March 2012 Vol. 12, No. 3

BRIEFINGS ON HIPAA

• Privacy • Security • Transactions • Training

Mobile devices another PHI challenge

'An Apple a day' takes on new meaning in healthcare

They are becoming as common in healthcare as a stethoscope draped around a physician's neck. Check the pocket of a doctor's white coat, and you're likely to find a mobile device, whether it be a tablet computer or a smartphone.

The use of these devices is exploding in healthcare, says **Christina Thielst,** a health administration consultant and blogger from Santa Barbara, CA. (See p. 10 for more on trends to watch in 2012.)

It's a phenomenon that hasn't escaped the notice of HHS. The federal agency is concerned about the expansion of mobile health technologies, which it says have changed the way providers are delivering healthcare in the United States and throughout the world.

HCPro

IN THIS ISSUE

In January, an HHS task force recommended the agency establish guidelines for managing privacy and security concerns if the government encourages and helps develop health text messaging and mobile health programs.

'Can't do without it'

Privacy and security officers should look for one particular trend: the growing number of hospital residency programs that are now equipping their physicians with mobile devices.

> **"I hope that other CIOs realize that mobile devices are here to stay, improve productivity, but must be managed wisely."**
>
> *—John Halamka, MD*

For example, in July 2011, the anesthesiology residency program at Mount Sinai School of Medicine in New York City decided to purchase an Apple iPad® for each of its 100 residents and fellows.

Adam I. Levine, MD, program director, got the idea to purchase tablet computers after some of the residents began using their own personal tablets on the job. After discussions about their use of mobile devices, he decided all of the residents and fellows could benefit from having an iPad.

"Residents were reporting that the iPad was becoming more useful to them the longer they used it. They told me it was almost to the point where they felt, 'I can't do without it,' " he says.

After Levine sought administration approval for the purchase, department leaders consulted with the hospital's legal department to address concerns about HIPAA and protecting patient data. They also worked with the IT department.

The hospital reallocated the textbook allowance given to the residents and fellows—instead of buying

books, it purchased the iPad packages, which cost $700 each. The program has also freed up the faculty book fund so its teaching physicians can purchase devices of their own.

The 'firestorm' is here

Mount Sinai's anesthesia department is the first that Levine knows of to use tablet technology on this scale, but he is sure it will not be the last. He's already fielded calls from colleagues and other program directors who have heard about the iPad program. And other residency programs at Mount Sinai are now taking the iPad plunge and buying devices for their residents, Levine says.

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.

"The firestorm is upon us," he says.

Residency programs outside Mount Sinai are purchasing tablet computers for their residents as well. The University of Chicago Medical Center was one of the country's first programs to purchase tablet computers for all of its internal medicine residents. The Stanford University School of Medicine recently announced a pilot program to provide an iPad for each first-year medical student. Columbia University Medical Center has also been introducing devices for use by its house staff.

A growing trend

These programs may be on the leading edge of a significant shift in the way physicians practice medicine. Regardless of whether programs are buying the devices, more physicians are using tablet computers and smartphones.

At Beth Israel Deaconess Medical Center in Boston, clinicians started making iPad purchases themselves, a trend that has only accelerated. About 1,000 of the devices are now in use, says **John Halamka, MD,** an emergency physician and Beth Israel's chief information officer (CIO). More than 1,600 smartphones are also connected to Beth Israel's network.

"I hope that other CIOs realize that mobile devices are here to stay, improve productivity, but must be managed wisely," Halamka says.

In Massachusetts, every CIO is aware of the benefits and risks of mobile devices because there has been a statewide forum on the topic, he notes.

And the benefits are substantial. At Mount Sinai, for instance, an iPad allows residents to access electronic medical records, the Internet, and an entire library of electronic textbooks, medical journals, and guidelines—all at the point of care. Residents have instant access to this information whether they're at a patient's bedside or inside the operating room. There are 16 e-books for anesthesia alone, says Levine.

However, chief among the concerns about use of the tablets is the need to protect patient privacy under

HIPAA. The theft or loss of mobile devices is now a major cause of breaches of PHI.

"HIPAA is a huge concern," Levine acknowledges.

A risk you need to manage

As their use spreads in the workforce, mobile devices pose a risk healthcare organizations need to address. Studies show more physicians and clinicians than ever were using mobile devices in 2011, yet unsecured devices are the cause of many data breaches.

A December 2011 benchmark study by the Ponemon Institute, which conducts independent research on privacy, data protection, and information security policy, showed 81% of healthcare organizations use mobile devices to collect, store, or transmit some form of PHI.

But 49% admit their organizations do nothing to protect these devices (see chart on p. 4). Only 23% use encryption to safeguard patient data. As a result, only 15% are very confident and 23% somewhat confident that patient data is protected from being accessed via mobile devices, the study showed.

Orrin I. Franko, MD, a resident at the University of California's orthopedic residency program in San Diego, has conducted research on the use of mobile devices. "The prevalence is increasing in the use of smartphones and tablets," he says.

Franko published a new study in the November 4, 2011, *Journal of Medical Systems* where he reported a growing demand for more mobile applications as smartphone use becomes more prevalent among healthcare providers.

It's been a rapid evolution. "Even four years ago, the iPhone® wasn't even on the market," Franko says.

A 2011 study by the Computing Technology Industry Association (CompTIA), a nonprofit association for the IT industry, found mobile health is becoming more of a reality as medical practices increasingly embrace mobile technologies. While laptop and notebook computers are commonplace in the medical community, the next wave of mobile adoption is well under way; providers are turning to tablets, smartphones, and applications to increase productivity and improve patient care, according to CompTIA's study, "Third Annual Healthcare IT Insights and Opportunities."

One-quarter of healthcare providers surveyed for the study currently use tablets in their practice, and another 21% expect to do so within 12 months. More than half currently use a smartphone for work purposes.

Keeping PHI safe

The growth in mobile devices has many healthcare organizations working to ensure the protection of PHI.

Providers will need to balance use and security of the devices, as well as adopt written terms of use for employees and contractors using them in the workplace, Thielst says.

The residents and fellows must sign an agreement governing their use of the iPad®, including provisions to not store PHI on the tablet and to keep it password protected.

Mount Sinai's anesthesiology department has addressed the concern about protecting PHI by prohibiting the residents or fellows to store any PHI on their iPad, Levine says. This way, if a device is lost or stolen, there is no risk of a data breach.

The residents and fellows must sign an agreement governing their use of the iPad, including provisions to not store PHI on the tablet and to keep it password protected. (See p. 5 for a copy of the agreement.)

Beth Israel's security policy requires all devices to be password protected and encrypted, says Halamka. All of the facility's applications are Web-based, so no data is stored on the devices, he says.

However, hospitals should protect their network from any malware or viruses that might spread from a clinician's personal mobile device, he says. To that end, Beth Israel is looking at multiple mobile device security products. Halamka authors the blog "Life as a Healthcare

CIO," and many of its recent posts discuss the challenge of security and device management. Visit *http://geekdoctor.blogspot.com/2011/12/cool-technology-of-week_16.html* for an example.

The University of Chicago's internal medicine residency program has created an iPad manual for its residents that outlines how the tablets should be used.

"With great power comes great responsibility," the manual advises the residents.

The manual urges residents to take care of their iPad and keep it secure. It also cautions them to be diligent about securing PHI and reminds residents that the device is for business purposes, and that downloads and applications are monitored periodically.

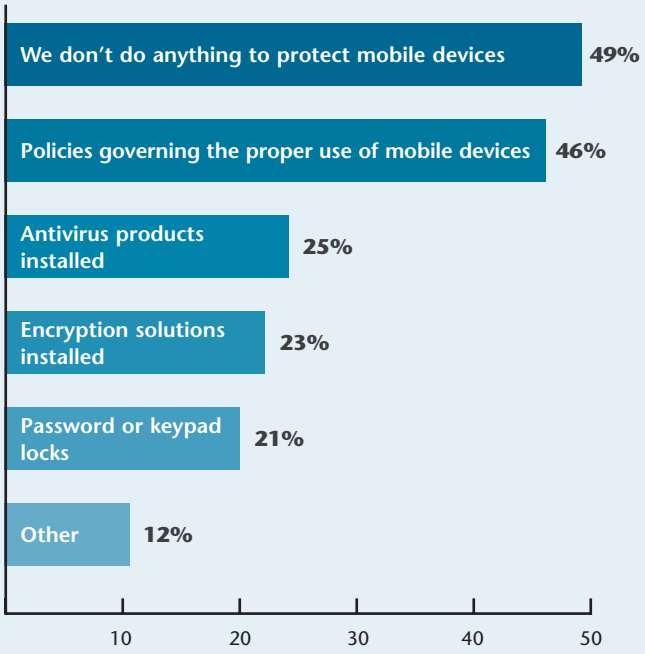
Residents are also made aware of the need for physical security. They are advised that to avoid losing their iPad, they should keep it with them at all times. They are told to avoid letting other people borrow their tablet and to be aware of their surroundings when using it. "Never leave your iPad unattended on the wards, workrooms, conference rooms, etc.," the manual advises.

Residents are advised to report the loss of their iPad immediately and to file a police report if it is stolen. They are also required to keep the security feature "Mobile Me-Find My iPad" turned on, which allows the device to be remotely located, wiped clean, and locked if it is lost or stolen.

When it comes to PHI security, residents are advised that they must not "jailbreak" their iPad or make any attempt to gain elevated privileges. Additionally, their iPad will be wiped clean of all content after five incorrect password attempts.

How organizations protect mobile devices

Does your organization use any of the following security solutions or procedures to safeguard patient data contained on mobile devices?



Source: Ponemon Institute's 2011 Benchmark Study on Patient Privacy and Data Security, *December 2011.*

Residents are not allowed to store any PHI locally on the iPad. They are advised to log out of their account when finished using the device and not to share the device or their passwords with others. They are also asked to update the iPad when any new security measures become available.

Levine says the iPad program at Mount Sinai helps residents with both their education and patient care. The hospital has adapted its electronic medical record system so physicians can access it via an iPad, Levine says. Currently the application is read-only, but it gives residents all of the patient information they need. A trial is under way and physicians will soon be able to write orders from their iPad as well, he says.

"It's really a win, win, win, win," says Levine about the use of the tablets. "I have yet to see a disadvantage. I bet this is going to be the wave of things to come." ■

Sample policy

MOUNT SINAI SCHOOL OF MEDICINE

July 1, 2011

Department of Anesthesiology
Apple® iPad® Initiative and House Staff Usage Agreement

We are pleased to announce that the department will be starting an Apple iPad initiative. Instead of book allowances, every CA 1–3 resident and fellow will receive a 3G-capable Apple iPad equipped with a protective case and a one-year AppleCare package. Trainees may use the iPad to access the Internet, electronic books, journals, and professional e-mail accounts, and eventually write orders into EPIC. In addition, CA 2–3 residents and fellows may use funds that will be set aside annually to purchase books and iPad applications that are relevant for academic or clinical purposes. The Mount Sinai WiFi will allow access to the Internet while on the medical center campus, and the iPad will be equipped with 3G capability. It will be the individual's responsibility to arrange and pay for that service, if desired. Purchased iPad devices are configured for either AT&T or Verizon service and individuals may choose according to their preference, subject to availability.

In order to ensure that the equipment is used correctly and to ensure everyone understands their responsibility for maintaining and protecting the iPad, each trainee must read and sign the following list of requirements prior to receiving an iPad:

1. Responsibilities:
   a. House staff will be given ONE (1) iPad during the duration of training without exception.
   b. House staff must safeguard against theft or damage.
   c. The department will neither provide nor reimburse for a replacement iPad.
   d. In the event of iPad failure, the house staff will be responsible for arranging service through Apple using the AppleCare warranty provided by the department, so long as that warranty is in effect. Repairs following expiration of the warranty are the responsibility of the individual.
   e. House staff are responsible for iPad maintenance, where applicable.
   f. House staff are responsible for arranging and paying for 3G service, if desired.
2. House staff must ensure that no PHI is stored on the iPad and that the iPad is password protected.
3. It is only permissible to use the iPad for recreational purposes in non-patient-care locations in the medical center (e.g., lounges or call rooms). Public areas require consideration.
4. House staff must abide by all institutional and departmental policies regarding the use of electronic devices and access to the Internet while in the hospital, operating rooms, or other patient care areas. While in patient care areas, iPad devices MUST NEVER be used to access the following types of materials:
   a. Music
   b. Lay press
   c. Lewd materials
   d. Video entertainment
   e. Twitter, Facebook, or other social media
   f. Personal e-mail accounts
5. Failure to comply with these responsibilities will result in confiscation of the iPad and may result in the loss of clinical credit, suspension, and possible termination.

I have read and agree to comply with the **Apple iPad Initiative and House Staff Usage Agreement.**

_____
Signature

_____
Print name

_____
Date

_____
Apple iPad serial number

Source: Adam I. Levine, MD, program director, residency training program, Department of Anesthesiology, Mount Sinai School of Medicine. Reprinted with permission.

Steps to help your organization respond to a breach

Breaches happen. How your organization responds when they happen can make all the difference.

Rebecca C. Fayed, Esq., associate general counsel and privacy officer at The Advisory Board Company in Washington, DC, recommends taking the following steps in response to a breach:

➤ **Prepare for the possibility of a breach.** You want to develop an incident response plan and establish an incident response team.

➤ **Investigate the incident.** If an incident occurs that you think may be a breach, you need to conduct a thorough investigation. When clients call and have had an incident, they are usually panicking, Fayed says. "I do say, take a breath," she advises. "How you respond effectively and efficiently is going to make or break you."

If a breach occurred, you can't undo it, she says, but you can control how you move forward and prevent future occurrences. Do you have a breach notification procedure and incident response team in place? If so, follow the procedure and initiate actions of your team. If not, you need to identify individuals in the best positions to help investigate and respond to the incident. You want to pull together the right group of people who can make decisions and keep your investigation moving, Fayed says.

You need to collect as many facts as possible about what happened, she says. Identify the following:

- The facts surrounding the incident. For instance, did it involve a stolen or lost laptop computer, a backup tape, or a portable storage device? Was an e-mail or fax sent to a wrong recipient? Were paper records thrown in the trash?
- Data elements. Did the incident involve names, addresses, phone numbers, PHI, Social Security numbers, or credit card numbers?
- Number of people affected.
- States in which affected people live and total affected people in each state.
- Whether the information was encrypted.

➤ **Mitigate the harm and take corrective action.** Ultimately, you want to be able to defend your organization's actions.

"You want to be able to say, 'I responded immediately. I did things to make sure the level of harm was reduced,' " Fayed says.

HIPAA requires that a covered entity (CE) must mitigate, to the extent practicable, any harmful effect that is known to the CE of a use or disclosure of PHI in violation of its policies and procedures or the Privacy Rule by the CE or its business associate (BA), per 45 *CFR* 164.530(f).

You want to be able to show OCR or the affected individuals that you took appropriate steps, such as filing a police report about a stolen laptop computer or contacting the recipient of wrongly sent PHI and asking for the information to be returned or destroyed.

When it comes to corrective action, you may need to terminate an agreement with a BA, revise your procedures, or sanction employees.

If your organization determines that a breach occurred, you will also need to determine whether you will offer credit monitoring services to those affected, Fayed says.

➤ **Assess and document whether the incident is a "breach" under the HITECH Act or the HHS breach notification rule.** "This is the biggie," Fayed says. You must determine whether a breach actually occurred as defined by the regulations "Breach Notification for Unsecured Protected Health Information: Interim Final Rule" (45 *CFR* Parts 160 and 164). You can access the regulations at *http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.*

The breach notification interim final rule, issued in August 2009, defines a breach as the unauthorized acquisition, access, use, or disclosure of PHI (either electronic or hard copy) that is not permitted by the Privacy Rule and compromises the security or privacy of PHI—that is, it poses a significant risk of financial, reputational, or other harm to the individual.

To determine whether an incident is a breach, ask these three questions:

- Did the incident involve the impermissible use or disclosure of PHI under the Privacy Rule?
- Did the incident compromise the privacy or security of PHI by creating significant risk of harm?
- Is the incident excluded from the definition of a breach?

Exclusions where notification of a breach is not required include the following:

- An unintentional use of PHI by a workforce member acting in good faith and within the scope of his or her authority, without further improper use or disclosure of that PHI
- An inadvertent disclosure of PHI by an authorized person to another authorized person, without further improper use or disclosure of that PHI
- A disclosure of PHI to an unauthorized person for which there is a good-faith belief that the unauthorized person would not reasonably have been able to retain the PHI

Then there is the question of whether you need to report the breach to affected individuals. Can you make a case that the breach did not cause significant harm?

"If it's a close call, I wouldn't play cute here. I wouldn't make a cute argument for why there was no harm. I tend to err on the side of notifying—be transparent," Fayed says.

The breach notification rule includes some examples of instances where an incident is not a breach.

The HITECH Act breach notification requirement applies only to the breach of unsecured PHI. The breach of secure PHI is not subject to the notification requirement.

If PHI is rendered "unusable, unreadable, or indecipherable" to unauthorized individuals, it is secure. Technologies and methodologies that render PHI secure include encryption and destruction.

➤ **Analyze whether the incident is a breach under applicable state law.** The vast majority of states have data breach notification laws, Fayed says. Many of them focus on protection of financial information.

You need to analyze the state law's definition of "personal information." A small number of states include health or medical information within their definition, she says.

You will also need to analyze any exceptions to breach notification obligations, such as encryption or harm-based standards.

If your state breach notification law is triggered, be aware that your state may have notification obligations in addition to those required by the HITECH Act.

➤ **Notify individuals (or the CE).** The HITECH Act and the breach notification interim final rule require that you provide notice to an affected individual "without unreasonable delay" and no later than 60 days after a breach is discovered.

"You should not use the 60 days. You want to move swiftly and quickly," Fayed says. If possible, make that notification sooner than the 60th day. Many state laws also require sooner notification, so be aware of what your state requirement mandates.

Provide notification via first-class mail unless the individual has specified a preference for e-mail. The notice must include the following:

- Description of facts about the breach
- Type of PHI involved
- Steps individuals should take to protect themselves
- What the CE is doing to investigate the situation and prevent future breaches
- Contact information to allow individuals to ask questions

A substitute notice may be required if you are not able to contact people.

BAs must notify the CE of a breach. Your contract with the BA may specify who will notify the individuals affected and who will pay for that notification.

➤ **Notify the media.** If you have breached the PHI of 500 or more individuals, you must notify prominent media outlets in the state.

➤ **Notify HHS and, if applicable, state agencies.** CEs must notify HHS of the breach if 500 or more individuals are affected. You must notify HHS contemporaneously with notification to the individual via an online notification.

If the breach involved fewer than 500 affected individuals, a CE must notify HHS via an annual log of events no later than 60 calendar days after the end of the calendar year.

Check your state laws to determine whether you need to notify any state agencies of a breach, such as the police department, consumer protection agencies, or the attorney general's (AG) office.

➤ **Reassess your privacy and security compliance policies and procedures.** Evaluate and revise your policies and procedures if they do not work for your organization or do not prevent privacy and security violations.

"Anything and everything that could be considered the cause of the breach should be addressed," Fayed says.

For example, if an incident involved a lost or stolen backup data tape, consider changing your procedure for transporting or storing these tapes. If an incident involved faxing information to a wrong number, consider changing your procedure to require contacting the intended recipient before the fax is sent (to confirm the number) and after the fax is sent (to confirm receipt). If an incident was the result of employee error, consider retraining employees. If an incident was the result of a BA's error, you might want to consider terminating the agreement or imposing more stringent safeguards under the agreement.

➤ **Prepare for the possibility of an HHS/OCR or state AG investigation.** HHS/OCR recently stated that the agency has initiated an investigation into every breach involving more than 500 individuals and reported to its office via the online notification system, notes Fayed.

OCR also trained state AGs on HIPAA enforcement during four sessions held in 2011. The purpose of the training was to help state AGs in investigating and seeking damages for HIPAA violations that affect residents in their states.

The OCR investigations Fayed is familiar with were initiated via telephone. Respond as soon as you get that call, she says. As evidenced by recent actions, OCR expects cooperation from organizations, Fayed notes. Anyone doubting the consequences of not cooperating need only look to the landmark HIPAA civil monetary penalty imposed on Cignet Health of Prince George's County, MD. In February 2011, Cignet was ordered to pay $4.3 million—a $1.3 million fine for violating 41 patients' rights by denying them access to their medical records and another $3 million for failure to cooperate with OCR's investigations and produce the records.

You should be prepared to provide any pieces of information investigators request. They will also be looking to see what you did to fix any problems.

Generally, OCR has asked organizations to provide:

- The facts surrounding the breach
- Copies of notification letters, media notices, and BA agreements
- Actions taken to locate missing data, prevent further loss of data, and protect affected individuals (e.g., credit monitoring services)
- HIPAA Security Rule risk assessments
- Description of safeguards in place to protect the information (specifically, information related to whether data was encrypted)
- Compliance efforts related to policy and procedure revisions, training, and imposed sanctions

Your best plan is to have a complete compliance program in place. "Make sure your compliance efforts are top-notch," Fayed says. ■

Are you ready for a HIPAA breach?

Do you think your organization is immune to the possibility of a data breach?

"Don't think it's not going to happen to you," says **Rebecca C. Fayed, Esq.,** an attorney in Washington, DC.

Breaches have occurred at some highly regarded healthcare organizations considered the "best and the brightest" in the industry, says Fayed, who is associate general counsel and privacy officer at The Advisory Board Company, a research, consulting, and technology services firm that works with healthcare organizations.

In 2011, Massachusetts General Hospital (MGH) and the University of California at Los Angeles (UCLA) Health System both paid a heavy price to OCR for HIPAA violations.

In February, after what became known as "the million-dollar subway ride," MGH agreed to a resolution agreement to pay the U.S. government a $1 million settlement and entered into a corrective action plan (CAP). The settlement resulted after a hospital employee left documents containing PHI on a subway.

In July, UCLA agreed to a settlement of $865,000 and a CAP for HIPAA violations that resulted from workforce members snooping into celebrity patients' records.

And in September, Stanford Hospital in Palo Alto, CA, which has a close relationship with Stanford University, found itself in the headlines after a contractor posted a private database containing medical records of 20,000 patients to a public website.

"These are not names usually in the headlines for providing poor patient care or for anything negative, but in the last year they were in the headlines for breaches and impermissible disclosures," Fayed says.

And as much as organizations work to put the right compliance programs in place and train workforce members, "quite frankly, sometimes [a breach] just happens," she says.

Organizations must prepare so they are ready if a breach does occur. "Being unprepared can be costly and embarrassing," says **Christine Arevalo,** director of healthcare identity management at ID Experts in Portland, OR.

Consider taking the following steps so your organization is ready to respond to a breach:

➤ **Prepare for the possibility of a breach.** Organizations should prepare themselves by developing and implementing an incident response and breach notification procedure, Fayed says. This way, if a breach happens you'll be ready to respond and notify affected individuals.

An incident response plan (IRP) serves as the baseline for a defensible response, allowing providers to react to complaints or data breaches in a timely, methodically, and documented way, says Arevalo.

Just as you plan for other crisis situations, prepare for a breach. "It is just as important as a backup and recovery or business continuity plan or fire evacuation plan," she says. However, ID Experts finds that most of its clients do not have a current IRP, Arevalo notes.

➤ **Establish an incident response team.** The IRP process is valuable because it forces crucial conversations in organizations, Arevalo says. The process of developing a response plan allows a leadership team to become aligned on topics such as breach survival, she adds.

As such, you will want to establish an incident response team, Fayed says. Involve people at the top of the organization who can make decisions and run the show if a breach occurs.

Arevalo recommends gaining support for an IRP via an executive meeting to set your organization's priorities for 2012. You will want to organize a cross-functional team meeting. Using a template for your IRP is okay, but Arevalo cautions against using a fill-in-the-blank approach. "A thoughtful IRP should be a living document, which is never allowed to collect dust."

➤ **Take preventive steps.** As part of the process, consider ways to prevent a breach from occurring. Encrypt all PHI, says Fayed. "Make this bold, underlined, and starred—encrypt your PHI. It's sort of your get-out-of-jail-free card," she says. If your patient info is encrypted, you are not subject to the breach notification obligations per the HHS interim final rule.

Also address how you will handle a breach that is the fault of a business associate (BA), Fayed says. When negotiating BA agreements, consider including an indemnification clause and a breach notification provision that addresses who is responsible for what if a breach occurs. You may also want to consider purchasing data security breach insurance, she says.

It may be helpful to have a consultant help you develop an IRP, Arevalo says. Having a third party facilitate this process has many benefits, such as bringing down political barriers in organizations, which sometimes prevent open dialogue about objectives. As part of the planning process, perform an inventory of your PHI and personally identifiable information, she says. "It's hard to protect data if you aren't sure where it is at."

Once you have a plan in place, you need to test it regularly and make improvements, as requested by OCR, Arevalo

says. The HIPAA Security Rule requires covered entities to identify and respond to security incidents and mitigate any harmful effects.

Although there's work involved, you will benefit in the long run. "There is evidence to suggest that having a plan in place can have a positive economic impact on the cost of response," Arevalo says. "Simply being deliberate about the process can be beneficial."

Being unprepared can cost you money and further damage your reputation on top of the hit caused by the breach.

"Unintended consequences of poorly executed breach plans can typically be pinned back to poor planning up front," Arevalo says. Poor planning can result in a lack of coordination and interdepartmental breakdown, making it more difficult to react quickly and effectively to a breach.

Rapidly changing world brings new HIPAA compliance challenges

A look at what's happening over the next nine months

Technology is changing rapidly, and it's creating big challenges for healthcare organizations when it comes to protecting PHI. Privacy and security officers should keep an eye on these changes—from more mobile devices to social media to cloud computing—over the next several months, according to a group of industry prognosticators.

The group of industry leaders focused on the following trends they say will be important in healthcare data:

➤ **Mobile devices, from tablet computers to smartphones, will continue to pose a risk for healthcare organizations.** Healthcare organizations will not be immune to data breach risks caused by the spread of mobile devices in the workforce, says **Larry Ponemon, PhD,** chair and founder of the Ponemon Institute in Traverse City, MI.

More physicians and clinicians than ever were using mobile devices in 2011 (see related story on p. 1). However, a recent Ponemon survey found that while more healthcare providers are using mobile devices, almost half don't take steps to secure them.

➤ **More class action lawsuits will be filed against healthcare organizations for failing to protect PHI.** Class action litigation firestorms are imminent, says **Kirk Nahra, Esq., CIPP,** partner in the Washington, DC, office of Wiley Rein, LLP. These lawsuits will be on the rise the rest of the year as patients sue healthcare organizations for PHI breaches, Nahra says.

2011 saw several class action lawsuits brought against organizations, some of which involved business associates (BA), due to breached patient data, he says. Regardless of their outcomes, these lawsuits are a significant risk and tremendous expense for organizations affected by them, Nahra says.

One of those class action lawsuits, filed in March 2011, sought $5 million in damages against Health Net, Inc., and IBM over the loss of computer storage devices that held the medical histories, financial data, and Social Security numbers of almost 2 million patients. The lawsuit was filed on behalf of current and former members of Health Net, alleging the managed healthcare organization and IBM violated California's patient privacy law. Health Net began notifying patients in March 2011 that their PHI was compromised following reports from IBM, its IT vendor, that several server drives were unaccounted for at a data center in California.

➤ **Social media risks will continue to grow.** As more physicians and healthcare organizations move to social media to communicate with patients and promote services, the misuse of social media will increase as will the risk of PHI exposure, says **Chris Apgar, CISSP,** CEO and president of Apgar & Associates, LLC, in Portland, OR. Too often organizations do not develop a social media use plan, and employees who use the online tools represent a significant risk; they can

potentially expose PHI through their personal social network pages, Apgar says. These exposures can lead to patient vulnerabilities, data breaches, civil penalties, and loss of business, he notes.

➤ **Cloud computing will create liability risks.** Because it will require fewer resources, cloud computing is an attractive option for some healthcare organizations, especially as health information exchanges increase.

However, cloud computing is not a panacea, says **James C. Pyles, Esq.,** principal at Powers Pyles Sutter & Verville, PC, in Washington, DC. Cloud computing is a quickly growing form of Internet data storage. It typically refers to a shared computer service and data storage infrastructure that resides in a large off-site server managed and controlled by a third party. The third party provides computing and storage resources to anyone anywhere with an Internet connection. A healthcare organization does not own, but rather leases, the physical hardware and stores its data on the remote servers provided by the cloud service provider.

The problem is that this technology is outpacing security and creating unprecedented liability risks, Pyles says. When it comes to cloud computing, privacy and legal issues abound, including compliance with HIPAA privacy and security regulations and allocation of liability when a privacy breach occurs, he says. A covered entity (CE) will need to enter into a carefully written BA agreement with a cloud computing vendor before disclosing PHI and should ensure that it has adequate cyber security insurance to cover the direct and indirect costs of a breach, Pyles advises.

➤ **Growing reliance on BAs will create new risks.** Economic realities will force healthcare providers to continue to outsource many of their functions, such as billing, to third-party BAs, says **Larry Walker,** president of The Walker Company in Lake Oswego, OR.

However, BAs are considered the "weak link in the chain" when it comes to data privacy and security, Walker says. Sixty-nine percent of organizations that participated in the recent Ponemon Institute survey said they have little or no confidence in their BAs' ability to secure patient data. Third-party mistakes account for 46% of data breaches reported in the study.

➤ **Organizations will continue to risk reputation fallout from data breaches.** Identity theft and medical identity theft resulting from data breach exposure causes patients financial and emotional harm, and can often result in patients seeking out different medical providers, says **Rick Kam,** president and cofounder of ID Experts, a Portland, OR, company. He is also chair of the American National Standards Institute's "PHI Project," a project to research the financial impact of a healthcare data breach. Data breaches damage reputations and cost money. According to the Ponemon study, the average lifetime value of one patient to a healthcare organization is more than $113,000, meaning the loss of even one patient can have a significant economic impact to an organization in terms of lost revenue.

➤ **The use of mobile devices will explode in healthcare.** The use of tablets, smartphones, and tablet applications in healthcare is growing exponentially, says **Christina Thielst,** a health administration consultant and blogger from Santa Barbara, CA.

Nearly one-third of healthcare providers use mobile devices to access electronic health record (EHR) systems, according to a study by the nonprofit Computing Technology Industry Association. Providers will need to balance usability, preferences, security, and budgetary concerns, as well as adopt written terms of use that cover employees and contractors who use personal devices at work, Thielst says.

➤ **More organizations will face HIPAA violations.** Increased emphasis on willful neglect by OCR will lead to greater enforcement of HIPAA, according to **Adam Greene, JD, MPH,** partner in the Washington, DC, office of Davis Wright Tremaine, LLP.

Many CEs will be focused over the next year on the 150 HIPAA Privacy and Security Rule audits mandated by HITECH, which OCR plans to conduct by the end of 2012, says Greene. OCR has hired contractor KPMG, LLP, to conduct the audits, and a pilot program of 20 initial audits is now under way. Organizations will also

focus on the publication of the final rules (not released as of presstime) implementing modifications to the HIPAA regulations, he says.

But the biggest change may be at the OCR investigational level, says Greene, OCR's former senior health IT and privacy specialist. Expect OCR to aggressively pursue enforcement against noncompliance due to "willful neglect" this year, resulting in a sharp uptake in financial settlements and fines in the coming years, he predicts. This year, OCR will expect everyone's privacy and security programs to have matured, Greene says.

➤ **Organizations will need to focus on training.** Privacy and security training will be an annual requirement, says **Peter Cizik,** cofounder and CEO of BridgeFront, based in Vancouver, WA. Healthcare organizations have gotten better at putting procedures in place, but staff are still not following them, he says. Because the majority of breaches are caused by human error, not technology failures, targeted training and awareness programs are one of the most effective ways to prevent data breaches, Cizik says.

➤ **Organizations will pay more attention to fraud risk education.** The rise in the number of people committing fraud will increase the need for fraud risk education, according to **Jonnie Massey, CPC, CPC-P, CPC-I, CPMA, AHFI,** supervisor of the Special Investigations Unit at Oregon Dental Service Companies in Portland. During hard economic times, there are more fraudsters and more opportunities for them to gain or keep healthcare benefits to which they are not entitled. Educating those at risk for fraud and communicating the consequences for committing it may deter someone from stepping over the line or prevent those at risk from becoming victims, Massey says.

➤ **Healthcare organizations will turn to cyber liability insurance.** As healthcare organizations continue to implement their EHR systems, they will consider options to protect themselves and their patients, according to **Christine Marciano,** president of Cyber Data Risk Managers, LLC, in Freehold, NJ. When a healthcare organization suffers a data breach, the damage is not only to its bottom line, but also to the reputation of its brand, Marciano says.

With their increased vulnerabilities and as part of a data breach response plan, healthcare organizations will increasingly turn to cyber security/data breach insurance policies, she predicts.

Given all these trends, privacy and security officers may need more than a couple of aspirin. The prognosticators advise organizations to view protecting patients' PHI as a patient safety issue. They warn that if the right actions are not taken, healthcare data breaches will reach epidemic proportions this year. ■

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

March 2012

Tips from this month's issue

Mobile device explosion (p. 1)

1. Balance use and security with mobile devices. Adopt written terms of use with employees and contractors who will be using personal devices in the workplace.
2. Consider prohibiting residents or fellows from storing any PHI on their device.
3. Have mobile device users sign an agreement governing the use of the device, including provisions that they will not store PHI on the device and must use password protection.
4. Require all devices to be encrypted.
5. Protect your network from malware or viruses that may spread from an employee's personal device.
6. Create a manual for mobile device users that outlines how the devices should be used.
7. Be careful about securing PHI. Caution employees that their devices are for business purposes and that downloads and applications on the devices will be monitored periodically.
8. Advise users to avoid losing their device by keeping it with them at all times.
9. Users should not let other people borrow their device and should be aware of their surroundings when using it.
10. Advise users to report losses of their devices immediately; if a device is stolen, they should file a police report.
11. Prohibit users from attempting to gain elevated privileges to their device.
12. Implement security measures that will wipe mobile devices of all content after multiple incorrect password attempts.
13. Advise users to log out of their account when finished using a device and not to share their passwords with others.
14. Update the device when any new security measures become available.

Breach response (p. 6)

15. Prepare for the possibility of a breach.
16. Develop an incident response plan and establish an incident response team.
17. If a breach occurs, investigate the incident.
18. Follow your procedures and initiate actions of your incident response team.
19. If you don't have an incident response team, identify individuals in the best positions to help investigate and respond to the incident.
20. Pull together the right group of people who can make decisions and keep your investigation moving.
21. Collect the following information:
    - The facts surrounding the incident. Did the breach involve a stolen or lost laptop computer, a backup tape, or a portable storage device? Was

an e-mail or fax sent to a wrong recipient? Were paper records thrown in the trash?
   - Data elements. Did the incident involve names, addresses, phone numbers, PHI, Social Security numbers, or credit card numbers?
   - Number of people affected.
   - States in which affected people live and total affected people in each state.
   - Whether the information was encrypted.

22. Mitigate the harm and take corrective action.

23. Be able to show OCR or affected individuals that you took appropriate steps, such as filing a police report about a stolen laptop computer or contacting the recipient of wrongly sent PHI and asking for the information to be returned or destroyed.

24. When it comes to corrective action, you may need to terminate an agreement with a business associate, revise your procedures, or sanction employees.

25. If your organization determines a breach occurred, you will need to decide whether you will offer credit monitoring services to those affected.

26. Assess and document whether the incident is a "breach" under the HITECH Act/HHS breach notification rule. Access the regulations at *http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.*

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. *March 2012.*