert said. KPMG prepared and sent draft reports for the first 10 audits, with the other 10 reports to follow. McMillan says the hospital he is working with has reviewed its draft report and responded to the findings.

"The reporting is fairly high level, follows exactly [OCR's] published format, and yet very broad in scope," he says. KPMG's recommendations for correcting findings "were not particularly prescriptive," McMillan notes, adding there was "some considerable room for interpretation."Audit teams spent up to seven days visiting audited organizations; smaller physician offices would probably undergo shorter audits of three or four days, Ebert said. "It's validating what you have in place and what you don't have in place," he said.

And as stated earlier, audit teams *are* finding compliance problems. "We've walked into entities that are not fully compliant," Ebert said. Some organizations have hoped to have findings removed from their report if they take immediate steps to correct them, he said. However, KPMG will not remove audit findings from the final report to OCR, although organizations can note in their response that they have corrected them.

Ebert did hint at one problem uncovered in a pharmacy included in the initial audits—patient consultation areas.

He said pharmacies should carefully consider how they set up these areas, ensuring they are private enough to prevent conversations between pharmacists and patients from being overheard.

It was interesting that a major national pharmacy chain had not addressed this issue in all of its stores, Ebert said. Pharmacies should also pay close attention to how they dispose of their PHI, he noted—both paper and medication labels.

The audits are currently focused on CEs, but will expand to include business associates in subsequent years, Ebert said.

OCR plans to publish broad-level audit results as guidance for organizations, highlighting problem areas as well as best practices.

Steps to take

In his presentation, Ebert highlighted some steps organizations can take to improve HIPAA compliance, including the following:

- Conduct a robust compliance assessment, and reassess annually or biannually.
- Determine the lines of business affected by HIPAA.
- Consider internal employee information as you conduct your evaluation. Employee information is considered private by both the U.S. Department of Labor and many state laws, Ebert said. Employee information can also contain PHI, so don't overlook it when performing your review, he advised.
- Map the flow of PHI within your organization, as well as how it is transmitted to and from third parties.
- Perform data discovery to find all of your PHI.
- Establish effective PHI safeguards, such as encryption, access management, and only allowing its use when required.

Ebert also urged privacy and security officers to plan ahead for the impact of HIPAA across their organization. This includes determining possible common responsibilities and oversight of IT, information security, and internal audit functions. Organizations should assess the overlap between controls oversight and management. You need to know what you are going after, Ebert said.

KPMG will not remove audit findings from the final report to OCR, although organizations can note in their response that they have corrected them.

Privacy and security officers should also engage other impacted departments, such as human resources, early in the planning process.

Try to combine HIPAA activities with other compliance activities, such as meeting payment card industry compliance standards, Ebert said. Unify your compliance programs to increase their effectiveness and efficiency, he advised. ■

Convince your leaders to invest their dollars

Make a business case to help protect your PHI

Sure, *you* understand the value of investing in improvements that will better protect your organization's PHI. But do the senior leaders who actually hold the purse strings get it?

HIPAA privacy and security officers must learn to speak the language of their CEOs and chief financial officers (CFO), said **Rick Kam,** president and cofounder of ID Experts in Portland, Ore., and chairman of the PHI Project.

When you are sitting at the table with organization leaders during your next budget cycle, you need to be able to make a strong business case for the resources and investments required to protect your PHI, Kam said.

The PHI Project's basic goal is to make that case. The project is a collaboration of the private, nonprofit American National Standards Institute in partnership with The Santa Fe Group/Shared Assessments Program Healthcare Working Group and the Internet Security Alliance.

Construct a business case

In March, the PHI Project released a 66-page report that outlines a method for covered entities and business associates (BA) to argue for the appropriate investments needed to better protect an organization's PHI. You can download a free copy of the report, *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security,* by visiting *www.webstore.ansi.org/phi.*

"We wanted to create an approach that organizations can use to customize a business case to their situation," said Kam, who spoke at a March webinar held to explain that method.

The PHI Value Estimator—dubbed PHIve ("five")—provides a way for privacy and security officers to calculate what a breach might actually cost their organization and then build a compelling business case for strengthening their compliance program, Kam said.

"Healthcare is one of the most breached industries," **Larry Ponemon, PhD,** chairman and founder of the Ponemon Institute, said in a release about the new report. "Healthcare providers and supporting organizations don't currently have sufficient security and privacy budgets, including adequate processes and resources, to protect sensitive patient data. This report will help them understand what they need to do to augment their efforts."

Follow the money

In a 2011 survey completed by the PHI Project, 59% of respondents said a lack of funding is the biggest impediment to strong PHI security, **Mary Chaput,** CFO and chief compliance officer at Clearwater Compliance, LLC, in Nashville, said in the webinar. Another 32% of survey respondents said a lack of senior executive support stands in the way of improved PHI security. (See Figure 1 on p. 9 for more detail on the survey responses.)

So how can you get the funding you need and gain support from top executives? As you compete for organization dollars, you need to think like a CFO, said Kam.

For instance, at a budget session you might be competing with the vice president of sales, who is asking for $20 million for a new MRI center that will allow your hospital to extend its market reach into the next county. For every $1 invested, the hospital will get back $2 over the next 10 years. You're also competing with a different vice president, who is seeking $10 million for a new patient privacy portal to improve customer satisfaction. She tells senior executives that for every $1 spent, the hospital will see a return of $1.50 over 10 years. Privacy and security officers must make the same kind of monetary argument, clearly stating the value of the investments you are proposing to the organization, Kam said.

Follow these five steps

PHIve helps organizations assess their security risks and evaluates the "at risk" value of their PHI. The tool estimates overall potential data breach costs and provides a method to determine an appropriate level of investment to strengthen privacy and security programs and reduce the probability of a breach.

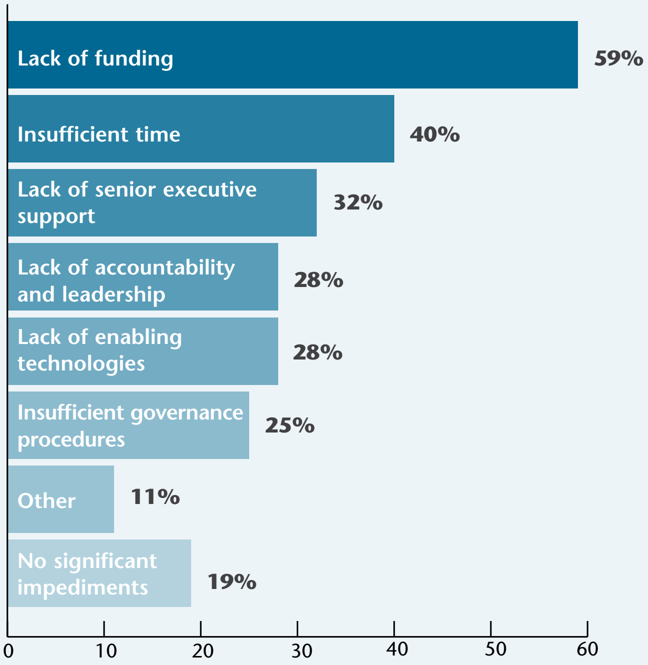
To use PHIve, organizations must take the following five steps:

➤ **Step 1: Conduct a risk assessment.** This allows you to assess the risks, vulnerabilities, and applicable safeguards and controls for each "PHI home." A PHI home is any organizational function or space (administrative, physical, or technical) and any application, network, database, or electronic system that creates, maintains, shares, transmits, or disposes of PHI or ePHI.

You'll want to list every PHI home in your organization and those of your BAs. By doing so, you'll consider potential risks such as the electronic penetration of your systems, the possibility of theft, or employee error. Is there a lack of encryption, improper disposal of written records, or lack of protection against threats to wireless connectivity? You'll rate your safeguards and controls such as your authentication of authorized users, your background checks for newly hired staff members, and your login and password management. The report has two tables that list numerous factors you need to assess.

Figure 1

What are the most significant impediments your organization faces to achieving a strong privacy and data security program with respect to how PHI is collected, used, and retained?



Source: PHI Project's 2011 PHI survey.

➤ **Step 2: Determine a security readiness score.** In this step, you will determine a score for each PHI home by determining the likelihood of a data breach based on a 1–5 scale. Is the likelihood of a breach extremely unlikely (score it a 1), or highly likely (score it a 5)? If you've encrypted all your laptop computers, your risk of a PHI breach may be virtually nil. However, if you allow the transmission of PHI through unsecured email, a breach is highly likely.

➤ **Step 3: Assess the relevance of risks and their cost.** While it is up to each organization to determine how much risk it is willing to accept, the report suggests a security readiness score of 1 or 2 might be considered acceptable and a score of 4 or 5 unacceptable. For each PHI home that you determine has an unacceptable score, you will then associate a cost with it.

A data breach can cause reputational damage, have financial implications, create legal and regulatory headaches, and present operational and clinical repercussions. Are you likely to face fines and penalties from the federal government? What will it cost to notify victims of a breach? What's the cost of providing credit monitoring to victims or hiring a public relations firm to help you control reputational damage? The report helps assess all of these things.

➤ **Step 4: Determine the impact.** The report will help your organization determine the impact of a breach based on the consequences you will likely face. For example, are you likely to experience reputational repercussions from a breach? Will you lose patients to competitors? Will you lose staff members? How about financial repercussions? Will there be an expense from changing BAs? Will there be increased insurance coverage? Will you face a class action lawsuit?

➤ **Step 5: Calculate the total cost of a breach.** Add up all adjusted costs to determine the total cost of a data breach to your organization. Where on the scale would you rate the impact of a data breach? Is it insignificant (less than 2% of revenue) or severe (greater than 6% of revenue)?

By determining the cost for failure to adequately protect PHI, privacy and security officers can calculate how much their organization should invest in those efforts based on their risk, Chaput said. They can use the data to calculate a return on investment that can help convince CFOs and CEOs to fund those improvements.

Ultimately, the above steps should allow a privacy or security officer to make a case for how much an organization should invest in privacy and security improvements, Kam said. "This provides a tool where an individual can answer when financial officers ask, 'What is the return on the dollar if I invest in this initiative?' " he explained.

Executives may underestimate the value of the PHI data their organization holds, he noted. This data can cost millions if it is lost in a breach. Using the five-step process, said Kam, your CEO and CFO may be convinced that privacy and security is a good investment. ■

Case study

Healthcare system develops mobile device checklist

Provides staff with steps to take for lost or stolen devices

Would all your staff members know what to do if their laptop computers were lost or stolen?

Well, **Nancy Davis, MS, RHIA,** director of privacy and security officer, and **Carol Saraceno,** security analyst, make sure that's the case at their organization.

Davis, Saraceno, and other leaders at Ministry Health Care in Wisconsin and Minnesota have developed a checklist that outlines the specific steps workforce members should take if a laptop computer or any mobile device is lost or stolen.

Since any of those devices have the potential to contain confidential patient, employee, proprietary, or business information, staff members must report a loss as soon as it happens, says Davis.

Even though Ministry has policies in place, Davis and other privacy and security leaders wondered whether staff members would know exactly what to do if they lost a device—particularly if the loss occurred after hours, when offices are closed and key leaders or supervisors might not be available.

So they decided a checklist would be a valuable resource to have on hand.

"We just thought it was a great idea. We have a policy, of course, but it is lengthy. People respond really well to checklists," Davis says.

Anyone might panic when they realize they have lost a laptop or other mobile device, she says. The checklist clearly guides the user and outlines the steps to take in response.

Mobile device risks

Like many other privacy and security officers, Davis worries about today's proliferation of mobile devices, such as laptop computers, tablet computers, and portable storage media. All of these might contain PHI and could lead to a breach if stolen or lost.

Ministry encrypts all of its laptop computers, but it is always a challenge to control mobile and portable storage devices. Staff members must know what to do if a device is lost, Davis says.

The data breaches reported on the OCR website, which lists entities reporting breaches of unsecured PHI affecting 500 or more individuals, clearly demonstrates that mobile devices can cause major problems for healthcare organizations.

Since OCR began posting breaches in February 2010, mobile devices have represented hundreds of breaches and exposed the PHI of more than 2 million patients. As of March 2012, OCR has received 409 reports of breaches affecting 500 or more individuals. Laptops and other portable storage devices accounted for 37% of these breaches, according to OCR statistics.

In a November 2011 survey by the Ponemon Institute, 81% of participants reported using mobile devices to collect, store, or transmit some form of PHI. However, 49% admitted their organizations do nothing to protect these devices.

Learning from experience

Saraceno came up with the idea for the checklist, Davis says. After Saraceno, Davis, and other organization leaders read an article about a vendor who experienced a PHI breach stemming from a laptop computer, creating the checklist seemed like a good plan. The vendor, who provided services to physician offices, described the steps the company had to take to remediate the problem, Davis says.

"We talked about it and based on the article, Carol suggested that we need to provide guidance to staff who may have similar experiences," she says.

While Ministry's leaders hoped staff members would know to immediately report to the IT help desk if they lost a mobile device, they decided having a checklist would reinforce the need to do so.

Getting started

Davis and Saraceno put together a small group with representatives from the IT service desk and the telecommunications department to create the checklist. They called on others as needed—the chief information officer, the vice president of human resources, and legal counsel—to review and approve the checklist.

"The checklist provides clear-cut direction where there previously was none other than reporting it as a security incident," Davis says. "The checklist clearly defines steps and responsibilities, which we like."

The list is available to staff members on the IT and privacy/security intranet sites. In addition, Davis plans to run an article in the staff newsletter and on the organization's intranet alerting people to its availability.

> **"The checklist provides clear-cut direction where there previously was none other than reporting [a lost or stolen device] as a security incident."**
>
> *—Nancy Davis, MS, RHIA*

Staff member responsibilities

The checklist covers both organization-owned and personally owned devices. It makes it clear that if staff members lose a personal device that they use to access, manage, or store any information belonging to the organization, they must report the loss as soon as possible. The list states that it is the device holder's responsibility to contact the IT service desk. It also lists the contact numbers for Ministry; its partner healthcare system, Affinity;

and its home care division. Finally, it details the type of information for which the IT service desk will ask.

"The IT help desk is always open. It's the best place to start," Davis notes.

Staff members are also advised to contact their supervisor, notifying him or her of the incident, and request a replacement device.

If the device is lost or stolen on any of the organization's campuses, staff members must contact the security or risk management department, at which point officials will contact the local police. If the loss or theft occurs externally or off the organization's property, the device owner is directed to contact police and request a copy of the police report.

Other responsibilities

The checklist also outlines the responsibilities of the IT service desk staff. They include determining whether the device is encrypted and contacting an IT manager or senior manager if it is not. The IT staff is also reminded to disable wireless service on organization-owned phones and laptop computers and tablets.

If there's a potential breach of confidential information, IT leaders are instructed to contact key system leaders depending on what kind of information may be compromised.

Remember, when it comes to the loss of information, it's not just PHI that can be problematic.

"We're trying to branch beyond HIPAA and recognize that there are other forms of confidential information at risk," Davis says. For example, devices can contain confidential employee information, as well as information proprietary to the organization.

Davis says Ministry's checklist can be duplicated in other healthcare organizations.

"They may want to have a response process in place for this, as chances are [a lost or stolen device] will occur," she says. ■

Staff newsletter promotes use of checklist

Ministry Health Care, located in Wisconsin and Minnesota, published the following article in its staff newsletter. The article alerts all staff members to the availability of a checklist with steps to follow if a mobile device is lost or stolen.

What to do if your laptop, BlackBerry, or other portable device is lost or stolen

It happens every day—laptops, tablets, BlackBerry® devices, cell phones, smartphones, or flash drives are lost or stolen. In November of last year, UCLA's system of hospitals and clinics notified 16,288 patients warning them their personal information was breached and subject to identity theft. This occurred because a computer hard drive was stolen from a doctor's home. The information was encrypted, but the password was on a scrap of paper near the computer (which was also missing). In December, a class action lawsuit was filed on behalf of the patients suing UCLA for $16 million.

A lost or stolen device that contains confidential Ministry patient, employee, or business information can result in great risk to the organization. While Ministry has in place safeguards (including encryption on laptops) to protect confidential information, there is always the need to evaluate risk when any device is missing and may contain vulnerable unsecured confidential information.

IT and corporate integrity have created a simple checklist for workforce members who experience a loss or theft of a laptop, tablet, BlackBerry, cell phone, smartphone, flash drive, or other portable device. The checklist is available on the corporate integrity and IT websites.

If you experience the loss or theft of a device, please access the list and/or contact the IT service desk immediately at XXX-XXX-XXXX or toll-free at XXX-XXX-XXXX.

Loss or theft of a device can happen to any of us no matter how careful we are. Help Ministry protect confidential patient, employee, and business information by following privacy and security policies and reporting loss or theft of devices immediately.

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

May 2012

Tips from this month's issue

Blue Cross Blue Shield breach (p. 1)

1. Update your policies to be sure they address technology you may have added since they were written, such as portable devices.

2. Ensure your policies and procedures are updated and aligned.

3. Organizations should also review the findings from the Office of Inspector General report from May 2011, *Audit of Information Technology Security Included in Health Information Technology Standards*. The report includes recommendations on topics such as securing wireless networks, adequate system patching, integrated and automated system event logging, minimizing shared user accounts, and controlling excessive user access and administrative rights.

4. Make sure training is robust.

5. Communicate policies effectively to your workforce.

6. Document your training, and be sure it covers portable devices. Develop scenarios to help train your workforce members. One scenario that can help educate staff members is what happened at Blue Cross Blue Shield of Tennessee.

7. Monitor the use of portable devices. Have an active monitoring program in place.

8. Your HIPAA security officer or compliance officer should schedule regular monitoring. For example, every three or six months he or she should walk through patient floors and see what is going on.

9. Look at past security incidents.

10. Go back and document as much detail as you can on those security incidents.

11. Ensure you address all areas outlined in the breach notification form; go beyond those requirements to ensure that incidents are not repeated in the future.

HIPAA/HITECH final rules (p. 4)

12. Know what the HIPAA/HITECH mega rule will include when published. It will:

– Strengthen protections on the use of PHI for marketing without an individual's authorization. If subsidized by a third party, covered entities (CE) will no longer be allowed to send marketing without an individual's authorization. One exception is prescription reminders.

– Address fundraising, making it easier for patients to opt out of receiving these communications.

– Address the sale of PHI. The final rule will contain a list of exceptions, but CEs will be prohibited from being paid to disclose information.

– Strengthen the provision giving patients the right to receive a copy of their health records in an electronic format if the CE uses or maintains an electronic health record. The rule will make it easier for an individual to obtain PHI from a CE in electronic form, as well as allowing patients to request that information be sent to a third party electronically.

  – Provide the right for a patient to request mandatory restrictions on disclosure of PHI for healthcare operations or payment purposes to health plans if the patient pays for medical costs in full and out of pocket. CEs must honor a patient's request not to share that information with his or her health plan.

13. However, one provision that won't be in this package is the accounting of disclosures proposed rule.

Preparing for an OCR audit (p. 6)

14. Conduct a robust compliance assessment, with an annual or biannual reassessment.

15. Determine the lines of business affected by HIPAA.

16. Consider internal employee information as you conduct your evaluation.

17. Map the flow of PHI within your organization, as well as how it is transmitted to and from third parties.

18. Perform data discovery to ensure that you find all of your PHI.

19. Establish effective PHI safeguards, such as encryption, access management, and only allowing its use when required.

20. Plan ahead for the impact of HIPAA across the organization. This includes determining possible common responsibilities and oversight of IT, information security, and internal audit functions.

21. Assess the overlap between controls oversight and management.

22. Know what you are going after in terms of compliance target areas.

23. Engage other impacted departments, such as human resources, in the early stages of the planning process.

24. Combine HIPAA activities with other compliance activities, such as those to meet payment card industry compliance standards.

25. Unify your compliance programs to increase their effectiveness and efficiency.

Privacy and Security Primer is a monthly, two-page **Briefings on HIPAA** insert that provides background information that privacy and security officials can use to train their staff. Each month, we discuss the privacy and security regulations and cover one topic. *May 2012.*