December 2012 Vol. 12, No. 12

BRIEFINGS ON HIPAA

• Privacy • Security • Transactions • Training

Audits to continue in 2013, OCR process evolving

If you've listened to OCR officials recently, the audits to assess HIPAA compliance will continue in 2013.

Top OCR officials have made it clear the audit program will continue next year, says **Mac McMillan, FHIMSS, CISM,** cofounder and CEO of CynergisTek, Inc., in Austin, Texas. There will be more audits going forward; HITECH requires them, says McMillan.

However, what the audit program will look like after this pilot year is still uncertain. It remains unclear how many audits OCR will conduct in 2013 and when it will expand from the existing covered entities (CE) and begin auditing business associates (BA), McMillan says.

Privacy and security officers must stay informed, says **Dena Boggan, CPC, CMC, CCP,** HIPAA privacy/security officer at St. Dominic Jackson Memorial Hospital in Jackson, Miss. She recommends subscribing to electronic mail services and using other sources of information.

Organizations must stay up to date with respect to HIPAA, HITECH, and OCR audit activities, Boggan says. OCR officials are learning about the best ways to assess compliance in this first year of the audit program.

This month's tip—Use the sample walk-around security review policy on. p. 5 to facilitate periodic review of your organization's physical security.

The process is evolving, and the program could differ somewhat in 2013, says McMillan.

Once OCR finishes this first year of audits, an independent third party will review the audit process and make recommendations that OCR will include in a report to Congress, McMillan says. OCR will consider the recommendations and may make revisions, he says.

It's clear OCR is modifying and refining the process. The audit protocol posted on the OCR website in June has already changed, he says. New key activities have been added, so privacy and security officers must stay up to date and not rely on old checklists. For example, Privacy Rule key audit activities now include review of BA contracts and organizations' processes for making disclosures for judicial or administrative proceedings and for obtaining authorization for internal use and disclosure of PHI.

OCR has also changed the audit reports it sends to CEs after on-site visits, including modifications to format and presentation of information, McMillan says. Reports now include findings and observations. Findings are deficiencies that pertain directly to the regulations; observations are best practices that auditors prefer, but that the regulations do not require, McMillan explains. ■

HCPro

IN THIS ISSUE

OCR HIPAA audits

An inside look at how one hospital is preparing

One thing is certain.

You don't want to wait until you receive a notification letter from OCR before you begin preparing for a HIPAA audit, says **Dena Boggan, CPC, CMC, CCP,** HIPAA privacy/security officer at St. Dominic Jackson Memorial Hospital in Jackson, Miss.

Boggan began preparing her facility for a potential audit when OCR announced last year that it would launch an audit program in 2012. Before year's end, OCR plans to audit 115 covered entities (CE) to measure their compliance with the HIPAA Privacy Rule, Security Rule, and breach notification requirements.

As the privacy/security officer at the 565-bed hospital, which has more than 3,500 employees, Boggan is responsible for deciding how to prepare should the organization be randomly selected for an audit.

Boggan discussed her hospital's audit preparation during "Inside an OCR HIPAA Audit: Prepare, Plan, and Execute an Effective Audit Strategy," a recent HCPro audio conference.

Consultant **Mac McMillan, FHIMSS, CISM,** co-founder and CEO of CynergisTek, Inc., in Austin, Texas, also shared his experiences while working with several organizations that underwent audits earlier this year.

Organizations must review OCR's audit protocol along with the HIPAA and HITECH regulations, Boggan says. They must also ensure that the necessary guidelines, policies, and procedures have been implemented and updated. "Be prepared. I stress the importance of being proactive, rather than reactive," she says.

So where can healthcare organizations begin?

Audit readiness

Ask yourself some basic questions to determine your audit readiness, Boggan says.

An audit begins with a notification letter from OCR that arrives via registered mail. You'll probably know that the letter is en route, says McMillan. Someone from KPMG, the firm retained by OCR to conduct the audits, will call beforehand to confirm the identity of the individual who heads the organization (e.g., CEO, administrator, practice manager) and the official mailing address.

If OCR audits your organization, who will receive the notification letter and how will you receive word of it? What documentation exists to demonstrate your HIPAA compliance, and where is it? Which members of your organization will constitute the audit team? How often should the team meet?

The recipient of the letter at St. Dominic would be the

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.

CEO, Boggan says. She has ensured that the CEO will notify her of receipt of a letter from OCR. High-level executives often don't open their own mail, so Boggan also communicated the importance of any communications from OCR to the administrative assistant. "You don't want that letter sitting on someone's desk for seven or eight days," she says.

The clock starts upon receipt of the letter, and organizations have only 15 business days to respond with all documents requested by the KPMG audit team. OCR says organizations should have 30–90 days until auditors arrive on-site; however, one consultant recounted an instance when auditors arrived after only three weeks.

Centralized accountability

Strive for centralized accountability. Boggan uses the HIPAA audit protocol posted on OCR's website *(www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html)* to guide her audit preparations. She also relied on reports about the audit process to develop a matrix that lists the documents auditors are likely to request.

Notification letters contain a list of items that organizations must produce (e.g., policies, procedures, plans, demographic information, forms that pertain to HIPAA compliance).

Boggan's matrix includes a column that identifies which team member is responsible for specific documentation (e.g., training documentation, incident response plan). Boggan compiles the information in an Excel® workbook and includes a column for comments.

Easy retrieval requires knowing where all the documentation is, says McMillan. "This is very much an evidentiary-based audit. Demonstration [of your compliance] is really what you need to focus on," he says.

Boggan also has created a central repository for guidelines, policies, procedures, forms, and other supporting documentation. "I've created an electronic file. It's ready to go," she says.

Review documentation

Remember that the list of documents you compile is most likely unique to your organization, Boggan says. The audit protocol is evolving and already has changed. OCR has revised its protocol, so your matrix must remain current, she says.

The audit protocol serves as a guide for audit activities, says McMillan. It currently includes 169 separate procedures—81 for privacy, 78 for security, and 10 for the Breach Notification Rule.

McMillan advises reviewing documentation with four C's in mind:

- **Completeness.** Do you have a complete set of policies and procedures that describes the controls you have to ensure privacy and security?
- **Compliance.** Do these policies and procedures meet the mandate of the rules?
- **Currency.** Are they up to date and do they reflect what is actually happening in your organization?
- **Consistency.** Are your policies and procedures consistent with your practice and evidence?

Organize an audit team

Decide who should be on the team, Boggan says. Her team includes representatives from IT, HIM, administration, and patient care services. The team need not be large, but it should include key individuals.

Assign tasks, responsibilities, and deadlines to team members. Assign backups if necessary.

The audit team should review policies and procedures, she says. Before an audit is the time to determine whether they comply with current regulations and make necessary revisions. Note the dates of reviews, revisions, and implementation. Revisions are necessary whenever the regulations or your operations change.

"Don't be like Scarlett O'Hara and say, 'I'll think about that tomorrow,' " Boggan says.

Maintain audit awareness

Begin communicating now, not when the letter arrives, says Boggan. Discuss audit probability, not possibility.

Conduct a reeducation program for your workforce to ensure that HIPAA and HITECH requirements remain at

the forefront. Keep that education light and incorporate humor if you can, Boggan advises.

"Refresher training is invaluable," says McMillan.

Boggan sends workforce members an email every Friday that focuses on a HIPAA topic and includes a cartoon to make it fun.

You want your staff to be prepared to answer questions from the audit team. Education is essential for staff members' audit preparedness. "I tell people, 'It's not like *Who Wants to Be a Millionaire*®. If you are asked a question, you can't call a lifeline,' " she says.

Ensure your administration is aware of what is happening. Privacy and security officers in many organizations may get the message from administration that they can handle audit preparation on their own. But to be effective, you need buy-in and support from administrators, she says. Boggan prepares a quarterly report for administration and meets quarterly with her operational team. She says she is fortunate to have access to the CEO.

Take a walk

Conduct walking audits in your facility, Boggan says. Be the auditor and audit your organization as if it were your first visit to the facility. Look for things that might raise a red flag for a real auditor. (Refer to the sample policy for walk-around security reviews on p. 5.)

Visit with staff members often so they know you are there and available, she says. Ask staff members questions during walking audits. Stick to the basics. "I'm asking questions they should know," Boggan says.

For example, ask about the policy for disposal of paper containing PHI or the appropriate action when stepping away from a computer when an application with PHI is in use. Test staff members' knowledge of the appropriate steps if they suspect a privacy or security breach.

Doing so helps staff become accustomed to questions that auditors might ask. If you need ideas, consider the questions that are part of your workforce members' annual HIPAA reviews. For example, St. Dominic workforce members must answer approximately 50 questions derived from the regulations during their annual HIPAA assessment. The questions help ensure that they are aware of and follow the regulations.

Staff members will reflect your comfort level and confidence, Boggan says, something you should realize and remember. ■

Sample policy: Walk-around security reviews

Title: Walk-around security reviews

Policy: This organization will perform periodic reviews of our physical security to ensure that we are adhering to our security policies and procedures.

Purpose: This policy and the general rules contained herein describe a periodic observational review of security practices in our organization. This simple process serves multiple purposes. It evaluates the current state of security practices that are easily observed, identifying weak areas for remediation. It appropriately distributes security responsibility and accountability to managers throughout the organization. It shows that security is important to management. It reinforces good security practices described in workforce training. It provides evidence of security compliance monitoring by this organization.

Scope: These walk-around audits or reviews will be performed in all our facilities. This policy also may apply to the facilities of our agents and trading partners, depending on the terms of the relationship. The audit/review includes only security practices that can be observed (seen, heard). It is noninvasive and nontechnical. Hence, it does not constitute a comprehensive security review, but is nonetheless an important security tool.

General rules

1. The information security officer (ISO) and facilities management director will coordinate and oversee performance of periodic facility security reviews.
2. Reviews will be performed quarterly, or more often if needed.
3. Department heads will be responsible for performing, or overseeing the performance of, the review for their areas. At any time, a review may be performed by the ISO, the facilities management director, or designee.
4. Reviews will be performed using a standard checklist (paper or electronic) prepared by the ISO and facilities management director, in collaboration with the privacy officer.
5. Any "yes" response, indicating a problem, will require further details describing the circumstances (for example, the name of the individual who failed to log off, or the location of an overflowing shredding bin). If the issue is resolved immediately, that should be indicated on the form. The person performing the review will sign and date the form. Completed forms will be sent to the ISO.
6. The ISO will ensure that forms are returned when due. The ISO will review completed forms and assess any "yes" responses to determine whether follow-up is needed. For example, the ISO may identify a pattern of problems and schedule a workforce security training session with that department. Or the ISO may determine that a particular situation calls for disciplinary action because it violates policy and puts organization information at heightened risk. (In that case, a security incident report should be completed and the incident response process followed.)
7. The ISO will summarize responses and the overall status, and report the results to organization senior management, as appropriate.
8. This process is not intended to be punitive. However, where security practices do not meet organization policy, standards, and training, the manager and the ISO will follow up and remediate the problem. In some cases, disciplinary action may be warranted.

Source: The No-Hassle Guide to HIPAA Policies: A Privacy and Security Toolkit *(updated for 2009), published by HCPro, Inc.*

CMS receives failing grade for breach notification

If you think complying with all of the HIPAA breach notification requirements is difficult, you're not alone.

CMS, the government agency once responsible for enforcing HIPAA security requirements, received a failing grade for compliance with the breach notification requirements implemented pursuant to the HITECH Act.

CMS did not meet several requirements with respect to reporting 14 breaches of PHI, according to a report by the Office of Inspector General (OIG) issued in October. The OIG said it prepared the report because of its concerns about medical identity theft.

Notification problems

CMS, which maintains the PHI of millions of Medicare beneficiaries, reported that it experienced 14 breaches of PHI that required notification between September 23, 2009 (when the notification requirements became effective) and December 31, 2011. The breaches affected 13,775 Medicare beneficiaries. CMS notified these individuals, but it did not meet all of the breach notification requirements, the OIG report said.

For example, CMS didn't always meet the time frame for sending the notifications or include all of the necessary information in the notices.

"I think it's a case of 'do as I say, not as I do,' " says **Chris Apgar, CISSP,** CEO and President of Apgar & Associates, LLC, in Portland, Ore.

"My first reaction is that the 'cobbler's children don't have shoes,' maybe because they are so resource-constrained that they can't afford the leather to make them," says **John C. Parmigiani,** president of John C. Parmigiani & Associates, LLC, in Ellicott City, Md., who at one time worked at CMS.

Apgar wondered whether CMS would face any fines from OCR as a result of its failure to comply with the breach notification rules. "CMS is a [covered entity (CE)] and should live up to the same rules," he says. "It's not a good message to send out."

However, Parmigiani says CMS is struggling like so many others organizations. "CMS, like other covered entities, [is] still feeling their way in developing a very granular, efficient breach notification process," he says. "This is a continuous improvement effort that eventually will result in comprehensive databases of patients—or beneficiaries in CMS' case—with sensitive triggers to quickly respond to potential breaches to guard against unauthorized access to medical records and to mitigate harm and medical identify theft."

The OIG report acknowledged that CMS has made progress with respect to medical identity theft. CMS has developed a compromised Medicare numbers database for its contractors. But the OIG said the agency could improve the database's usefulness.

The OIG report said contractors do not consistently

Breaches requiring notification reported by CMS (September 23, 2009–December 31, 2011)

Breach	Number of breaches	Number of affected beneficiaries
Medicare Summary Notice printing error	1	13,412
Beneficiary information posted online	2	190
Mismailings or loss during transmit	10	165
Stolen beneficiary information	1	8
Total	14	13,775

Source: October 2012 OIG report, CMS Response to Breaches and Medical Identity Theft.
Access the report at https://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf

develop edits to stop payments on compromised Medicare numbers. It said contractors vary in the extent to which they develop edits for compromised numbers and differ in the types of edits they develop. CMS offers some remedies to providers, but fewer remedies are available to beneficiaries affected by breaches, the report said.

What went wrong

CMS' breaches generally involved beneficiaries' names, Medicare identification numbers, dates of birth, diagnoses, and services rendered, according to the OIG report. (The chart on p. 6 lists the causes of the breaches.)

Failure to meet notification requirements

CMS notified all of the beneficiaries affected by the 14 breaches, but it didn't meet the time requirement for mailing notification letters in seven cases. According to the Breach Notification Rule, CEs must notify individuals "without unreasonable delay" and no more than 60 days after they discover the breach.

In some cases, notification was sent four days after the 60-day period expired. In others, notification was sent more than four months after the deadline, the OIG report said. The notification letters for the largest breach were sent within the required time frame.

Notification letters often lacked required information, the report said. (Refer to the chart below.)

Media outlets must be notified when a breach affects 500 or more residents of a state or jurisdiction. CMS complied with the time requirements but failed to include steps that affected individuals should take to protect themselves. In its response to the OIG findings, CMS said that its policies and procedures reflect the breach notification requirements. Problems arose with respect to following them.

CMS said it will develop new procedures and/or modify existing ones to improve the breach notification process. It will also analyze its current process to identify gaps and make improvements.

The OIG recommended that CMS do the following:

- Ensure that breach notifications meet ARRA (PL 111-5) requirements, including time constraints and required information
- Improve the compromised Medicare number database
- Provide contractors guidance with respect to using database information and implementing edits
- Develop a method for ensuring that beneficiaries who are victims of medical identity theft retain access to needed services
- Develop a method for reissuing Medicare identification numbers to beneficiaries affected by medical identity theft ■

Editor's note: Access the OIG report at https://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf.

CMS breaches and Recovery Act notification requirements

Notification requirement	Number of breaches not meeting requirement
Failed to send notification within 60 days of breach's discovery	7
Failed to provide description of breach investigation, loss mitigation, and protection against further breaches	6
Failed to include date breach occurred or was discovered	7
Failed to provide types of PHI involved, contact procedures, or steps to protect from harm	3

Source: October 2012 OIG report, CMS Response to Breaches and Medical Identity Theft.
Access the report at https://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf

What you can learn from CMS' breach notification mistakes

When the federal government's top healthcare agency fails to meet breach notification requirements, there are important lessons to be learned.

An October report from the Office of Inspector General (OIG) reveals that CMS notified individuals affected by 14 breaches of PHI but failed to meet all of the requirements of the Breach Notification Rule. (Refer to the related article on p. 6.)

The lesson for healthcare organizations? Be certain you are prepared to respond to a privacy or security breach, advise healthcare attorneys and consultants.

"It is disappointing that CMS, acting as the largest health plan in the country, has failed to satisfy the breach notification requirements," says **Adam H. Greene, JD, MPH,** a partner at Davis Wright Tremaine, LLP, in Washington, D.C. "The breaches in question are not especially large, and health plans dealing with far larger breaches have been able to meet their deadlines," says Greene.

Until recently, Greene worked at OCR, the agency responsible for enforcing HIPAA and the Breach Notification Rule. "I was especially surprised that, apart from the delays, the notifications themselves were not compliant in many cases," he says.

John R. Christiansen, JD, principal of Christiansen IT Law in Seattle, says he's not surprised that CMS has experienced breaches. "I think this just confirms what I always tell my clients: Always start by assuming you will have a security breach, sooner rather than later," he says.

What is the reason? "Security is not easy," he says. "Systems are complex and risks cannot be eradicated.

Five tips to help ensure patient privacy

Despite efforts to prevent data breaches in healthcare, they continue to cause alarm.

Almost 20 million patient health records have been compromised in the past two years, according to statistics from HHS.

OCR, the agency that enforces the HIPAA Privacy and Security Rules, broke the 500 mark in October for the number of large breaches posted on its breach notification website. At presstime, OCR reported 502 patient-information breaches affecting 500 or more individuals since the agency began posting the information, as required by the HITECH Act, in February 2010. Access the website at *www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.*

The American Hospital Association (AHA) brought together senior executives from healthcare, information security, compliance, and legal backgrounds in September to discuss best practices for creating a culture of patient privacy compliance.

So how can you help make patient privacy part of your organization's DNA? Consider the following best practices to minimize data breach risks and create a culture of patient privacy compliance:

Encrypt

Encrypt, encrypt, encrypt, says **Kimberly B. Holmes, Esq.,** deputy worldwide product manager for healthcare at the Chubb Group of Insurance Companies in Warren, N.J.

"While there currently are no federal minimum standards or guidance around the quality and level of encryption that should be implemented to secure PHI, having some form of encryption applied to all PHI—and especially to PHI that is stored on mobile and portable devices—mitigates the risk of potentially serious HITECH fines or penalties when a breach occurs," says Holmes.

Prepare

Prepare for a breach, says **Cheryl A. Parham, Esq.,** associate general counsel at New York-Presbyterian Hospital in New York City.

"Identify first responders with knowledge of your organization as well as the rules regarding notification and

The larger your organization is, the more prominent a target you are—though of course size doesn't matter that much." For example, Christiansen recently helped a two-partner physician office respond to a rather costly breach.

"So I'm not surprised CMS experienced breaches. It's a very big target and it has a lot of complex systems. Frankly, I'd have been surprised if it were found they hadn't had breaches," he says.

However, the agency didn't respond adequately and this is where healthcare organizations can learn some important lessons from the OIG report.

Be ready to respond

"If you start by assuming a breach, you realize the importance of being ready to respond," says Christiansen.

Christiansen was involved in the breach response to one of the first major breaches in healthcare, which occurred after the California breach notification law became effective. Response requirements were not common at the time and no one really knew what to do, which made it very difficult for the organization, he says.

Breach notification requirements are now a matter of law, and they describe the actions a healthcare organization must take if a breach occurs.

Test policies and procedures

Most organizations have at least adopted policies and procedures for breach response, Christiansen says. However, most probably haven't tested them, which healthcare organizations must do to identify flaws or gaps and ensure those policies and procedures are workable, he says.

CMS responded to the OIG report by stating that it has policies and procedures in place, but that it did not follow them in all instances.

reporting. When a breach occurs, find out the facts first, then respond—but do it in a timely way," she says.

Assess compliance

Conduct a privacy and security compliance assessment annually, says **Doug Pollack, CIPP/US,** chief strategy officer at ID Experts in Portland, Ore. "A key action for your healthcare organization to reduce your risks of being fined by OCR is to have a privacy and security compliance assessment carried out every year, and to clearly document the remedial actions that you've taken to address the most severe patient data privacy risks that were identified," he says.

Close gaps

Find the gaps and close them, says **Meredith Phillips, MHSA, CHC, CHPC,** chief privacy officer at Henry Ford Health Systems in Detroit. "When engaging with OCR, be a partner and show that you are being proactive," she says. "When we look at our programs, we see where there are some gaps and we tell OCR what we are going to do to fix the gaps and report back. We want to show that we are taking action to correct any issues."

Focus on prevention

Focus on prevention efforts, preparation, and a well executed response plan, says **Marcy Wilder,** partner and co-chair of the global privacy and information management practice at Hogan Lovells in Washington, D.C.

"Prevention efforts, preparation, and a well-executed response plan can go a long way toward mitigating the financial, legal, and reputational harm that a security incident involving patient information can cause," she says.

"Whether a breach begins with an external attack, employee malfeasance, or an innocent mistake, an organization's initial response can help minimize harm to affected individuals and manage the risks to which an institution is exposed. To start, have a written post-breach response plan ready and tested before a breach happens," she says.

The group was clear with respect to the direction that healthcare organizations should take, says **Michelle Collins,** marketing director at AHA Solutions. They need interdisciplinary incident response teams, she says.

"The report doesn't really comment on the adequacy of CMS' policies and procedures, which probably means they are facially appropriate, but because of the basic failures in some of the notifications and the inadequacy of some of the response procedures it identifies, I suspect there was little or no testing," says Christiansen.

Exercises designed to test the ability of your organization to respond to a situation, in this case a breach, take time, but can really pay off, he says.

Establish systems for notification compliance

Ensure that notification letters sent meet legal requirements. "I think it's a lesson to any covered entity [CE] to ensure that systems are in place to check the content of breach notifications before they go out," says Greene.

Tools can help you comply. "It may prove helpful for organizations to include checklists and templates as part of their incident response program and procedures to ensure these tools are used," Greene says.

For example, the OIG report noted that the Breach Notification Rule requires notification to each affected individual to include the following information:

- A description of what occurred, including the dates of the breach and its discovery, if known
- The types of unsecured PHI involved
- Steps individuals should take to protect themselves from potential harm
- A description of how the CE is investigating the breach, mitigating losses, and protecting against further breaches
- Contact procedures for individuals who want to learn more

Document breach response

Carefully document what you do, says **Chris Apgar, CISSP,** CEO and president of Apgar & Associates, LLC, in Portland, Ore.

OCR currently is auditing CEs for compliance with the HIPAA Privacy Rule, Security Rule, and breach notification requirements. If you are audited by OCR, you must demonstrate that you met the breach notification requirements, Apgar says.

Now is a good time for organizations to put their houses in order, says **John C. Parmigiani,** president of John C. Parmigiani & Associates, LLC, in Ellicott City, Md. "Scrutiny by the OIG of CMS should serve as an additional clarion call to the healthcare industry—both CEs and their business associates—that regulatory enforcement at the federal and state levels is being emphasized and strengthened in efforts to curb fraudulent activities and impermissible accesses and disclosures," he says. ■

HIPAA Q&A

Security cameras, UB-04 forms, unreviewed test results

by Mary D. Brandt, MBA, RHIA, CHE, CHPS

Q Our hospital recently installed security cameras throughout the facility. A physical therapy aide is concerned about a camera focused on the treatment table and thinks this violates HIPAA. I also consider this inappropriate, but I am unable to find a HIPAA regulation that addresses this situation.

A No specific section of the Privacy Rule addresses this issue, but your concerns are appropriate. The security camera should not be focused on a treatment table because this violates patient privacy. Instead, the security camera should focus on nonpatient treatment areas, such as entrances and exits, which may be of more concern from a security perspective.

Both CMS and Joint Commission surveyors are attuned to this type of privacy violation and are likely to cite this as a violation of patient privacy if they become aware of it during a survey.

Q Do I have the right as a Medicare beneficiary to access the UB-04 form that a hospital submits as a bill for payment to Medicare? May I access and receive a copy of my coding abstract? I understand that these documents are part of the electronic data that is part of my record, which is considered part of the designated record set.

A The Privacy Rule gives you the right to access records in the designated record set. This is defined as information used by a covered entity to make decisions about individuals. For providers, the designated record set includes medical and billing records. For health plans, the designated record set includes enrollment, payment, claims adjudication, and case management records.

The UB-04 form is a billing record, so it is part of the designated record set to which you have access.

The coding summary is an administrative record and may not be considered part of your medical record. If the covered entity defines the medical record to exclude administrative records, such as coding summaries, the covered entity may deny your request to access your coding summary. However, codes that were submitted for billing will appear on the UB-04.

Q Our records system is still paper based. Patients sometimes request copies of their records before their physicians have reviewed and signed off on the documents or test results.

May we give patients copies of records and/or test results not yet reviewed by their physicians? May we accommodate patients by providing these records but identifying them as "unreviewed" so patients know that physicians have not reviewed them?

A You may release "unreviewed" test results to patients upon request if your organization's policy permits this. You may designate these results as "preliminary" or "unreviewed" if you choose to do so. If your organization does not address this in a formal policy, consider developing a policy with medical staff input. You may agree on a reasonable time for physician review (e.g., 48 hours) after which results may be released to patients even if the provider has not reviewed or signed off on them. ■

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.

Product watch

Spectrum offers attractive option for EHR conversion

by Chris Apgar, CISSP

As increasingly more healthcare providers transition to electronic health records (EHR), the need for secure conversion of paper charts to electronic patient documentation also increases.

Spectrum Information Services NW, Inc. (Spectrum) is a vendor worth seeking out; it provides a solution that is cost-effective and secure.

Spectrum specializes in customized and secure medical records conversion. The service focuses on converting paper charts and converting only the documents necessary to create a complete patient record electronically and minimizing post-conversion paper chart retention. Most importantly, charts are securely converted and paper charts are destroyed after conversion and validation.

The functionality generally exists to support manual conversion by a healthcare provider to an EHR, but it can be labor-intensive and time-consuming. It also can result in the breach of PHI if paper charts are not properly destroyed after conversion. Also, if a converted chart is incomplete or an important part of the record is not converted, the result is loss of integrity, a HIPAA Security Rule violation, and potential harm to patients. Spectrum has partnered with several EHR vendors to directly convert paper charts into EHRs, thereby protecting the integrity of the soon-to-be electronic patient records.

Several providers have contracted with Spectrum for complete rescanning of projects whose initial results included poor quality, lost files, and intermingled patient information. Spectrum uses a project management approach that appears to reasonably ensure accurate, legible, and complete conversion of all documents. Its project management approach also protects against intermingling patient records from different healthcare providers.

Spectrum claims to ensure compliance with the HIPAA Security Rule and the so-called "mini security rule" in the HIPAA Privacy Rule. Compliance includes enforcing required security policies and strong physical safeguards to protect paper charts scheduled for conversion. Spectrum provides ongoing HIPAA training for its workforce and retains an independent auditor who conducts an annual HIPAA compliance assessment. When contracting with business associates, it's important to reasonably ensure that they have sufficient resources to indemnify covered entities in the event of a breach of PHI, litigation, or other action that could harm covered entities. Spectrum also carries sufficient liability insurance to protect covered entities in the event indemnification is needed.

Requiring vendors to provide documentation regarding HIPAA compliance and the implementation of a sound security program is always wise. Spectrum appears to have implemented appropriate security controls, but verifying any statements it makes in this regard remains a good idea. Also remember to include indemnification language in this and all other business associate contracts.

Document conversion can result in a breach of unsecure PHI and loss of patient record integrity. Both are significant risks, and Spectrum can help minimize the security risks associated with paper file conversion. ■

Editor's note: Apgar is president of Apgar & Associates, LLC, in Portland, Ore. He has more than 17 years of experience in information technology and specializes in security compliance, assessments, training, and strategic planning.

To access additional information about Spectrum, visit www.sisnwinc.com.

Questions? Comments? Ideas?

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

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

December 2012

Tips from this month's issue

OCR HIPAA audits (p. 1)

1. OCR audits to assess HIPAA compliance will continue in 2013. There will be more audits going forward; HITECH requires them.
2. It remains unclear how many audits OCR will conduct in 2013 and when it will expand from the existing covered entities (CE) and begin auditing business associates.
3. When OCR finishes this first year of audits, an independent third party will review the audit process and provide recommendations that OCR will include in a report due to Congress in early 2013.
4. The audit protocol posted on OCR's website in June has already changed. New key activities have been added, so privacy and security officers must stay up to date and not rely on old checklists.
5. OCR has changed the audit reports that it sends to CEs after on-site visits, including modifications to format and presentation of information. Reports now include findings and observations. Findings are deficiencies that pertain directly to the regulations; observations are best practices that auditors prefer, but that the regulations do not require.

Sample policy: Walk-around security reviews (p. 5)

6. While not explicitly required by the HIPAA Security Rule, it is standard practice to conduct a physical security audit periodically by simply walking through an area or building, looking for vulnerabilities.
7. Adopt a policy that includes general rules for periodic observational review of security practices in your organization. This simple process serves multiple purposes. It evaluates the current state of security practices that are easily observed, identifying weak areas for remediation. It appropriately distributes security responsibility and accountability to managers throughout the organization. It shows that security is important to management. It reinforces good security practices described in workforce training, and it provides evidence of security compliance monitoring by your organization.
8. This policy also may apply to the facilities of an organization's agents and trading partners, depending on the terms of the relationship. The audit/review includes only security practices that can be observed (seen, heard). It is noninvasive and nontechnical.
9. Reviews should occur quarterly or more frequently if necessary.
10. Department heads should be responsible for conducting or overseeing the performance of the review of their areas.
11. Reviews should be conducted with a standard paper or electronic checklist prepared by the information security officer (ISO) and the facilities management director in collaboration with the privacy officer.
12. The process is not punitive in intent. However, where security practices do not meet organization

policy, standards, and training, managers and the ISO should follow up and remediate any problems. In some cases, disciplinary action may be warranted.

Breach notification compliance (p. 6)

13. An October report from the Office of Inspector General reveals that CMS notified individuals affected by 14 breaches of PHI, but failed to meet all of the requirements of the Breach Notification Rule. The lesson for healthcare organizations? Be certain that you are prepared to respond to a privacy or security breach.

14. Most organizations have at least adopted policies and procedures for breach response. However, most probably haven't tested them, which healthcare organizations must do to identify flaws or gaps and ensure those policies and procedures are workable.

15. Ensure that notification letters sent meet legal requirements. Implement systems to check the content of breach notifications before they are sent.

16. The Breach Notification Rule requires that notification to each affected individual include the following information:
- A description of what occurred, including the dates of the breach and its discovery, if known
- The types of unsecured PHI involved
- Steps individuals should take to protect themselves from potential harm
- A description of how the CE is investigating the breach, mitigating losses, and protecting against further breaches
- Contact procedures for individuals who want to learn more

17. Now is a good time to put your house in order. Government scrutiny should serve as a clarion call to the healthcare industry that regulatory enforcement at the federal and state levels is being emphasized and strengthened in an effort to curb fraudulent activities and impermissible accesses and disclosures.

18. Carefully document what you do. OCR currently is auditing CEs for compliance with the HIPAA Privacy Rule, Security Rule, and breach notification requirements. If you are audited by OCR, you must demonstrate that you met the breach notification requirements.

19. Always start by assuming you will experience a security breach, sooner rather than later. Security is not easy; systems are complex and risks cannot be eradicated.

Best practices to protect patient privacy (p. 8)

20. No federal minimum standards or guidance exist with respect to the quality and level of encryption necessary to secure PHI, but some form of encryption applied to all PHI, especially that stored on portable devices, mitigates the risk of potentially serious HITECH fines or penalties when a breach occurs.

21. Prepare. Identify first responders with knowledge of your organization and the rules regarding notification and reporting. When a breach occurs, obtain the facts first and then respond in a timely fashion.

22. Conduct a privacy and security compliance assessment annually.

23. Find the gaps and close them. When engaging with OCR, be a partner and show that you are being proactive.

24. Focus on prevention efforts, preparation, and a well-executed response plan. This can go a long way toward mitigating the financial, legal, and reputational harm that a security incident involving patient information can cause.

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. *December 2012.*