June 2012 Vol. 12, No. 6

Briefings on HIPAA

• Privacy • Security • Transactions • Training

Get your HIPAA privacy program in compliance

Steps to keep your organization out of the headlines

If you are a HIPAA privacy officer, it might be looking pretty scary out there, said **Adam Greene, JD, MPH.**

"We're really entering into a new era of enforcement," said Greene, a partner at Davis Wright & Tremaine, LLP, in Washington, D.C., and a former regulator at OCR, the government agency that enforces the HIPAA Privacy and Security Rules.

Greene, who until last year was OCR's senior health IT and privacy specialist, spoke at the 20th National HIPAA Summit March 26 in Washington, D.C. "This is the year to take the training wheels off of your HIPAA program," he told the audience. "Many organizations are still not riding that bike particularly well."

So what can organizations do in this era of increased enforcement? Here's where Greene said organizations should focus:

➤ **Update your privacy program.** If your HIPAA privacy program hasn't changed since 2003, that's not a good thing, Greene said. When it comes to HIPAA, you need to have a culture of compliance in the following areas:

– Start with your policies. Were the policies you put in place in 2003 freshly purchased from a consultant? "If you bought HIPAA-on-a-shelf, if you are audited, the government will probably recognize that and may not be impressed," he said. Instead, make sure your policies are field tested and regularly revised. Consider your policies and procedures in terms of what works in practice. If your 10-year-old policy requires busy staff to dispose of all PHI by walking it to a shredder, chances are that policy is not working, Greene said.

> **"If you bought HIPAA-on-a-shelf, if you are audited, the government will probably recognize that and may not be impressed."**
>
> *—Adam Greene, JD, MPH*

– Look at your training program. In 2003, you probably provided HIPAA 101 to your workforce members—a one-hour summation of the Privacy Rule, along with certification they completed that training. In 2012, consider providing comprehensive training, Greene said. Make it specific to the recurring issues you see and to the workforce you have. If your training doesn't reflect the issues that pop up again and again when you look at your history of privacy incidents, it is not working. A policy is like a tree falling in the woods that no one hears if nobody is trained on it, he said.

– Be serious about sanctions for workforce members who violate HIPAA privacy. Your attitude in 2003 may have been that everyone was just learning about HIPAA; violators would get a proverbial slap on the wrist. Now your sanctions should demonstrate that you take privacy seriously, Greene said. If you are audited, the government will expect to

HCPro

IN THIS ISSUE

see you take appropriate sanctions for violations. You can't have a culture of compliance if there are no consequences to people's actions, he said.

– Audit your organization. In 2003, you may have said, "Let's keep our fingers crossed." Now you need to be looking at what is actually working in your organization and fixing what isn't working, Greene said.

➤ **Focus on continuous compliance.** Think of compliance as a loop. "Privacy is not a moment in time," Greene said. You should continually revise your policies and procedures. Train your workforce on those changes. Enforce sanctions on a continuing basis, and then self-audit. "That's the piece that most often gets lost," he said.

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

There is nothing in the Privacy Rule that says organizations need to do a self-audit, Greene said. However, the rule requires reasonable and appropriate safeguards. So expect OCR to look for organizations assessing what works.

➤ **Evaluate your training.** Does your training adequately cover basic concepts? For example, do your workforce members know what is considered PHI? Is your training tailored to particular issues arising in your organization? Does training focus on spotting issues, such as potential breaches?

Not every employee needs to be a HIPAA expert, but everyone should recognize the potential for a HIPAA violation and know they should bring it to someone's attention, Greene said. For instance, if employees are taking paperwork that contains PHI off-site, do they know how to properly secure that information? Does your training focus on real-world situations? Tailor training to what is happening in your organization.

➤ **Enforce consequences for noncompliance.** In practice, a nurse or billing agent who violates HIPAA may get fired. A physician may get peer review and that's the end of it, Greene said. Noncompliance should have consequences for *all* members of the workforce, he noted.

Sanction policies can be flexible to handle different levels of compliance. You may want to consider a zero-tolerance policy, but that is not the only solution, Greene noted. Think carefully about what will work in your organization. For instance, one organization had a zero-tolerance policy. Everyone in one department accessed a patient record, and all of the employees were fired. Unfortunately, there was no contingency plan for how to deal with the loss of an entire department, he said.

Whatever sanctions you impose, whether retraining or discipline, document it in your records. Make sure your policies, training, and safeguards reflect those sanctions. "Make it a continuous feedback loop," Greene said, and document where there have been changes.

➤ **Ensure auditing effectiveness.** "Auditing PHI is not just something to do under the Security Rule. It is something you should do under the Privacy Rule," Greene said. Start by following the PHI in your organization.

Where is PHI created? Where is it maintained? "PHI is throughout your organization," not just in your electronic health record system, Greene said. That includes places where you don't want it to be.

For instance, you may have a policy that says workforce members must not store any PHI on personal mobile devices. But just because you have a policy does not mean that people are following it. You need to audit across your organization.

Also, look at how PHI is destroyed. You only have to look at the settlement agreements with the CVS and Rite Aid pharmacy chains to know that improper disposal of PHI can get you in trouble, Greene said. Consent agreements with HHS revealed both pharmacies disposed of pill bottles and prescriptions that included PHI in trash containers without proper safeguards. Agreements included a $2.25 million settlement for CVS (announced February 18, 2009) and a $1 million payment by Rite Aid (announced July 27, 2010). How is PHI actually disposed of? This is a big challenge, but you need to make sure PHI is shredded or otherwise properly disposed of, Greene said.

Proper storage of PHI should also be considered. Just because an employee has access to a filing cabinet with a lock doesn't mean he or she is storing documents containing PHI there or even locking the cabinet.

As you audit, keep in mind that some procedures you have in place will not work. You need to discover these problems before patients or the government do, Greene said.

Do your employees understand the training you provided? Don't just give employees a generic quiz to assess their understanding. Is PHI being properly maintained at workstations? If you walk around your organization, you will rarely find that employees leave a wallet or stacks of bills out on their desks. Yet you will likely see stacks of paper records left there—records that potentially equate to millions of dollars of exposure, Greene said.

➤ **Document, document, document.** Be sure you have documentation for the following:

- Policies and procedures, both old and new. If OCR audits your organization, it may ask to see the documents in effect at the time of an incident, Greene said. Keep your documentation for six years from its effective date. (Why six? See below.)
- Patient privacy requests. Document these requests, as it will be hard to defend your organization in an investigation if you have no records, he said.
- Complaint investigations. Keep records of any internal investigations you conduct as a result of HIPAA complaints. Keep in mind that the statute of limitations for the government to take action under HIPAA is six years, Greene said. Records will allow you to defend your organization five or six years down the road if it takes that long for the government to launch an investigation.
- Training. If you don't document training, from an audit standpoint, it did not happen, Greene said. Document the substance of that training and the certifications given to workforce members. You don't want to find that your system overwrites your training documentation when workforce members receive new training.
- Sanctions. Document all sanctions you take as a result of HIPAA violations, including any retraining or counseling of workforce members.
- All safeguards of PHI. Document where you maintain information and how you dispose of it. "In the 2012 world of compliance you need to have robust documentation of all the safeguards you have, and that includes verbal information," Greene said. So, if important information is relayed at a team meeting, be sure to document it. If workforce members are warned not to talk about a patient's PHI in elevators where they can be overheard, document that warning in your policies.

It's been almost 10 years since the implementation of the Privacy Rule. Now that OCR is stepping up enforcement, be sure you beef up your own privacy program, Greene said.

"There are reasonable steps you can take to stay out of those headlines," he said. ■

Do your policies and procedures pass the test?

By now you know how critical policies and procedures are to your organization.

Assessing all of your privacy policies and procedures is key to your HIPAA compliance program, said **Adam Greene, JD, MPH,** a partner at Davis Wright & Tremaine, LLP, in Washington, D.C., and a former regulator at OCR.

Be sure to look closely at these key areas and ask yourself the following questions:

- **Privacy rights.** Are patients actually receiving notices of your privacy practices? Do you simply ask them to sign that they acknowledge your Notice of Privacy Practices? Do you provide them with a copy? Or if they ask for a copy, does someone say, "I'll get back to you"? Are all requests for restrictions considered? When are requests for alternative communications reasonable? Do you have a policy, and is your organization consistent about it? Are access and amendment requests recognized and handled in a timely manner, or do these responses fall through the cracks? Do you maintain disclosure logs? If you are audited, you may need to produce them.
- **Uses and disclosures.** Do your policies address recurring categories of uses and disclosures? This should be a fluid process. Do these procedures prove effective in real-world situations? For example, if a police officer requests information about a patient, do your procedures outline the process staff members should follow? Have minimum necessary policies been created for routine requests, uses, and disclosures? This is one of the most challenging areas to comply with, Greene said. Are minimum necessary criteria applied to nonroutine requests, uses, and disclosures? Are people following your policies and procedures in practice so they are always making reasonable efforts to disclose only the minimum necessary information?
- **Breach notification.** Do your policies and procedures provide a clear path for notification within your organization? Be sure your workforce members understand what to do if they suspect a breach. Are they notifying their supervisor? Do supervisors pass on the information to the privacy officer? "You have huge exposure if anyone in your organization knows about a breach and doesn't know who to notify," Greene said. Are there objective criteria for judging what constitutes a breach? "This has been a big issue of debate," he said. You need some criteria for how you determine whether a breach actually occurred.

While you may have a verbal policy and all your workforce members may understand what they need to do, put everything in writing. If you are audited, you need a documented policy and procedure to demonstrate HIPAA compliance, Greene said.

Are your workforce members texting PHI?

Another worry: Text messages that contain PHI

Belinda Setters, MD, knew she was possibly violating HIPAA regulations. But she had no intention of stopping.

Just what was the doctor doing that was so wrong? She was texting messages that contained PHI via her smartphone to fellow physicians and other healthcare professionals. And even though she knew the text messages were not encrypted and she could be violating HIPAA, Setters said the method of communication was too convenient for her to stop using it.

So Setters—who is director of hospital services and the geriatric medicine fellowship, as well as an associate professor of geriatric medicine, at the University of Louisville in Kentucky—urged those responsible for HIPAA privacy and security to take action. And they did, buying an application that encrypts text messages and thus protects the university system from a HIPAA breach.

"I flat out told my HIPAA folks, 'I'm not giving up texting. We've got to find a way to do this. I'm a very busy hospitalist. You've got to help me find a way to make this happen,' " Setters said. A pilot program is working successfully in her department, and the organization plans to roll it out universitywide and hospitalwide to include all of the facilities within the system.

Setters was one of several speakers to participate on a panel at the 20th National HIPAA Summit March 27 in Washington, D.C., to discuss the use of mobile messaging.

Panel members were clear: Mobile messaging can present a risk when it comes to HIPAA privacy, and organizations need to take steps to address the danger.

Communication via texting

Greg Young, information security officer at Mammoth Hospital in Mammoth Lakes, Calif., said he heard the same pleas from physicians at his facility. "That assertiveness of, 'I'm going to text, and I'm not going to give it up,' I definitely saw that in our physicians," he said.

Young said doctors at his organization, like Setters, insisted that texting is more efficient than using the telephone to communicate about patients. He said some physicians were arm-twisting staff to use their personal cell phones to text them patient information.

Young decided the hospital needed to come up with a solution to allow physicians and other staff to send text messages without creating a privacy and security risk. Like the University of Louisville, he turned to one of the vendors in that market, TigerText, Inc., based in Santa Monica, Calif. TigerText is a secure mobile messaging platform that encrypts text messages on both senders' and receivers' phones.

A growing phenomenon

Brad Brooks, cofounder and president of TigerText, who moderated the panel, said texting has infiltrated many aspects of communication, including communication at work. Thirty percent of adults say they actually prefer to be contacted via text over voice.

The smartphone revolution has been embraced by physicians and other healthcare professionals, Brooks said. One survey found 80% of physicians use smartphones and 73% of physicians text about their work, he said.

While texting is a potential area for privacy and security vulnerability, it's also an opportunity to improve communication, Brooks noted.

It may not be HIPAA compliant, but texting is now the chosen means of communication for many physicians, said Setters. It's used by physicians, residents, and medical students at the University of Louisville. Many have tried to keep identifying patient information out of their text messages, she said, but that can create its own danger.

Setters said she modified text messages to omit PHI but was concerned that could still be a HIPAA violation and a risk to patient safety.

For instance, instead of texting about Sue Jones in room 575 at Jewish Hospital who has pancreatitis, doctors might instead refer to "the patient with pancreatitis on the fifth floor." But what happens if patients have the same diagnosis? If physicians don't clearly identify a specific patient in their text message, that presents a huge risk in terms of patient safety, Setters said. The wrong patient could ultimately get the wrong medication or treatment.

Setters said she has also seen residents and nurse practitioners send photos of CT scans and MRIs to physicians via text that clearly showed the patient's name, medical record number, or date of birth.

Harshul Patel, MD, a hospitalist at Trover Health Systems in Madisonville, Ky., agreed an encryption solution makes texting safer. Instead of sending a message that says, " 'Call me regarding the patient on the fourth floor,' now we can say what needs to be done or even write orders to the nursing staff," he said.

The advantages of texting

Why are physicians and other healthcare professionals so adamant about texting information? Both Patel and Setters said it makes their jobs easier.

With a traditional pager, you have to page someone and wait for them to come on the phone or call you back, Patel said.

With text messaging, you can tell whether someone received and read the message, said Setters. The response is usually pretty instant. "It's a huge time-saver," she said.

While it might take 24 hours on average to respond to an email, Brooks said the average response to a TigerText message is less than five minutes.

"I'm convinced it shaves an hour off my day," Setters said—freeing up time for her to do other tasks.

The next generation of physicians may be even more impatient when it comes to communication. "The better the technology gets, the more impatient we get. We want the information, and we want it now. We want the latest device, and we just don't want to hear why we can't have it. We just don't have time for that," Setters said.

But without encryption, PHI in a text message can be accessed by an unintended recipient. Setters recalled a physician who texted another doctor about the death of a patient. Unfortunately, he entered the wrong telephone number, and the message went to the wrong person. With texting, there's no way to authenticate who you are sending a message to, she said. A message with confidential information could go to a random person on the street—someone who has no business having it.

"I'm a really heavy user," admitted Setters, who sends close to 100 texts a day.

How it works

Young said Mammoth Hospital adopted a texting solution and put out a policy to staff. The texting solution encrypts text messages on both the sender's and recipient's phone and on the server it passes through. The hospital's policy makes it clear to staff that the facility is providing a HIPAA-compliant way to text and that is what they must use, he said.

"Use our solution, and you can text anything you want," he said.

The hospital is now rolling out the application to its medical staff. The hospital sets up an account for each user and assigns a login name and password, which it can revoke at any time, Young said. If a phone is lost or a physician decides to leave the hospital's medical staff, the hospital can immediately bar access, he said.

The information is encrypted in case a phone with sensitive text messages is lost or stolen. "It's always protected for the patients' sake," Young said.

Copies of the text messages are encrypted and saved on the server they are transmitted through, he said. Mammoth saves messages on the server for two days, but facilities can change that length of time to whatever they desire, Young said.

If healthcare professionals want to save messages, they can print them out and put them in the medical record, he said, noting that hospitals should have a policy and procedure for doing so.

Setters and Patel said healthcare professionals at their facilities can use their own personal mobile phones to send text messages. Patel said people can use their own device as long as the application is downloaded to their phone and they have a user ID and password to log onto the TigerText servers.

When evaluating a system, Setters said hospitals need to be sure the encryption service works on all the devices your staff owns. While most physicians at the university have an iPhone®, some residents have a BlackBerry® or Android™, she said. If that is the case in your facility, it is important for your encryption solution to work on a variety of platforms.

Justifying the expense

So how can healthcare organizations convince those holding the purse strings to spend money on a new application to encrypt text messages? Show them what it could cost if they don't protect their facility's PHI, said Young. In California, for a first offense, a single breach from a text message could result in a $17,000 fine, he said.

"It makes your physicians more efficient, and it's a safe solution. The return on investment would be if you're not using a safe HIPAA-compliant text solution and you had a breach, it's going to cost you," he said.

"That's the argument I made when I approached our administration and said we have to do this," Setters said. "The university did not want to hear that they needed to purchase something else."

However, the cost was actually less than the cost of pagers, which most physicians aren't using, she noted.

Physicians are also worried about paying the price for a HIPAA violation. Setters recalled hearing a radio report about the million-dollar fine one healthcare system had to pay for a HIPAA violation. "It scared the crap out of me," she said. "I intentionally know I'm violating HIPAA. I could face fines per text. I'm a university professor. I don't have the money to pay that."

Texting also has the benefit of increasing physicians' efficiency. Faster communication frees up physician time for other tasks, including the possibility of seeing more patients. Setters said she billed about $40,000–$60,000 more in patient care last year while working the same number of hours.

"It's really improved our efficiency," she said. ■

Editor's note: Sign up for HCPro's audio conference "Mobile Devices and Text Messaging: The Risk of Unencrypted PHI." To sign up for the 90-minute, June 4 show (1 to 2:30 p.m., EDT), go to http://tinyurl.com/bnafosn.

Free tool can help you determine whether it's a breach

When is a breach a breach? Only when it meets the criteria set out by the government.

But knowing when an incident that has occurred in your healthcare organization is truly a HIPAA breach can be a challenge.

When an incident occurs—such as a lost laptop computer or a discovery that backup computer tapes are missing—most organizations hit the panic button, says **Frank Ruelas, MBA,** principal of HIPAA College, based in Casa Grande, Ariz.

Privacy and security officers may be tempted to sound the alarm and call in outside help to assist in the crisis at hand. But Ruelas says that at this stage of the game, he advises HIPAA leaders to take a deep breath, calm down, and assess the situation. Do you really have a breach on your hands?

Ask questions to determine a breach

Ruelas says organizations can use a free tool to help them decide whether an incident constitutes a breach: the HITECH Act Breach Notification Risk Assessment Tool developed by the North Carolina Healthcare Information & Communications Alliance, Inc. (NCHICA).

"I am a very strong supporter of the NCHICA breach risk assessment tool for evaluating incidents to see if they rise to the level of a breach, and if they do, to determine the potential for harm," says Ruelas.

The risk assessment tool is one of the most popular features on the NCHICA website, says **Holt Anderson,** executive director of the nonprofit consortium of more than 230 organizations representing the many sectors of the healthcare industry. "It's been downloaded thousands of times," he says. You can find the tool at *www.nchica.org.*

NCHICA developed the tool, which helps walk organizations through different steps, in response to the interim final rule on breach notification issued by HHS' OCR in 2009. You can find the interim final rule, "Breach Notification for Unsecured Protected Health Information," at *http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf.*

Note: As of presstime, OCR has yet to issue a final rule on breach notification. OCR in March sent the final rules, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules," to the Office of Management and Budget for review—a process that can take up to 90 days.

In addition to looking at the federal requirements, NCHICA also incorporated the laws specific to North Carolina in the tool. Facilities located in other states should also consider their own applicable statutes that govern breach notification, Anderson says.

Adapt for your organization

Covered entities (CE) can modify and use the breach assessment tool so long as they retain the copyright and attribute the document to NCHICA.

Over the past year, Ruelas says he has taken the first section of the tool, which poses a series of questions to help organizations determine whether they've suffered a breach, and put it into a spreadsheet. Organizations can project it on a screen during their risk management or compliance meetings as they review reported incidents and take their first pass at determining whether any of the incidents may be a breach, he says.

You can find a copy of Ruelas' adapted form on p. 10. For an electronic version, go to *www.hipaacollege.com* and locate the filesharing page, where an icon will take you to the skydrive location that contains the file "HIPAA-Section 1 NCHICA Tool."

The tool is especially helpful for small and mid-sized organizations, as well as physicians' offices, Ruelas says.

There are two other sections to the NCHICA tool—an assessment to determine whether a breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent it requires notification, as well as a scoring system to help rank the risk level. Organizations can take those sections and design their own similar risk assessment worksheets, Ruelas says.

Know the current requirements

While many people use the words "incident" and "breach" interchangeably, they are really two different things, says Ruelas.

Keep in mind that not every incident is a breach, he says. To be considered a breach, an incident needs to meet the definition found in the interim final rule on breach notification.

"When there's an incident, oftentimes people say, 'We've had a breach.' However, a breach equals an incident that you've assessed to have a level of harm where it requires a response," Ruelas says.

The interim final rule requires that CEs notify each affected individual of a breach of "unsecured PHI."

The HHS breach notification guidance says PHI is "unsecured" if it is not encrypted or properly destroyed. A breach is defined as the unauthorized acquisition, access, use, or disclosure of PHI.

The regulations provide exceptions for inadvertent, harmless mistakes. They include:

- Disclosures where an unauthorized person who receives information would not reasonably have been able to retain the PHI
- Certain good faith or inadvertent access by or disclosure to workforce members in the same organization
- Inadvertent disclosures among persons similarly authorized to access PHI

The interim final rule also includes a harm threshold. A breach occurs when an organization believes an incident "poses a significant risk of financial, reputational, or other harm to the individual." So the guidance provides the possibility for an organization not to notify individuals—if it performs a risk assessment and determines the risk of harm is significantly low.

A breach can be a costly problem for CEs. It requires notification of all the patients affected by a breach without unreasonable delay (no later than 60 days) after the CE discovers or should have discovered the breach.

If 500 or more individuals are affected, you must notify the Secretary of HHS of the breach and OCR will post the details on its website. You must also notify the media if more than 500 people are affected.

Figure it out

So the rules leave organizations to figure out whether a breach occurred. For instance, a staff member just faxed a patient's information to five different hospitals. Should you be worried?

No, says Ruelas, because all of those hospitals are covered by HIPAA regulations and are bound to protect that information. "You don't have a breach," he says.

However, if a staff member leaves a medical record on a bench in a subway station, and the file contains a patient's HIV and genetic information, you do have a breach because the information can be accessed by unauthorized individuals and it is not encrypted.

The NCHICA tool helps organizations assess the situation and make the appropriate determination.

"I've used this tool 50 times over the last couple of years. The actual times it was a breach was not very many," Ruelas says.

While people may get emotional at the thought that patient PHI has been compromised, "the tool is devoid of emotion and the rush to judgment," Ruelas says. Instead, it simply asks a series of yes-or-no questions, thus allowing organizations to make decisions on a consistent basis, he says.

"It allows you to screen the emotion and the anxiety out. In the end you have your own assessment, based on X, Y, and Z," Ruelas says.

Ruelas recalls a large hospital that hired a third party to conduct its data analysis. He strongly recommended the hospital ensure the third party have USB drives with auto encryption. The third party lost those USB drives, which contained some 100,000–200,000 patient records.

Ruelas received a frantic call from hospital officials. “I said, ‘Bring up the tool. Everybody relax. Do you have a situation where there is a HIPAA violation? Yes. Does it involve unsecured or unencrypted PHI? No,’ ” he says. “The USBs are undecipherable. You don’t have a breach. You are done [with the process].”

Breach notification tool

Indicate yes or no to the following three questions:		
1. Is there a HIPAA Security/Privacy Rule violation?	Yes—Proceed to next question	No—Stop, no breach has occurred that requires notification of affected individuals
2. Was data secured or properly destroyed in compliance with the requirements in the breach notification rule?	Yes—Stop, no breach has occurred that requires notification	No—Proceed to next question
3. Does this incident qualify as one of the following exceptions? (see below)	Yes—Stop, no breach has occurred that requires notification	No—Breach apparent, proceed to risk assessment worksheet*
Good faith, unintentional acquisition, access, or use of PHI by employee/workforce member	Example: A billing employee receives and opens an email containing patient PHI, which a nurse mistakenly sent. The billing employee notices he is not the intended recipient, alerts the nurse of the misintended email, and then deletes it.	
Inadvertent disclosure to another authorized person within the entity or Organized Health Care Arrangement (OHCA)	Example: A physician who has authority to use or disclose PHI at a hospital by virtue of participating in an OHCA with the hospital is similarly situated to a nurse or billing employee of the hospital.	
Recipient could not reasonably have retained the data Data is limited to limited data set that does not include dates of birth or zip codes	Example: A covered entity (CE), due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOB) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the CE can conclude that the improper addressees could not reasonably have retained the information.	

* If you did not hit a “Stop,” proceed to work through the risk assessment to determine whether the breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent that it would require notification. You can find this assessment at *www.nchica.org.*

Source: Frank Ruelas, principal of HIPAA College, Casa Grande, Ariz. Reprinted with permission. Adapted from the HITECH Act Breach Notification Risk Assessment Tool developed by the North Carolina Healthcare Information & Communications Alliance, Inc.

HIPAA Q&A

Notification of a patient with HIV; HIPAA-mandated software; unencrypted messages

by Chris Apgar, CISSP

Q **If a physician uses an answering service and receives unencrypted messages from an answering service, is it a violation of the HIPAA Security Rule?**

A If a physician uses his or her smartphone to contact an answering service, it is not a violation of the HIPAA Security Rule. It may represent a risk, but generally phone transmissions (mobile and landlines) do not need to be encrypted unless the answering service is an automated service where messages are stored on a server that is open to the Internet (such as cloud-based answering services).

Even then, encryption is not required, but it is strongly recommended. Conduct a risk analysis, identify risks such as those related to unencrypted PHI, and then determine whether those risks are acceptable risks. A covered entity or business associate can elect to prohibit physicians and other workforce members from using a smartphone to access messages from an answering service. That, though, is a decision that is made at the entity level and is not a HIPAA mandate.

Q **Do caregivers employed by a continuing care retirement community (CCRC) have the right to know the diagnosis of a patient or resident if the diagnosis is HIV? The standard of practice followed by all workforce members employed by the CCRC is abiding by universal precautions.**

A Caregivers do not need to know if a patient or resident is HIV positive. The HIPAA minimum necessary standard applies here. If the caregivers are providing assistance with daily living, they don't need to know the patient's or resident's diagnosis, whether it's HIV or a host of other ailments. Employed or contracted physicians, nurses, physical therapists, and so forth do need to know because they are providing healthcare treatment. To assess and properly treat the patient or resident, they need to know the patient or resident's diagnosis.

Q **A home health agency was informed by an assisted living facility that the home health agency was prohibited from leaving its patient information book at the facility because it was a violation of HIPAA. The patient information book does not include any PHI. The assisted living facility stated the home health agency could not see patients if it leaves the patient information book. The home health agency is required by state law to distribute information**

Last six months of HIPAA 2012: What are your plans?

HIPAA in 2011 was marked by a lot of negative headlines for organizations.

In 2012, we want to keep the headlines going—but for the final six months of this year, we want to generate more positive ones.

HCPro, Inc., which publishes **Briefings on HIPAA,** wants to hear the good things that are happening in the world of HIPAA compliance in 2012.

We invite you to share your success stories with us, and you and your organization could be featured in one of our publications.

To share your stories, please contact Senior Managing Editor Dom Nicastro at *dnicastro@hcpro.com.*

contained in the patient information book. Is this a HIPAA violation?

A It is not a HIPAA violation. HIPAA addresses protecting the privacy of individuals' individually identifiable health information or PHI. If making certain information available to residents of a long-term care facility such as an assisted living facility is required by state law, the home health agency would be violating state law if the patient notifications are not made available to residents. There is no prohibition related to leaving what amounts to educational material for residents to review.

If the purpose of the patient information book is to market certain services provided by the home health agency, it moves into that gray area in HIPAA regulations called marketing. As long as the same information is available to all residents and is not used for targeted marketing to certain individuals with specific diagnoses, it would not violate the marketing provisions of HIPAA or HITECH.

Q A physician is converting from paper charts to an electronic health record (EHR) that is federally certified. Until the conversion and implementation is complete, the physician uses a specific application for dictation. The vendor for the software informed him he is required to use this particular software because of a HIPAA mandate. Is this really a HIPAA mandate?

A None of the HIPAA regulations require the use of a specific application or specific software. HIPAA spells out privacy, security, and transaction related requirements but is technology neutral. This was not changed by the passage of HITECH. The EHR that will be implemented has been federally certified to meet the meaningful use incentive program requirements. Even the implementation of a federally certified EHR is not a HIPAA or HITECH mandate. It is only required if the physician is interested in taking advantage of the meaningful use incentive program. ■

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

A supplement to **Briefings on HIPAA**

Privacy & Security Primer

A training tool for healthcare staff

June 2012

Tips from this month's issue

HIPAA privacy compliance (p. 1)

1. Update your privacy program. If your HIPAA privacy program hasn't changed since 2003, that is not a good thing.

2. Have a culture of compliance when it comes to HIPAA.

3. Start with your policies. Make sure your policies are field tested and regularly revised.

4. Consider your policies and procedures in terms of what works in practice.

5. Look at your training program. Consider providing comprehensive training.

6. Make training specific to the recurring issues you see and to the workforce you have.

7. Be serious about sanctions for workforce members who violate HIPAA privacy.

8. Your sanctions should demonstrate that you take privacy seriously. You can't have a culture of compliance if there are no consequences for people's actions.

9. Audit your organization. Look at what is actually working in your organization and fix what isn't working.

10. Focus on continuous compliance. Think of compliance as a loop.

11. Continually revise your policies and procedures.

12. Train your workforce on those changes.

13. Enforce sanctions on a continuing basis, and then self-audit.

14. Evaluate your training. Does your training adequately cover basic concepts? For example, do your workforce members know what is considered PHI? Is your training tailored to particular issues arising in your organization? Does training focus on spotting issues, such as a potential breach? Do employees taking PHI off-site know how to properly secure that information? Does your training focus on real-world situations?

15. Tailor training to what is happening in your organization.

16. Enforce consequences for noncompliance. Noncompliance should have consequences for all members of the workforce.

17. Consider a zero tolerance policy, but remember that is not the only solution. Think carefully about what will really work in your organization. Whichever policy you choose, document it in your records.

18. Look at the sanctions you impose and make sure you reflect that experience in your policies, training, and safeguards.

19. Ensure auditing effectiveness.

20. Follow the PHI in your organization. Where is PHI created? Where is it maintained?

21. Look at how PHI is destroyed.

22. As you audit, keep in mind that some procedures you have in place will not work. You need to discover these problems before patients or the government do. Do your employees understand the training you provided?

23. Don't just give employees a generic quiz to assess their understanding. Ensure that they actually do understand. For example, make sure PHI is being properly maintained at workstations.

24. Make sure PHI is shredded or otherwise properly disposed of.

25. Document, document, document. Be sure you have documentation for the following:

- Policies and procedures, both old and new
- Patient privacy requests
- Complaint investigations
- Training
- Sanctions

Privacy questions (p. 4)

26. Are patients actually receiving notices of your privacy practices? Do you simply ask them to sign that they acknowledge your Notice of Privacy Practices? Do you provide them with a copy? Or if they ask for a copy, does someone say, "I'll get back to you"? Are all requests for restrictions considered? When are requests for alternative communications reasonable? Do you have a policy, and is your organization consistent about it? Are access and amendment requests recognized and handled in a timely way, or do these responses fall through the cracks? Do you maintain disclosure logs? If you are audited, you may need to produce them.

27. Do your policies address recurring categories of uses and disclosures? This should be a fluid process. Do these procedures prove effective in real-world situations? Have minimum necessary policies been created for routine requests, uses, and disclosures? Are minimum necessary criteria applied to nonroutine requests, uses, and disclosures? Are people following your policy and procedure in practice so they are always making reasonable efforts to disclose only the minimum necessary information?

28. Do your policies and procedures provide a clear path for notification within your organization? Do supervisors pass on the information to the privacy officer?

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