August 2012 Vol. 12, No. 8

BRIEFINGS ON HIPAA

• Privacy • Security • Transactions • Training

Too many organizations noncompliant

OCR releases data from first 20 HIPAA compliance audits

Too many healthcare organizations are receiving failing grades for HIPAA compliance, an analysis of OCR's first 20 initial audits reveals.

The biggest concern for **Linda Sanches,** OCR senior advisor and health information privacy lead for the audit program, was that some organizations have done little, if anything, to comply with HIPAA regulations.

"I was surprised to discover some entities have not put much effort into meeting their compliance responsibilities. Some had made no efforts to be in compliance," says Sanches, who discussed the results of those 20 initial audits with **Briefings on HIPAA.**

At the other end of the spectrum, some organizations are doing well with respect to compliance. **Michael D. Ebert,** national HIPAA services leader at KPMG, LLP, the company hired by OCR to conduct the audits, was surprised by how well at least one covered entity (CE) performed in the audits.

"Out of the first 20, two did extremely well," says Ebert. One was a larger, more complex organization, he says. "The other in my view was a surprise," he says. That organization (which he declined to identify) typically has struggled with HIPAA compliance, Ebert notes.

This month's tip— Learn what a compliance officer contributes to a successful and effective compliance program on p. 10.

Worse than expected

Based on the small initial sample, the conclusion is that most healthcare organizations have a long way to go with respect to HIPAA compliance.

Ebert expected to find one-third of organizations broadly compliant with HIPAA, one-third having some problems with compliance, and one-third broadly noncompliant. "Many more were noncompliant than at least I expected," he says.

The magnitude of the noncompliance, and the amount of findings or deficiencies, were also worse than anticipated. "Organizations did much worse than [OCR officials] expected," says **Mac McMillan, CISSM,** CEO of CynergisTek in Austin, Texas. "I think it was an eye-opener."

"The industry has a long way to go," says McMillan, who had an insider's look into the audit process. He was retained as a consultant to help a hospital that was selected to undergo one of the initial 20 audits.

More audits to come

As required by HITECH, OCR launched the audit program to understand how well CEs are complying with

HCPro

IN THIS ISSUE

the HIPAA Privacy Rule, the HIPAA Security Rule, and breach notification requirements. The 20 initial audits to test the audit protocol were done during the winter; OCR plans to conduct another 95 audits before the end of the year.

Sanches says the audits will be conducted in waves during the next few months. Ebert says the notification letters have been sent and audit teams are now conducting site visits at approximately 15 CEs, with more to follow.

Audit protocol released

OCR released the audit protocol on its website in late June. Access the protocol at *http://ocrnotifications.hhs.gov/hipaa.html*.

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.

OCR revised the protocol based on the initial audits, mostly eliminating repetitious questions, Sanches says.

Ebert cautions that CEs should not expect the protocol to provide a "holy grail" with respect to audits.

However, McMillan urges organizations to carefully review the protocol. "It will give you an insight into the questions that auditors will ask and what kind of activities they want to see," he says. "I think it is going to be very instructive, particularly as a tool for examining your ability to demonstrate compliance with your policies and procedures based on the protocol's questions."

Overall audit findings

The audit teams uncovered findings in all of the 20 initial audits, Ebert says. The audits included eight health plans, 10 healthcare providers, and two healthcare clearinghouses. Providers included three allopathic and osteopathic physicians, three hospitals, a laboratory, a dental practice, a nursing and custodial care facility, and a pharmacy.

Compliance with the Security Rule was much more difficult than compliance with the Privacy Rule. The

OCR advises next steps to consider

Healthcare organizations have a common question—what is necessary for HIPAA compliance?

Linda Sanches, OCR senior advisor and health information privacy lead for the HIPAA compliance audit program, suggests the following five strategies:

- Conduct a robust review and assessment. "Do a risk analysis. Look at what you are doing," she says. If you have made major changes, update your policies and procedures to reflect your current operations.
- Determine the lines of business affected by HIPAA. Many hybrid organizations exist, she says. Some business lines are covered by HIPAA and some are not.
- Map the flow of PHI movement within your organization, as well as how it flows to and from third parties. (See related article on p. 8.)
- Find all of your PHI. (See related article on p. 8.)
- Access guidance from OCR at *www.hhs.gov/ocr/privacy*.

Security Rule was responsible for 65% of the total findings, while the Privacy Rule accounted for 26% of the findings and the breach notification rule 9%, says Sanches. (Refer to the chart at right.)

However, the data doesn't reflect the fact that there are more possible overall findings under security than privacy, she notes.

Healthcare providers experienced more problems than health plans or clearinghouses. While providers comprised 50% of the audited entities, they accounted for 81% of the deficiency findings, while health plans were responsible for 16%, and clearinghouses 4%. Again, more provisions of the HIPAA rules apply to providers, with fewer requirements for health plans, Sanches explains.

Small CEs had more findings than large ones. Six of the 20 audited CEs were so-called "level four" entities—described as small providers (e.g., physician practices with 10–50 providers, or community/rural pharmacies) that make little or no use of health information technology (HIT) and have revenues of less than $50 million. They accounted for 66% of the audit findings, including 77% of privacy findings and 61% of security findings.

"These results are consistent with the findings from surveys and studies that have been conducted in the industry with respect to privacy and security," says McMillan. "Many organizations have not made compliance with the rules a priority."

Privacy findings

There were no clear-cut issues with respect to compliance with the HIPAA Privacy Rule. Privacy challenges were widely dispersed throughout the protocol with no clear trends based on CE type or size, says Sanches.

Providers accounted for 84% of privacy findings, while health plans were responsible for the other 16%. (Refer to the chart on p. 4 for a breakdown.)

The findings were scattered across the board with small numbers of findings on many privacy requirements, says McMillan. For example, with respect to administrative requirements (§164.530) there were four findings related to policies and procedures. The audit results don't say what specifically caused the findings—they could be due to an organization's failure to follow its own policies and procedures, or a lack of necessary policies and procedures, says Sanches.

Some of the major privacy issues pertained to the following:

- Review process for denials of patient access to records
- Failure to provide appropriate patient access to records
- Policies and procedures
- Uses and disclosures of decedent information
- Disclosures to personal representatives
- Business associate contracts

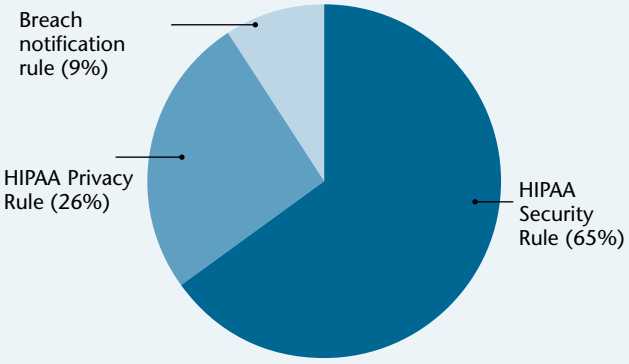
Security findings

The audit teams found a much higher level of noncompliance with the Security Rule, Sanches says. Again, there are more possible security findings than privacy findings.

"Security is a concern," she says. "Entities are facing more challenges with compliance responsibilities on security."

Analysis of overall audit findings

This chart illustrates a breakdown of the findings from OCR's initial 20 audits to assess HIPAA compliance.



Source: Linda Sanches, OCR senior advisor, health information privacy lead, HIPAA compliance audits. Access the chart at http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.

Providers accounted for 79% of the security findings, health plans 15%, and clearinghouses 5%.

Level four providers—typically small providers—accounted for 61% of security audit issues. But even level one providers—large providers or health plans with extensive use of HIT and revenues or assets greater than $1 billion—had their share of problems, accounting for 15% of security findings.

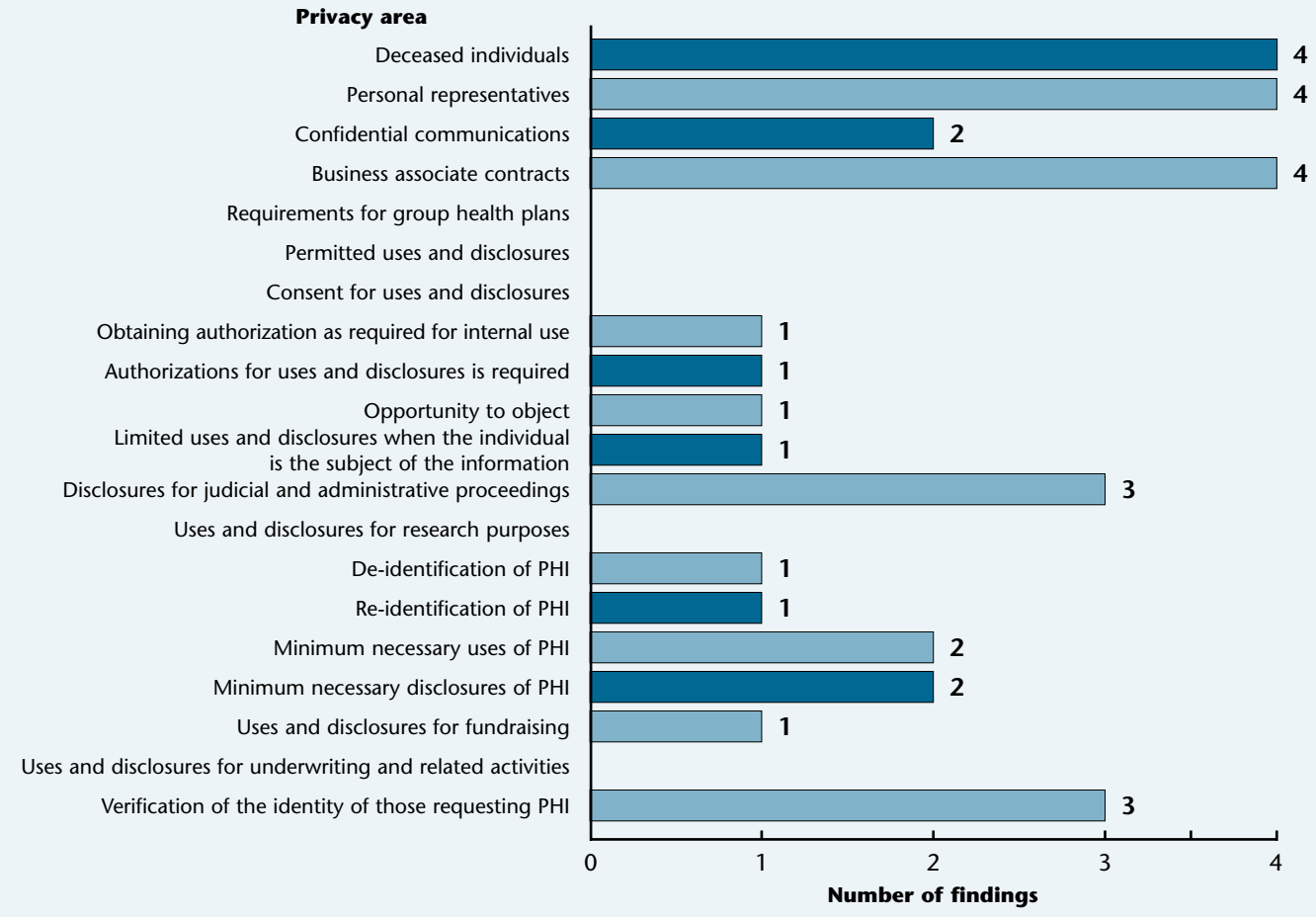
Noncompliance with administrative safeguards (§164.308) was responsible for 42.7% of findings; technical safeguards (§164.312) were responsible for 40.54% of findings; and physical safeguards (§164.310) were responsible for 16.76% of findings.

"Clearly security is the big trouble spot," says McMillan. Smaller providers are especially struggling because most have less money, time, resources, and attention available to pay to security, he says.

Unlike privacy issues where there were no clear trends, there were some security issues that resulted in large numbers of findings. (Refer to the chart on p. 5

Initial 20 privacy analysis findings: Uses and disclosures

In the first 20 initial audits conducted by OCR to assess HIPAA compliance, the agency found the following privacy findings pertaining to uses and disclosures.



Source: Linda Sanches, OCR senior advisor, health information privacy lead, HIPAA compliance audits.
Access the chart at http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.

for a breakdown.) For example, the top three problems were user activity monitoring (which accounted for 46 findings), contingency planning (resulting in 34 findings), and authentication/integrity (resulting in 19 findings).

Other major findings pertained to media reuse and destruction, risk assessment, and granting and modifying user access.

"Risk analysis is a basic requirement for a security program," says McMillan. "If it has not been accomplished or performed properly, the rest of the program would be suspect."

Preliminary observations

Various results from the initial 20 audits piqued the interest of OCR officials. "There was no major red flag for us," Sanches says. However, the agency highlighted these observations:

- **Policies and procedures.** If you have not updated your policies and procedures in the last 10 years, you have a problem, Sanches says. You must implement your policies and procedures, and they should reflect your current operations, she says.
- **Priority for HIPAA compliance programs.** Some organizations clearly have not prioritized HIPAA compliance. "Some entities have not attempted to meet their compliance responsibilities," Sanches says.
- **Small providers.** Because they don't have the same resources as larger organizations, small providers may need technical assistance and guidance, says Sanches. "We're interested in that," she says.
- **Larger entities still face security challenges.** Even larger entities struggled with security, Sanches says.
- **Conducting risk assessments.** "Risk analysis is a very important foundation," notes Sanches.
- **Managing third-party risks.** With respect to breach requirements, a CE is not on the hook for third parties if it is unaware of a compliance problem, Sanches says. However, if the CE knows of compliance issues, it must take action, she says.

Future audits

OCR plans to conduct a total of 115 audits by the end of December. The agency will review the findings to try to identify trends. "Our goal is to survey a wide range of entities," Sanches says.

Sanches and Ebert say it is likely compliance audits will continue beyond 2012. "It is our understanding the program will continue," says Sanches.

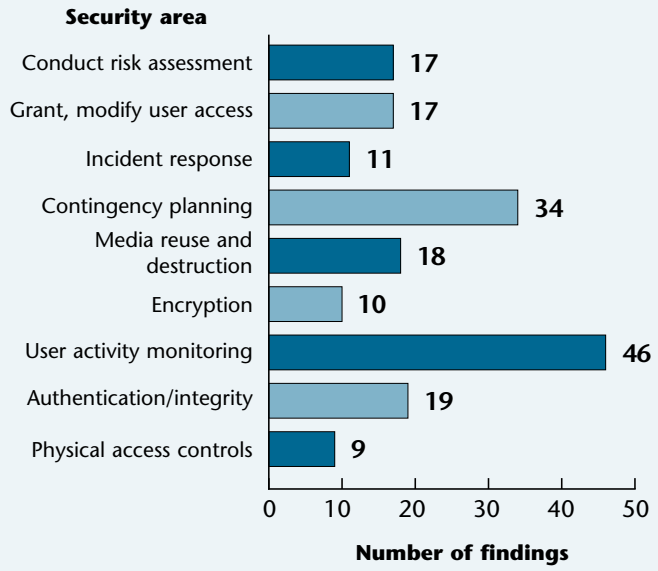
BA audits in future

OCR plans to audit business associates (BA) in a later wave of audits. These audits are in the planning stage, with the agency exploring many different options, says Sanches. "We're keenly interested in determining the best way to organize the audits of BAs," she says.

Are those audits likely to occur in 2013? "I can't address the future timing of those," Sanches says. ■

Initial 20 findings: The top security issues

In the first 20 initial audits conducted by OCR to assess HIPAA compliance, the agency found the following security findings were most frequently cited.



Source: Linda Sanches, OCR senior advisor, health information privacy lead, HIPAA compliance audits. Access the chart at http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.

What you can learn

Important takeaways from OCR audit results

Phyllis Patrick, MBA, FACHE, CHC, wasn't surprised by the results of the initial 20 OCR HIPAA compliance audits.

"I tell people, if you're doing the right things and have privacy and security programs in place, you should be okay," says Patrick, founder of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y.

However, the many findings that resulted from the initial audits, conducted last winter by KPMG, indicate that many organizations are clearly not okay.

Back to basics

Patrick's advice is to go back to the basics.

Mac McMillan, CISSP, CEO of CynergisTek in Austin, Texas, also wasn't surprised by the audit results. He and his consultants assess organizations' HIPAA compliance, and he knows that issues exist.

In the initial audits, most organizations performed far better with respect to privacy than security. The scattering of small amounts of findings across many different areas indicates no clear trends with respect to privacy shortcomings, McMillan says. His advice? Pay better attention to detail. "Organizations have programs and policies. They just are not disciplined in how they implement them," he says. "I would say to them, 'Keep doing what you are doing, but be more diligent.' "

Patrick and McMillan advise organizations to enhance their training and education. Don't rely on the same old boring methods, says Patrick."Keep it fresh, relevant, and take it to them," says McMillan.

Privacy or security

Culturally, privacy is easier to grasp, McMillan says. Understanding the importance of not discussing patients when you can be overheard or not leaving patient records where unauthorized individuals can see them is simple for staff. "It is easier to do privacy than security," he says. "It's pretty straightforward and a lot easier to get your hands around. Healthcare workers inherently understand it as part of their job."

Security is another matter. "The results for security were abysmal," he says. "From what I understand, one organization hadn't done anything."

Organizations should pay attention to security trouble spots such as encryption and proper destruction of media, he says. (See the chart on p. 5 for a list of top security findings.) "If anyone asks, 'Where are the areas where organizations have the most trouble?' this is something you can look at," he says. "Then ask, 'Where do I stand?' "

Once again, risk assessments

Audit teams found 17 findings related to conducting security risk assessments. Conduct that risk assessment, says Patrick. "Organizations should have been doing it. It's not that hard," she says.

"Those who did regular assessments performed better," says **Michael D. Ebert,** national HIPAA services leader for KPMG, LLP, the company hired by OCR to conduct the audits. A regular assessment is one completed every two years or after a major change in your organization, he says. Ensure that it is comprehensive across both privacy and security.

"A risk assessment is kind of a truth teller," says McMillan. "It is the core and basis for your compliance plan." Too many organizations have not done an assessment, or have done it poorly. Be sure your risk assessment is thorough and current.

Most organizations that had an external third party help with risk assessment fared better, McMillan says. Ebert urges organizations to use a qualified, independent source to help with assessments.

Correlate your risk assessment tools with OCR guidance and National Institute of Standards and Technology (NIST) documents that relate to HIPAA security, says McMillan. NIST is the federal technology agency that sets computer security standards for the federal govern-

ment; the OCR audits use these standards, he says.Pay particular attention to NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, available at *www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf*.

Invest in technology

Security requires money and technology, McMillan says. For example, monitoring user activity requires automated systems. Organizations must invest in people and technology, he says. "Almost all the areas where there are deficiencies are reliant on technology," McMillan notes. However, some organizations are unwilling to invest in systems to achieve HIPAA compliance, he says.

Some IT staff members hope the audit results will force leadership to give them money to address security problems, says Ebert. IT staff at some large entities approached audit teams and essentially said, 'Here's everything that's wrong,' " he says.

As part of the audit process, organizations receive a report with the audit findings and must tell OCR how they plan to address them. All of the organizations have provided corrective action plans, he says.

When organizations performed assessments and reported results to their executives, they received much more funding, Ebert says. Seek support from your C-suite and ensure that executives and board members understand the importance of compliance.

McMillan worries that the audit results give the perception that HIPAA compliance and security of patient information is not a priority. "The healthcare industry appears not even committed to doing what is right, which is not the case across the board," he says. "That, however, could be the message that is received when the audit program is reviewed next year, and that could have a real impact."

One hospital's results

McMillan was hired as a consultant by one of the hospitals selected for an initial audit. "They did fairly well. They had a number of findings, but they stayed focused on what was important about the process—learning and seeing how they could improve their programs," he says.

The organization's results were consistent with the overall results: a small number of privacy findings but more security findings, McMillan says. Most are easily addressed, but some (e.g., encryption, monitoring users) will require more investment of resources and dollars. A hospital's response to an audit report explains how it will remedy items identified, he says.

HIPAA fundamentals

OCR audits measure whether organizations understand the fundamentals of HIPAA compliance, says Ebert. "This isn't a deep dive" with auditors spending months conducting a detailed review, he says. One organization clearly understood HIPAA; it did so well that Ebert was surprised. Its chief information officer understood the principles and what was needed, and secured appropriate funding, he says. Joining IT and compliance departments in alignment and awareness is a best practice. HIPAA is a joint responsibility, Ebert says. Information security leaders should serve on compliance committees, he says. Use of identification access management is another best practice.

Focus on policies and procedures, says Patrick. Ensure they are up to date and communicate them to your workforce. The fewer policies and the simpler their language, the better, she says.

Pay attention to business associate (BA) relationships, says Patrick. Some audit findings resulted from BA contracts. Organizations that have many BAs should focus on those that handle PHI regularly, she says.

"It's not rocket science," Patrick says. If resources are tight, leverage them. For example, seek help from your internal audit department or human resources.

"We've known about this a long time. To me, there are no excuses. We've had one regulation [Privacy Rule] in place since 2003 and the other [Security Rule] since 2005," she says. "Organizations are looking for the magic bullet. They think, 'Give me the checklist.' It doesn't work that way." ■

Know where it goes: Map the flow of your PHI

If you don't know where all of your PHI is, how can you ensure that you protect it?

Linda Sanches, OCR senior advisor and health information privacy lead for the audit program, suggests mapping the flow of PHI movement internally and externally to and from third parties. It was one of the strategies she recommended during a recent presentation focusing on the HIPAA compliance audits.

With audits under way, healthcare organizations want to know what they must do to become compliant, says Sanches. (Refer to the article on p. 2 for a list of all her recommended steps.)

"[Mapping PHI] is another way of asking, 'What are your uses and disclosures?' " Sanches says. "How do you use PHI? Is it consistent with your minimum necessary policy? Is it consistent with the safeguards you have in place?" (Refer to the chart on p. 4 to learn where audit teams discovered use and disclosure deficiencies in the 20 trial audits conducted earlier this year.)

Sanches also recommends that organizations find all of their PHI. If organizations wrote their policies and procedures 10 years ago, and they have implemented new technology, they must address those changes, she says.

Time to revisit an old idea

These are valuable recommendations, says **Phyllis A. Patrick, MBA, FACHE, CHC,** founder of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y.

"Mapping of PHI was something that we talked about a lot when the HIPAA rules first came out, but the idea has lost some steam in the intervening years," Patrick says. "It is still a critical step to understanding where an organization's PHI resides and consequently possible risks associated with these areas." However, people often forget about mapping PHI. Alternatively, organizations might not maintain inventories of where their PHI resides, she says. "This goes back to the basics," Patrick says. An effective risk assessment includes identifying processes and locations where you store, receive, maintain, and transmit PHI.

Many organizations first inventoried the use and disclosure of PHI as part of their HIPAA Privacy Rule compliance, even though it was not a direct requirement. Later, the HIPAA Security Rule required organizations to complete a risk analysis to identify potential risks and vulnerabilities to the confidentiality, availability, and integrity of ePHI they create, receive, maintain, or transmit.

Update your inventory

Many organizations have already reviewed the kind of PHI they have and where it's stored and located, says Patrick. Some have continued the survey process and have current information on the location of their PHI, but many have not done this, she says.

Organizations may have added new systems and moved toward adoption of an electronic health record (EHR), Patrick says. Therefore, reexamining where your PHI resides is essential. If you last reviewed your systems when the Security Rule became effective in 2005, it's time to take another look. You will likely have a very different inventory of systems, she says.

Some covered entities (CE) have been caught short as they apply for meaningful use funds and realize they never completed a risk assessment. If you've never conducted a risk assessment that identifies your PHI and ePHI, it is time to do so, Patrick says.

You can survey your organization by taking steps such as interviewing staff or reviewing documentation. Alternatively, you may have data tracking systems that allow you to see all of the information on your network.

Mapping PHI involves looking at its flow, Patrick says. Consider where PHI comes from and where it goes. Identify the individuals and technology that handle PHI. Then determine the risk areas your organization faces.

Consider the following with respect to PHI:

- **Internal creation.** Consider both centralized sources (e.g., medical records department) and PHI that resides among employees, says **Adam Greene, JD, MPH,** a partner at Davis Wright & Tremaine, LLP, in

Washington, DC, who until last year was OCR's senior health information technology and privacy specialist. For example, are researchers creating PHI-rich spreadsheets that only they know about?

Employees often have Microsoft® Excel® spreadsheets on their computer desktops where they store PHI, says Patrick. Smaller information systems used by only a few individuals (e.g., a donor registry system that includes PHI) may also not be on the radar, she says. If you don't train staff members and they don't know your policies, they may not adequately protect this PHI, she says.

➤ **Receiving.** Are business associates (BA) creating PHI and sending it to you? What records do you receive from other CEs, including healthcare providers and health plans? Are you receiving PHI via email, flash drives, or other channels? These are the kinds of questions you should ask, says Greene.

➤ **Maintenance.** Consider both centralized and employee storage, says Greene. Do members of the workforce have PHI in their offices? If so, do they ensure that PHI is physically secure? Is ePHI stored on workstations, flash drives, compact discs, mobile devices, or personal devices? Is PHI stored on medical devices, copying machines, and other electronic devices that may include storage as a secondary function? CEs and BAs should consider that employees might store PHI in unsecure locations despite policies that require otherwise, he says.

➤ **Transmission outside the organization.** What are the authorized channels for transmitting billing and medical information (e.g., faxes, electronic health information exchange, mail)? What is the risk that PHI is transmitted through unauthorized channels, even if there are contrary policies?

➤ **Disposal.** Are central records properly destroyed? What assurances do you have from third parties that handle destruction? Is PHI being improperly discarded in publicly accessible trash? Is electronic media being properly sanitized? Ask these kinds of questions, Greene says.

Organizations should have data and document retention policies that define how long information is kept. Make sure your disposal of PHI and personally identifiable information (PII) is consistent with these policies and that the policies reflect current requirements, including retention of electronic information, says Patrick.

Think and act proactively

Assess your staff and processes so that you have a current inventory of where your PHI resides, says Patrick. Consider all the various functions and departments that use PHI, such as admitting, accounts payable, billing, clinical activities, emergency department, and HIM.

You don't have to do this alone, she says. Recruit other departments involved in the survey process. Also involve your information technology and information security experts. If you implement an EHR system, review the work flow and its effect on your PHI.

Also, expand your thinking. Patrick encourages organizations to look at PHI and all PII. Some states' breach notification laws address protection of PII, she says.

Vermont and Connecticut recently updated their breach notification laws. The modifications highlight the growing trend of states requiring notification to the state's attorney general (AG) under new compressed time frames, she says.

CEs in Vermont now have 45 days to notify residents whose information has been breached. They must provide the approximate date of the security breach and other information included in a consumer notice. Notice to the state AG is required within 14 business days. Connecticut's existing law was repealed and replaced with an amended version that clarifies the definition of a breach and adds the requirement that the AG receive notice no later than the time when notice is provided to residents.

There's a continuing trend toward use of the term PII, Patrick says. Expand the concept to include protection of all confidential information, she advises. For example, along with thinking about patient information, protect the confidential information of your employees who may participate in your insurance plan. ■

Compliance building blocks

The role of compliance officers and committees

A compliance officer is responsible for providing leadership for a healthcare organization's compliance program.

But this is not a job that the compliance officer has to do alone, says **Frank Ruelas, MBA,** principal of HIPAA College, based in Casa Grande, Ariz. Committees and other groups within a healthcare organization can help compliance officers in their mission.

A strong compliance program may be more important than ever. The Supreme Court's June 28 ruling upholding the Patient Protection and Affordable Care Act will likely trigger a floodgate of increased internal attention on compliance programs within organizations that participate in Medicare, Ruelas says. The law requires an effective compliance and ethics program as a condition of participation in Medicare.

Responsibilities

A compliance officer is responsible for day-to-day oversight, such as auditing and monitoring, and responding to related issues that may arise. He or she is often the first responder when someone reports noncompliance with HIPAA or other regulations.

Resources

Think about staffing, budget, and training. Many compliance officers, especially in smaller organizations, are a department of one. Some compliance officers may have a small staff.

Most compliance officers wear more than one hat. For example, they may also serve as their organization's privacy officer or risk manager.

Questions? Comments? Ideas?

Contact Contributing Editor Joanne Finnegan
Email *joannef100@hotmail.com*

Help from external third parties may be necessary at times. You may need outside assistance from consultants, trainers, or investigators. If you don't have the necessary resources in-house, you may need assistance from your regional or corporate headquarters. Internally, you may need to request help from other departments.

Budgets are tight, but at times you may need capital for computers or workspace. Providing training opportunities for compliance with HIPAA regulations and other standards is a large and challenging situation in many organizations, Ruelas says.

Consider specific areas you can target. Understand which regulations apply to your organization. Consider tasks which require training, such as conducting investigations or managing an effective meeting. "So often we assume a person has the skill set to accomplish a task," Ruelas says.

Consider department training. What knowledge and skills are necessary to manage a department? What do employees need to know to process payroll?

Autonomy

Compliance officers must be able to complete their responsibilities with a level of autonomy, Ruelas says. They need to make sound, logical, rational decisions without undue pressure from other entities. For example, they may need to seek legal counsel or have access to individuals within an organization.

Some issues and situations are sensitive political hotbeds that could involve individuals at the highest levels of an organization. Autonomy allows a compliance officer to decide who needs to receive a sensitive report or information (e.g., the governing body, the CEO, other senior-level officials).

Some might argue that a compliance officer needs to report directly to the general counsel, but Ruelas disagrees. Case studies dispute this organizational reporting structure, he says. General counsel represents

the best interests of the organization, and this means some filtering of information can occur, he says. The general counsel may say, "Don't worry, I will take that information to the CEO."

"If you can't verify that, you are setting yourself up for a very delicate situation," Ruelas says. The general counsel may not provide the complete picture you want the CEO or other top official to have. It is better to provide information directly.

Compliance officers may also need to seek external legal counsel. The CEO or someone at corporate headquarters should authorize the compliance officer to do this, Ruelas says. You may need the expertise of an outside legal counsel or want to have a third-party perspective on a compliance issue.

Appropriate bodies

Internal and external committees have a role to play in compliance. Internal committees could include the compliance committee, administration, and ad hoc committees. External committees could include regional, corporate, and professional associations.

A compliance committee should include various senior officers, such as the CEO or chief operating officer; ad hoc members; and directors from your various departments. Include representatives from pediatrics, surgery, emergency medicine, and other departments.

A committee generally includes standing and voting members who always participate. However, there are times when you develop an investigation and response to an issue that arises. In these cases, ensure that committee proceedings include the leaders who might be involved in that particular issue. For example, if confronted with an ethical issue, consider including your chief of staff, chaplain, or social workers in the committee discussion.

External committees could include a regional committee consisting of compliance officers from the members of a health system. Another committee could address local challenges, such as revisions in state laws.

There are few issues that another compliance officer or organization have not already addressed, Ruelas says. Take advantage of this experience and learn from what others have done.

Consider participating in corporate-level committees or in professional associations, such as your state hospital association's compliance committee. These committees can support and supplement the work of a compliance officer. ■

Editor's note: This is the second in a series on basic compliance featuring expert Frank Ruelas, MBA. In this series, Ruelas introduces those new to compliance to some basic principles proven helpful in establishing effective compliance programs.

HIPAA Q&A

Copy fees, inquiries about deceased patients

by Mary Brandt, MBA, RHIA, CHE, CHPS

Q Can you tell me whether the parent of a patient now over 18 years of age may receive information relating to a medical bill for services provided when the patient was still a minor?

A Because the patient is now of legal age, you should obtain the patient's written authorization to release this information to the parent. Alternatively, you can release the information directly to the patient, who can decide whether to share it with the parent.

Q We often receive requests from out-of-state attorneys who want us to bill for copies of records in accordance with their state laws. Should we abide by the law of the attorney's jurisdiction or Texas, where the patient underwent surgery?

A You are governed by the laws of the state where you do business. If your facility is located in Texas, charge for copies of records in accordance with Texas law. Remember that Texas law establishes a maximum fee that may be charged for copies of medical records, but you are free to charge a lower fee if you wish to do so.

Q How may an individual obtain access to health records after a patient dies? More specifically, do any provisions of HIPAA or other privacy laws allow release of records without relying on state probate law? Does your opinion differ if the situation involves a minor child and a parent who had access to the records before the child's death?

A The Privacy Rule does not establish rules for determining the appropriate legal representative for an individual after death. These rules are established by state law, so you will need to follow the hierarchy required by the laws of your state. In the case of a minor child, there is generally no will and thus no named executor. In these cases, either parent is considered the child's nearest of kin, as long as parental rights have not been severed by a court of law and no other individual has been appointed the child's legal guardian.

Q If relatives from out of state call to inquire about a deceased patient, may we provide this information without violating HIPAA? The family members call one week after the patient expires. The facility is unable to verify the relationship of these family members to the patient. What information may the facility release? Who should notify the family members that the patient has died?

A The facility directory section of the Privacy Rule (45 *CFR* §164.510) allows covered entities to release general information about a patient's condition to anyone who inquires about the patient by name, as long as the patient did not opt out of the facility directory upon admission.

In this case, telling family members that the patient expired on a certain date is permissible. A member of the clinical staff who cared for the patient (e.g., physician or nurse) should respond to the inquiry. More detailed information (e.g., cause of death) may be shared with the nearest of kin if the relationship can be verified. ■

Editor's note: Brandt is vice president of HIM at Scott & White Healthcare in Temple, Texas. She is a nationally recognized expert on patient privacy, information security, and regulatory compliance. Her publications provided some of the basis for HIPAA's privacy regulations.

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

August 2012

Tips from this month's issue

First 20 HIPAA compliance audits (p. 1)

1. Access the OCR audit protocol at *http://ocrnotifications.hhs.gov/hipaa.html.*
2. Based on the initial audits, the conclusion is that most healthcare organizations have a long way to go with respect to HIPAA compliance.
3. Compliance with the Security Rule was much more difficult than compliance with the Privacy Rule. The Security Rule was responsible for 65% of total audit findings, while the Privacy Rule accounted for 26% of the findings.
4. Privacy challenges were widely dispersed with no clear trends based on covered entity type or size. Providers accounted for 84% of privacy findings; health plans were responsible for the other 16%.
5. Some major privacy issues pertained to the following:
   - Review process for denials of patient access to records
   - Failure to provide appropriate patient access to records
   - Policies and procedures
   - Uses and disclosures of decedent information
   - Disclosures to personal representatives
   - Business associate contracts
6. With respect to security findings, providers accounted for 79% of the findings, health plans 15%, and clearinghouses 5%. Level four providers—typically small providers—accounted for 61% of security audit issues. But even level one providers—large providers or health plans with extensive use of health information technology and revenues or assets greater than $1 billion—had their share of problems, accounting for 15% of security findings.
7. Noncompliance with administrative, technical, and physical safeguards were responsible for 42.7%, 40.54%, and 16.76% of security findings, respectively.
8. Unlike privacy issues where there were no clear trends, some security issues resulted in large numbers of findings. The top three problems were user activity monitoring (46 findings), contingency planning (34 findings), and authentication/integrity (19 findings). Other major findings pertained to media reuse and destruction, risk assessment, and granting and modifying user access.
9. OCR plans to conduct a total of 115 audits by the end of December. The agency will review the findings to try to identify trends. Its goal is to survey a wide range of entities.
10. Access information about the HIPAA privacy and security audits at *http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.*

Map the flow of your PHI (p. 8)

11. Look at where you internally create PHI.
12. Look at where you receive PHI.
13. Look at where you maintain PHI.

14. Look at how you transmit PHI outside your organization.

15. Look at how you dispose of PHI.

Compliance program building blocks (p. 10)

16. A compliance officer is responsible for providing leadership for a healthcare organization's compliance program, but this is not a job that the compliance officer has to do alone. Committees and other groups within a healthcare organization can help compliance officers in their mission.

17. A strong compliance program may be more important than ever. The Supreme Court's June 28 ruling upholding the Patient Protection and Affordable Care Act will likely trigger a floodgate of increased internal attention on compliance programs in organizations that participate in Medicare. The law requires an effective compliance and ethics program as a condition of participation in Medicare.

18. A compliance officer is responsible for day-to-day oversight, such as auditing and monitoring, and responding to related issues that may arise. This individual is often the first responder when someone reports noncompliance with HIPAA or other regulations.

19. Many compliance officers, especially in smaller organizations, are a department of one. Some compliance officers may have a small staff. Most compliance officers wear more than one hat. For example, they may serve as the organization's privacy officer or risk manager.

20. Help from external third parties may be necessary at times. You may need outside assistance from consultants, trainers, or investigators. If you don't have resources in-house, you may need assistance from your regional or corporate headquarters. Internally, you may need to request help from other departments.

21. Providing training opportunities for compliance with HIPAA regulations and other standards is a large and challenging situation in many organizations. Consider specific areas you can target. Understand which regulations apply to your organization. Consider tasks which require training, such as conducting investigations or managing an effective meeting.

22. Compliance officers must be able to complete their responsibilities with a level of autonomy. They need to make sound, logical, rational decisions without undue pressure from other entities. For example, they may need to seek legal counsel or have access to individuals within an organization. Some issues and situations are sensitive political hotbeds that could involve individuals at the highest levels of an organization. Autonomy allows a compliance officer to decide who needs to receive a sensitive report or information (e.g., the governing body, the CEO, other senior-level officials).

23. A compliance committee should include various senior officers, such as the CEO or chief operating officer, ad hoc members, and directors from your various departments. Include representatives from pediatrics, surgery, emergency medicine, and other departments.

24. There are few issues that another compliance officer or organization have not already addressed. Take advantage of this experience and learn from what others have done. Consider participating in corporate-level committees or with professional associations, such as your state hospital association's compliance committee. These committees can support and supplement the work of a compliance officer.

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. *August 2012.*