April 2012 Vol. 12, No. 4

Briefings on HIPAA

• Privacy • Security • Transactions • Training

Hospital undergoes one of first OCR trial audits

An inside look from one of 20 facilities that underwent initial government scrutiny

Mac McMillan, CISSM, has an insider's look at what it's like to undergo a HIPAA compliance audit.

One of the hospitals randomly selected by OCR for its initial audit phase consulted with McMillan to help with the audit process. The hospital underwent an audit by KPMG, LLP, the company that OCR hired to conduct the audits.

McMillan, CEO of CynergisTek in Austin, TX, shared what he learned during the February 15 webcast "2012 OCR Audits and Enforcement: A View From the Front Lines," which was sponsored by ZixCorp.

OCR selected the hospital as one of its initial 20 audits.

After it completes the pilot testing, OCR will evaluate the process, and KPMG audit teams will conduct up to 130 additional random audits of healthcare organizations before the end of 2012. Those audits are scheduled to begin in May.

The HITECH Act mandated the audits, which will measure healthcare organizations' compliance with the HIPAA Privacy and Security Rules, as well as breach notification rules.

Show and tell

So what was the hospital's biggest challenge during the audit?

Producing evidence it's actually in compliance with HIPAA, McMillan says.

The hospital needed to show that it had implemented the policies and procedures it had on paper and that staff members are in fact following them, he says.

> **"You don't *get* ready for audits, you *are* ready for audits."**
>
> *—Mac McMillan, CISSM*

"It's very clear from what occurred with our client that it is absolutely an evidence-based audit," McMillan says.

In other words, you not only need to have a policy and procedure, you must demonstrate that it has been enforced. KPMG's on-site visit has since ended, and the audit team was scheduled to complete a draft report detailing the findings of its investigation. The hospital had 10 days to respond, after which KPMG would write a final report to be submitted to OCR. McMillan says he expected the process to be completely finished sometime in March (after presstime).

Before the audit, the hospital knew it had some weaknesses with HIPAA compliance, he says. Many other organizations are in the same position.

"I think there will be a demonstrable amount of deficiencies identified at a good percentage of organizations selected for audit," McMillan says.

HCPro

IN THIS ISSUE

Prediction for what lies ahead

While OCR may use the results of the 20 initial audits to tweak the process, McMillan says he doesn't think the agency will radically alter how it conducts the audits.

"I'm sure there is a lot of learning in this first round of audits. There probably will be some change. How much? Who knows," he says. Each audit may be somewhat different in terms of auditors' focus depending on the specific organization. However, the overall picture won't change very much, he predicts.

"What will really be important are the conclusions that OCR and others draw from these audit results in the aggregate," McMillan says. "In other words, what will the overall impression be? Is HIPAA working? Has enforcement been effective?"

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 e-mail: *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.

Where the auditors focus

McMillan says privacy and security officers must be engaged in the following areas in order to be prepared for an audit:

- People
- Documentation
- Policies and processes

Be sure to provide staff with both routine and periodic reminders on privacy and security topics, he says. You can conduct mock audits and assessments to test their audit readiness.

Implement your policies and processes and review them regularly, he says. Practice what your policies state.

Ensure documentation is complete, accurate, and current, McMillan says. Be organized so you can retrieve documents in a timely manner when the auditors request them. Check all the dates on your forms. The forms in use by your staff must match your policies, he says. For instance, did you update a policy but never change a related form to reflect the update? You don't want to hand auditors a form that refers to an outdated version of a policy.

The auditors will ask you for a lot of information. Much of it you will need to produce before the auditors even arrive at your door (see p. 5 for a list of documents auditors may request). When you receive a letter notifying you that OCR has selected your organization for an audit, you will have only 10 business days from the date of the letter (not the date you receive it in the mail) to provide KPMG with all of the information it requests.

It's a tight time frame, McMillan says, and it is not likely auditors will grant extensions. Keep in mind the HIPAA Privacy and Security Rules have been in place for years. KPMG and OCR expect you to have the proper documentation in place, so you should be able to turn it over quickly, he says. Also, KPMG needs to complete numerous audits before December 31, so its auditors really need to stick to their timeline.

"They pretty much stayed within the playbook of their audit process," McMillan says.

If you haven't focused on HIPAA compliance, that is likely to show in your audit. "You don't *get* ready for audits, you *are* ready for audits," he says.

Typically, an audit team composed of three to five members will conduct an on-site visit that can last six to 10 business days. McMillan refrains from specifying how many auditors visited the hospital, but says it was not a full team. You can expect that different members of the audit team will look at different aspects of your HIPAA program simultaneously so they can cover more ground, he says.

Preparing for Privacy Rule compliance

First of all, you need to have performed a rigorous self-assessment. Do you have comprehensive policies in place? These need to address privacy rights, limits on uses and disclosures of PHI, and administrative requirements, McMillan says.

Do you have a comprehensive training program? Do staff members know how to handle patient privacy issues? Do you have documentation, such as a disclosure log, since the Privacy Rule requires covered entities (CE) to track disclosures of PHI? Have you addressed both administrative and physical safeguards so workforce members understand requirements such as the use of proper passwords and the proper disposal of PHI?

Be sure you have a business associate (BA) contract in place with each BA, McMillan says, noting that auditors focused on this. Have you done due diligence? Are your BA contracts compliant with both the Privacy and Security Rules? Are you exchanging PHI with your BAs?

You should also be sure you have minimum necessary policies for sharing PHI. Are they part of your third-party contracts?

Additionally, do you have specific policies governing PHI access by members of the clergy and law enforcement? For instance, what PHI should staff members provide to law enforcement?

Preparing for Security Rule compliance

McMillan says organizations should follow the PHI life cycle. Where is PHI created? How is it used and protected in your organization? Where is it maintained? Where is PHI transmitted? And finally, how is PHI destroyed?

Twelve quick tips for audit readiness

The chances may be slim, but if your organization gets randomly selected for one of OCR's HIPAA compliance audits, you should be prepared.

Mac McMillan, CISSM, CEO of CynergisTek in Austin, TX, and **Adam Greene, JD, MPH,** partner at Davis Wright & Tremaine, LLP, in Washington, DC, and a former regulator at OCR, each spoke during a February webcast, "2012 OCR Audits and Enforcement: A View From the Front Lines," sponsored by ZixCorp.

They offered the following tips:

- Ensure that upper management is aware of the audit and engaged in the process
- Orient key staff to the audit process and timeline
- Focus on the initial documentation task
- Perform triage; focus on your biggest compliance issues and easy fixes
- Consider refresher training for your organization's workforce
- Conduct walk-throughs and mock interviews for workforce members
- Prepare an orientation for the audit team
- Comply with minimum necessary and information technology access management requirements
- Organize an audit response team and collect feedback throughout the audit
- Prepare a response to the audit report with a focus on remediation of deficiencies noted by the audit team
- Engage audit and legal experts early in the process
- Remain flexible and positive

Does your risk analysis identify all areas of ePHI? Where is your high-risk PHI? This includes large repositories of PHI and sensitive PHI—with sensitivity being determined by the person or condition involved. For example, you want to ensure you protect the PHI of celebrity patients or those with HIV/AIDS.

Are your wireless networks secure? Is data in your organization encrypted? This includes e-mail, mobile devices, media, and other transmissions. If you don't use encryption, have you documented your organization's alternatives to encryption?

Are mobile devices secure? Do you maintain audit logs? How do you manage passwords? How do you handle access control? Is your workforce trained on security and is the training well documented? Do you impose sanctions where appropriate?

Be sure you have policies in place to address these requirements. Auditors may check the dates that you hired employees, when you trained them, and when you gave them access to your systems, says McMillan. Auditors also placed a lot of emphasis on contingency plans, McMillan notes.

Be sure you have such plans documented for all systems containing, processing, or transmitting PHI, he says. This includes backup plans, downtime procedures, emergency operations, and third-party service providers. Auditors looked closely at third-party providers, McMillan says. HIPAA requires that before CEs provide PHI to a third-party service provider, they have a BA contract requiring the third party to implement reasonable safeguards to protect the confidentiality and integrity of PHI. So be sure you have identified your BAs and have verified their security readiness, McMillan says. You should have documented evidence that you have requested your vendors' policies and procedures to ensure the protection of PHI, he adds.

Auditors also wanted to ensure the hospital had documented plans, procedures, and records concerning any incidents, McMillan says. Your documentation should include your incident response plans, breach notification procedures, records of any incidents, and the training and awareness of your workforce.

For records of breach incidents, auditors will want to see that there was a learning process, he says. What steps did you take to protect against future incidents?

Also look at how your organization deals with device and media reuse and destruction, McMillan advises. Are your processes documented and recorded? Do you verify that your processes were followed?

The bottom line is that you should ensure continuous monitoring of your HIPAA compliance. You want to be constantly paying attention to your policies and procedures. Be sure they are thorough and up to date. Equally important, be sure your staff is trained and is able to not only articulate your policy, but follow what it says, McMillan advises. ■

Timeline of a HIPAA compliance audit

If your organization is chosen for one of OCR's HIPAA compliance audits, here's the timeline the audit will follow, according to **Mac McMillan, CISSP,** CEO of CynergisTek in Austin, TX:

Day 1: Notification letter from OCR explaining that you have been selected and requesting documentation

Day 10: Letter due to KPMG auditors containing requested documentation (10 business days from the date of the notice)

Days 30–90: Start of the site visit (30–90 days from the initial notice)

Post-site visit:

- ➤ Additional analysis and questions
- ➤ Draft audit report issued by KPMG (20–30 days after end of site visit)
- ➤ Comments from organization on draft audit report due (10 business days from draft audit report)
- ➤ KPMG submits final audit report incorporating the site's comments to OCR (30 days after organization comments)
- ➤ Final disposition from OCR (time not specified)

Have these documents ready for a HIPAA compliance audit

As soon as healthcare organizations receive notice that OCR has selected them for a HIPAA compliance audit, the work begins.

The notification letter from OCR will also include a request for what's likely to be a lengthy list of the organization's documentation—all of it due within 10 business days from the date on the letter.

The documentation review—which the audit team will complete prior to the on-site visit—can include many documents, according to **Mac McMillan, CISSM,** CEO of CynergisTek in Austin, TX, whose company has been working with one of the hospitals that underwent an initial OCR audit.

Organizations should review the list at right and make sure they have these documents in case they are chosen to undergo an audit. McMillan says the documentation review can include the following types of documents:

- Demographic information
- Policies and procedures
- Information about key people in the organization
- Organizational chart
- Incident response plans
- Contingency plans
- System-generated information (e.g., log files)
- Technical controls information
- Physical safeguards
- Network diagrams
- Notice of privacy practices
- Privacy documentation
- Training documentation
- Complaint handling and sanction policies
- Mitigation practices
- Policies and procedures regarding uses and disclosures
- Breach notification policies and procedures

Stage 2 won't increase HIPAA requirements

Proposed EHR meaningful use requirements renew focus on security risk analysis

If your healthcare organization hasn't yet completed a security risk analysis, you just got another reason to conduct one.

Proposed Stage 2 meaningful use measures include a requirement to complete a security risk analysis with particular focus on encryption and protecting data at rest that is stored in your electronic health records (EHR).

Healthcare organizations working to implement EHR meaningful use requirements got a break in February when CMS announced a notice of proposed rulemaking (NPRM). The proposed rule, "Electronic Health Record Incentive Program—Stage 2," will give healthcare organizations an additional year to meet meaningful use Stage 2 requirements. You can read the 455-page NPRM, which CMS will publish in the *Federal Register,* at *www.ofr.gov/OFRUpload/OFRData/2012-04443_PI.pdf.*

In Stage 2, which CMS will implement in 2014 under the proposed rule, meaningful use includes new standards such as online access for patients to their health information and electronic health information exchange between healthcare providers.

Under the HITECH Act, eligible healthcare professionals, hospitals, and critical access hospitals can qualify for Medicare and Medicaid incentive payments when they adopt certified EHR technology and use it to demonstrate "meaningful use" of that technology by achieving the objectives set by CMS.

Focus on security

In order to have successful EHR technology, organizations must protect patients' PHI, CMS indicated in the proposed rule.

In Stage 2, CMS proposes organizations protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities. "Protecting electronic health information is essential to all other aspects of meaningful use," CMS said in the proposed rule. Unintended or unlawful disclosures of PHI could diminish consumer confidence in EHRs and electronic health information exchange, the agency said.

To meet that objective, organizations must conduct or review a security risk analysis in accordance with HIPAA requirements under 45 *Code of Federal Regulations (CFR)* 164.308(a)(1). They must address the encryption and security of data at rest requirements under 45 *CFR* 164.312 (a)(2)(iv) and 45 *CFR* 164.306(d)(3). Organizations must also implement security updates as necessary and correct identified security deficiencies as part of their risk management process.

The measure is the same as in Stage 1, except that it now specifically addresses the encryption and security of data stored in certified EHR technology—what is considered data at rest.

Effect of breaches

The Health IT Policy Committee, a federal advisory committee, recommended HHS specifically highlight the importance of organizations reviewing their encryption practices because of the large number of breaches reported to OCR involving lost or stolen devices, the NPRM said.

"Recent HHS analysis of reported breaches indicates that almost 40% of large breaches involve lost or stolen devices. Had these devices been encrypted, their data would have been secured," HHS stated in the proposed rule.

No new HIPAA requirements

Those wondering whether the meaningful use Stage 2 measures would increase HIPAA requirements for organizations moving toward adoption of EHRs got encouraging news, says **Frank Ruelas, MBA,** principal of HIPAA College, based in Casa Grande, AZ. "The NPRM clearly stated no."

While not changing the HIPAA requirements, HHS wants organizations to assess encryption as a means to secure ePHI and, if they determine it is not reasonable and appropriate, to adopt equivalent alternative measures.

CMS wants organizations to conduct a review for each EHR reporting period. To demonstrate meaningful use, the EHR reporting period for an eligible provider's first year is any continuous 90-day period within the calendar year. In subsequent years, the reporting period is the entire calendar year. Organizations must implement any security updates and correct any deficiencies that they identify in their risk management process.

Sharing data with patients

The proposed rule also includes requirements for sharing data with patients and information exchange among providers. HIPAA privacy and security officers should note a proposed objective for eligible providers to provide clinical summaries to patients within 24 hours for more than 50% of office visits, Ruelas says.

A relaxed time frame

In a move that will give healthcare organizations more time to prepare their systems for the transition to Stage 2 of meaningful use, the proposed rule gives providers an additional year to implement Stage 2 criteria.

CMS originally planned to require that any provider who first attested to Stage 1 criteria in 2011 would have to begin meeting Stage 2 criteria in 2013. Under the proposed rule, CMS delayed Stage 2 criteria for all providers until 2014. The agency said it made the change to allow the needed time for vendors to develop certified EHR technology that can meet the Stage 2 proposed requirements. ■

Case study

Newsletter keeps HIPAA front and center

How one organization reminds staff about compliance

How well you train your workforce members will determine whether you score points or encounter problems during a HIPAA compliance audit.

From all indications, training is going to be one area that KPMG auditors, acting on behalf of OCR, zero in on. (See p. 1 for an inside look at an audit.) As such, you should provide not only initial and annual training to all members of your workforce, but also periodic training to keep HIPAA top of mind.

Erika Walton, director of risk management at the Illinois Bone and Joint Institute, LLC (IBJI), does just that. Walton augments new employee and annual training with a HIPAA newsletter she sends out regularly.

IBJI is one of the largest orthopedic specialty groups in the country with many locations in the Chicago area. “We are a very large company with about 800 employees in more than 30 sites. There’s no way I can talk to everyone,” Walton says, referring to spreading the HIPAA message.

New employees undergo a three-hour training session, which includes about 45 minutes on HIPAA and IBJI’s requirements.

Existing employees also complete annual online training, which includes a quiz to demonstrate their knowledge of how to comply with HIPAA.

The challenge? Reminding workforce members about the need for compliance.

“The newsletter augments that so they don’t go a year without hearing about HIPAA,” Walton says.

One-page solution

Walton keeps HIPAA compliance on everyone’s mind with *HIPAA-Notics*, the one-page newsletter she sends out every two or three months.

“I put out the newsletter when I see an issue or a trend or I have someone calling with a question,” she says. “I don’t want to overdose them.”

The newsletter also doesn’t require staff members to take time away from the job for HIPAA training, Walton says. Like many other healthcare organizations, it can be very difficult for supervisors to release staff for training time, she says.

The newsletter keeps staff up to date on HIPAA news. For instance, in the November 2011 newsletter, Walton alerted staff that OCR audits would start this year. She provided a brief summary of what organizations can expect with the audits and what staff can do to achieve HIPAA compliance. “Follow correct procedures and use common sense whenever accessing, disclosing, handling, or managing PHI,” she advised.

She reminded staff members to conduct conversations involving PHI in private areas where they cannot be overheard and to use adequate precautions when faxing or transmitting PHI and ePHI.

In other newsletter issues, Walton has focused on protecting PHI with the use of electronic health records and double-checking that staff members are accessing the correct patient record.

She also keeps staff informed about HIPAA fines, such as the $1 million resolution settlement last year in which Massachusetts General Hospital in Boston agreed to pay HHS after an employee left patient records containing PHI on a subway train.

The message? HIPAA violations can cost lots of money, Walton says.

She also writes about security breaches and highlights what staff members should do if, for instance, a laptop computer is lost.

Short and easy to read

"The one-page length to me is key. If you give them too much to read, it gets buried. This takes all of two minutes to read," Walton says. This is particularly crucial when you have busy staff members. She keeps the message simple and straightforward.

Some reminders consist of one sentence:

- Protect ePHI by using only strong passwords
- Treat others' PHI as you want yours to be treated
- Do not refer to PHI on social networks

A quiz and prizes

In every issue of the newsletter, Walton also includes a short quiz. It usually deals with something that has happened in the organization or something she has read about.

She also likes to relate the quiz to a policy, form, or procedure. For instance, one month she asked staff members to identify the form in the medical record on which they need to document if they have faxed PHI to an incorrect number.

It's a great way to involve staff members. Walton urges people to e-mail her their answers. Unless the question is particularly difficult, she usually gets 20–25 responses within an hour.

"I respond back to everyone that plays," she says. If they've answered incorrectly, she gives them the right answer and urges them to try again.

She often offers a prize for the first five staff members who answer correctly. Winners get $5 gift cards or some other small prize. She also publishes the names of the winners in the next issue of the newsletter.

"I'm pretty proud of it," Walton says about the newsletter. "Even if I get 10 people thinking about it, and those 10 talk to another 10 people, they are raising awareness about HIPAA." ■

HIPAA Q&A

Encryption levels, disclosures to BA, employee sanctions

by Chris Apgar, CISSP

Q Please explain in an understandable way for nontechnical individuals what level of encryption is needed for e-mail to be considered secure as defined in the interim final breach notification rule.

A All ePHI, including e-mail, is considered secure if it is secured at a level consistent with the National Institute of Standards and Technology (NIST). Most NIST documents are not easily decipherable to nontechnical individuals. There are several different standards that can be used to encrypt data transmitted via e-mail. One common approved standard is called the Advanced Encryption Standard (AES). A second, usually used for website encryption and webmail encryption, is Secure Socket Layers (SSL). If you are encrypting your e-mail using AES or SSL, or another NIST approved standard, that's a good place to start.

The next step is to determine how strong the mathematical algorithm used to protect, or "scramble," your data is. If the algorithm is less than 128-bit, it is not secure. The larger the number of bits, the stronger the algorithm. A number of vendors and healthcare entities are moving to 256-bit encryption. This exceeds the NIST standard but is worth considering because it better protects any PHI you are transmitting over the Internet.

The specific NIST standards that address PHI transmitted via e-mail are NIST 800-52, NIST 800-57, and Federal Information Processing Standards 140-2.

For more information, OCR has published guidance in an FAQ that may be helpful regarding what is considered "secure" electronic PHI when transmitted over the Internet or in an e-mail *(http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2006.html)*.

Q A nurse in a skilled nursing facility asked if she could post a paper form called "Turn and Position Sheet" on the wall in the residents' rooms so employees can document each time they turn and position the resident. It would indicate to a visitor or other non-nursing facility staff that the resident suffers from pressure sores. Is this a violation of HIPAA and would it be considered a breach of PHI?

Q It could represent an inappropriate disclosure of PHI given the care setting. Covered entities cannot eliminate incidental disclosure but are required to limit it as much as feasible. On the other hand, if the paper form is posted where it is not easily viewable to anyone but the workforce member, and if the heading on the form was "TP" or another code understandable to workforce members only, it would strictly limit the possibility of incidental disclosure of patient information and would likely not be considered an inappropriate release of PHI.

Q During a recent webinar, a presenter indicated disclosure of PHI to business associates needed to be included in the disclosure accounting log. Aren't disclosures of PHI to business associates considered disclosure for healthcare operations purposes?

A The disclosure of PHI to a business associate does not need to be included in the disclosure accounting log as long as the disclosure is related to treatment, payment, and healthcare operations. Disclosures of PHI to a business associate are not necessarily classified as disclosures only for healthcare operations. As an example, if a health plan discloses PHI to a third-party administrator, the disclosure would likely be for payment purposes. A valid business associate contract or other written arrangement (government entities) needs to be executed before any PHI is disclosed to the business associate, though.

Q A covered entity is required to impose sanctions against workforce members who violate the covered entity's privacy and security policies and procedures. Can the covered entity include PHI as part of the disciplinary process without the authorization of the patient? The disciplinary process is conducted by an arbitrator.

A No, a covered entity cannot disclose patient information to the workforce member or the arbitrator. The patient information must be de-identified. The sanctions process should focus on the actions that led to a violation of the covered entity's policies and procedures. This does not require inclusion of patients' PHI. ■

Editor's note: Apgar is president of Apgar & Associates, LLC, in Portland, OR. He has more than 17 years of experience in information technology and specializes in security compliance, assessments, training, and strategic planning. Apgar is a board member of the Workgroup for Electronic Data Interchange and chair of the Oregon and Southwest Washington Healthcare, Privacy and Security Forum.

Product watch

Data availability with some caveats

by Chris Apgar, CISSP

All covered entities (CE) face the question, "Will the data be there when I need it?"

Dell, Inc., now offers cloud services support that can either replace your existing servers or augment them. The failure of mission-critical applications such as an electronic health record can have catastrophic consequences for patient care if the patient information, and oftentimes the application, cannot be recovered quickly.

If a piece of hardware fails and no backup hardware exists, it will likely be days before you can repair the workstation or replace the server. But for CEs, it may not be sufficient to back up PHI and store it securely off-site.

Dell produces "mission critical" four-hour support, meaning it will produce a new server or repair the failed server within that four-hour window.

To take advantage of cloud-based services, make sure backup tapes are readily available along with the hardware, or configure what is called a RAID array (redundant array of independent disks) that allows redundant PHI storage across several physical drives or disks.

Dell has made previous claims regarding the level of support it is able to provide for servers and workstations. Too often, it can't support those claims. One of the keys to surviving hardware failure is not to rely on promises from hardware vendors such as Dell.

That said, Dell's cloud services are secure and offer redundancy if hardware fails. Data is stored remotely and can generally be instantly accessed; this limits potential harm to patients when healthcare professionals can't access PHI needed for patient care.

You can establish a virtual environment where you only need to rely on a laptop, tablet, or other hardware device (versus the server that's storing all of your patient information) to access data that's stored in the cloud.

Cloud storage really boils down to this: You are sharing someone else's server with other healthcare organizations and businesses rather than using your own. The cost is also reasonable and based on a per-user figure.

Despite cloud storage's convenience, it has raised a number of security questions. Cloud security is generally based on what you require. Your patient data can be very secure as long as you implement appropriate security safeguards. Often you will need to work with your cloud services vendor—in this case, Dell—to reasonably ensure your data is both secure and can be accessed in the event of a disaster.

Even if you're using cloud services, make sure you have at the very least a backup computer in the event your computer or server fails. You still need hardware to access the cloud. If you are running a small practice with only one computer and that computer fails, you won't have access to your data no matter where it's stored.

Dell has made a number of claims relating to service such as "next business day" support, "mission critical" four-hour support, and so forth. Again, don't rely on such support claims. You need to make sure you can access your patient information when it is needed and not wait for a technician or a replacement part to show up, which could take several days.

Dell's cloud services are an inexpensive solution, and they can get you away from total reliance on your vendor's hardware and "hands-on" support. Remember, though, if it's in the cloud, you still need a computer to access it. ■

Editor's note: Apgar is president of Apgar & Associates, LLC, in Portland, OR. He has more than 17 years of experience in information technology and specializes in security compliance, assessments, training, and strategic planning. Apgar is a board member of the Workgroup for Electronic Data Interchange and chair of the Oregon and Southwest Washington Healthcare, Privacy and Security Forum.

Teach your physicians, staff proper social media protocol

Navigating the new world of social media is challenging for many professions, but perhaps none more so than the medical profession, where physicians and other healthcare professionals must balance a tell-all online culture with the HIPAA Privacy Rule's mandate to protect patient privacy.

With their ever-increasing popularity, social media sites such as Facebook and Twitter™ blur the lines between private and professional identities. Physicians must carefully consider their online lives and recognize that they're navigating a public space that can get them into trouble, say two Boston physicians.

Arash Mostaghimi, MD, MPA, and **Bradley H. Crotty, MD,** physicians at Beth Israel Deaconess Medical Center, offered some recommendations in their "ideas and opinions" piece published April 19, 2011, in the *Annals of Internal Medicine.*

"Unlike previous advances in communication, such as the telephone and e-mail, the inherent openness of social media and self-publication, combined with improved online searching capabilities, can complicate the separation of professional and private digital personae," they wrote.

Hospital elevators and social media

The physicians likened social media to hospital elevators, where most organizations now post signs to remind staff not to discuss patients in public settings where conversations can be easily overheard. Details can facilitate identification even when a patient's name is not mentioned.

"Social networks may be considered the new millennium's elevator: a public forum where you have little to no control over who hears what you say, even if the material is not intended for the public," Mostaghimi and Crotty wrote in the article.

Even if a physician has no intention of doing anything wrong, social media can get doctors into trouble with violations of patient privacy, says Crotty.

A case in point

The Rhode Island Board of Medical Licensure and Discipline found a Westerly Hospital physician guilty of unprofessional conduct after she posted information on Facebook that allowed identification of a patient.

The board disciplined the physician, who had recounted some of her emergency department experiences on Facebook, *The Providence Journal* reported April 18. Noting that the physician did not include patient names and did not intend to disclose confidential information, the board nonetheless said the nature of one patient's injuries allowed an unauthorized individual to ascertain the patient's identity.

The physician deleted her account when she learned what had occurred. The board reprimanded her and fined her a $500 administrative fee.

The hospital terminated the physician in 2011, revoking her emergency department privileges for posting information about the trauma patient online, *The Boston Globe* reported April 20.

Physicians should assume that all posted materials are public and therefore exercise care to protect themselves and patient privacy, Crotty and Mostaghimi warned in their article.

Educating physicians—and everyone else

In addition to cautioning physicians about maintaining separate personal and professional identities online, hospitals have a role in educating physicians and other staff, says Crotty. He and his colleague urge hospitals and healthcare organizations to develop standards and educational materials to guide physicians.

"We're not suggesting that physicians should be prohibited from using social media sites," Mostaghimi said in a Beth Israel press release. "Doctors just need to be savvy regarding the content and tone of what they post online. People share information openly using social media, but posts intended for one audience may be embarrassing or inappropriate if seen by another." ■

How hospitals can help physicians meet social media challenges

Hospitals should develop standards and create educational materials to guide physicians in their use of social media, say two Boston physicians.

Arash Mostaghimi, MD, MPA, and **Bradley H. Crotty, MD**, physicians at Beth Israel Deaconess Medical Center, offer recommendations to help physicians meet the challenges they face when using social media. Their recommendations first appeared in an April 19, 2011, opinion piece in the *Annals of Internal Medicine*.

Hospitals can share these recommendations with their physicians, says Crotty. "It's a starting point. We intended this as a frame of reference," he says.

Physicians can take the following steps to meet these challenges:

➤ Manage your professional identity and image. Encourage physicians and all staff members to employ these strategies to protect their professional online identities.

➤ Monitor your online presence with electronic self-audits. Google yourself or use other search engines to conduct regular audits to learn what information others can see. What personal information do you share online? Do your political affiliations or personal photos appear? Do physician rating sites provide your correct name and office address? Who shares your name, and how can that affect how others might mistakenly view you?

➤ Maximize online privacy settings for personal profiles and social networking sites. Separate your personal and professional lives online. Maximize the privacy settings on your personal Facebook page to control access. Carefully consider what information you post. Don't post information that you might later regret. Remember that the Internet is archived. Once something is posted, "it's almost impossible to take back," says Crotty.

➤ Establish online "dual citizenship" with separate professional/public and personal/private networking profiles. Physicians can maintain a professional identity online and a private identity among friends and family by establishing online dual citizenship. Do this by maintaining a separate online profile intended to appear among the top results when someone searches online for a specific physician. Create a professional home page, post an online curriculum vitae, or use services such as Google Profiles™ *(www.google.com/profiles)*. This is particularly advantageous for those entering the medical field because new profiles can redirect traffic from other Internet content that may no longer be under their direct control. Create a professional website, a public Facebook page, or a Twitter™ account specifically for work purposes.

➤ Create a professional biography for patients and others who find you via an online preferential search. Physicians who desire an outward, professional presence on social networking sites, such as Facebook, can create a public persona to better control information. This method also obviates the need to accept or deny friend requests from patients or others. Alternatively, physicians can use professional social networking sites, such as LinkedIn and Sermo. Hospitals can create physician profiles on their websites. Physician profiles can include office hours, contact information, education, and professional experience.

Use social media in a professional manner

Employ these strategies to encourage physicians and all staff members to conduct themselves in a professional manner online:

➤ Ensure staff members understand that all posted content must be considered public and permanent. Information on the Internet is archived and often transmitted from one individual to another. This makes it difficult, if not impossible, to remove information.

➤ Encourage physicians, nurses, physician extenders, and office staff to exhibit online behavior that mirrors office behavior standards.

➤ Educate staff with respect to HIPAA privacy requirements. They must understand that patient privacy extends to the Internet.

Remember that all patients may not have access to electronic resources. Not everyone is using social media to communicate. Your facility must reach those patients through different media.

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

April 2012

Tips from this month's issue

OCR audit readiness (p. 1)

1. Answer these questions to help you prepare for an OCR audit:
- Where is PHI created? How is it used and protected in your organization? Where is it maintained? Where is PHI transmitted? How is PHI destroyed?
- Does your risk analysis identify all areas of ePHI? Where is your high-risk PHI?
- Are your wireless networks secure? Is data in your organization encrypted? This includes e-mail, mobile devices, media, and other transmissions. If you don't use encryption, have you documented the alternatives to encryption you have in place?
- Are mobile devices secure? Do you maintain audit logs? How do you manage passwords? How do you manage access control? Is your workforce trained on security and is the training well documented? Do you impose sanctions where appropriate?

2. Be sure you have policies in place to address these requirements.

3. Be sure you have identified your business associates and have verified their security readiness.

4. Have documented evidence that you have requested your vendors' policies and procedures to ensure the protection of PHI.

5. Ensure your documentation includes your incident response plans, breach notification procedures, records of any incidents, and the training and awareness of your workforce members.

6. Ensure that upper management is aware of the audit and engaged in the process.

7. Orient key staff with regard to the audit process and timeline.

8. Focus on the initial documentation task.

9. Perform triage; focus on your biggest compliance issues and easy fixes.

10. Consider refresher training for your organization's workforce.

11. Conduct walk-throughs and mock interviews for workforce members.

12. Prepare an orientation for the audit team.

13. Comply with minimum necessary and information technology access management requirements.

14. Organize an audit response team and collect feedback throughout the audit.

15. Prepare a response to the audit report with a focus on remediation of deficiencies noted by the audit team.

16. Engage audit and legal experts early on in the process.

17. Remain flexible and positive.

Physicians and social media (p. 11)

18. Manage your professional identity and image. Encourage physicians and all staff members to employ these strategies to protect their professional identities.

19. Monitor your online presence with electronic self-audits. Google yourself or use other search engines to conduct regular audits to learn what information others can see.

20. Maximize online privacy settings for personal profiles and social networking sites.

21. Separate your personal and professional lives online.

22. Maximize the privacy settings on your personal Facebook page to control access.

23. Carefully consider what information you post. Don't post information that you might later regret.

24. Establish online "dual citizenship" with separate professional/public and personal/private networking profiles.

25. Create a professional biography for patients and others who find you via an online preferential search.

26. Employ the following strategies to encourage physicians and staff members to conduct themselves in a professional manner online:

- Ensure they understand that all posted content must be considered public and permanent
- Encourage physicians, nurses, physician extenders, and office staff to exhibit online behavior that mirrors office behavior standards
- Educate staff with respect to HIPAA privacy requirements

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. *April 2012.*