

BRIEFINGS ON

HIPAA

- Privacy
- Security
- Transactions
- Training

HIPAA can pose unique challenges for assisted living facilities

Complying with the HIPAA Privacy Rule isn't always easy, but it can be even more complicated for assisted living facilities.

A privacy officer in Wisconsin—who oversees a critical access hospital, a skilled nursing facility, and an assisted living facility—sums up some of the difficulties. The tenants in the assisted living facility share meals and activities, and many become good friends with one another, she says.

It's only natural that these elderly tenants share news with their friends and neighbors, but how does HIPAA come into play when they ask facility caregivers to share information? "They are a close-knit community and it is

hard to keep tenants and caregivers from talking among themselves," says the privacy officer.

While it's not a problem for tenants to share information, the caregivers, who are workforce members of the assisted living facility, may be bound by HIPAA not to reveal tenants' PHI.

For instance, one tenant recently ended up in the hospital with an illness. When one of the resident assistants from the assisted living facility visited her, the tenant said she wanted her friends to know how she was doing and did not care if the employee told the other tenants what was wrong with her.

"It is a very good idea to make sure such verbal requests or verbal permission to share health information is documented to avoid problems later for the facility."

—Chris Apgar, CISSP

How does such a desire mesh with the HIPAA Privacy Rule, which requires covered entities (CE) to protect individuals' PHI? For assisted living facilities, this question can be somewhat complicated.

A CE or not?

One of the first questions to consider is whether the assisted living facility is a CE under the Privacy Rule definition. There are many different assisted living models, and facilities can provide a variety of services and financial arrangements.

CEs, which must comply with HIPAA, include healthcare providers that transmit health information electronically using standard transactions. Not all healthcare providers are CEs; however, healthcare providers that bill or check health plan benefit eligibility electronically—for example, in connection with a transaction for which HHS has adopted a standard—will generally be categorized as such.

IN THIS ISSUE

p. 4 Data breaches: A case study
Seattle Children's Hospital's proactive approach to data security serves as a model for other organizations.

p. 7 Cloud computing
A technological advance in data storage offers healthcare organizations quick access to important information, but is the cloud right for your organization?

p. 8 Top 10 tips to consider for data storage
Elizabeth H. Johnson, Esq., a partner at Poyner Spruill, LLP, offers 10 points to consider before committing to the cloud.

p. 9 HIPAA Q&A
You have questions; we have answers.

p. 11 2012 story index
Looking for a **Briefings on HIPAA** story from 2012? We have an index of all them for you to reference easily.

Inside: Privacy & Security Primer

HCPPro

Is an assisted living facility considered a “provider” under the privacy rule? It depends. To help healthcare providers, HHS has a question and answer decision tool on its website, with guidance on how to determine whether an organization is a CE under HIPAA, says **Kate Borten, CISSP, CISM**, president and founder of The Marblehead Group in Marblehead, Mass. To view the tool, go to www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf.

Borten says a good question to ask is whether your assisted living facility submits electronic claims for medical care to a healthcare insurer, such as Medicare, Medicaid, or a private insurer, for payment. If so, or if

you use a third party to do that billing, then without a doubt you are covered by HIPAA, Borten says. It doesn't matter if you only submit claims once in a while, she adds; you are a CE under HIPAA regardless of submission frequency.

Look at your setup

Are most assisted living facilities CEs? It depends on their setup, Borten says.

“The question raises some complicated issues,” agrees **Adam H. Greene, JD, MPH**, a partner at Davis Wright Tremaine, LLP, in Washington, D.C., who until recently worked as an OCR regulator.

For instance, if a hospital, nursing home, and assisted living facility are one legal entity, then they are a single CE under HIPAA, he says. But if the assisted living facility does not conduct any HIPAA-covered transactions electronically, then the CE has the option of treating itself as a hybrid entity and can choose whether to include the assisted living facility in the healthcare component that is covered under HIPAA, Greene says.

If it is included in the healthcare component, then the assisted living facility is fully subject to HIPAA, but it will be able to more readily share information internally for its overall healthcare operations. If the facility is excluded from the healthcare component, then it is not subject to HIPAA, but the entity as a whole must be careful to ensure that PHI does not flow from the hospital and nursing home side to the assisted living facility side unless certain criteria are met under HIPAA, Greene says.

Different assisted living facilities may reach different conclusions as to whether it makes sense to be subject to HIPAA, he says.

Generally, independent assisted living facilities are not CEs, says **Chris Apgar, CISSP**, CEO and president of Apgar & Associates, LLC, in Portland, Ore. However, there are variations across the states, and there may be cases where at least part of an assisted living facility is a CE, he says. For instance, if the facility includes a clinic with physicians who provide healthcare treatment to

Editorial Advisory Board		Briefings on HIPAA
HCPPro		Editor: Jacqueline Fellows
		Contributing Editors: Chris Apgar, CISSP, President Apgar & Associates, LLC, Portland, Ore.
		Mary D. Brandt, MBA, RHIA, CHE, CHPS, Vice President of HIM Scott & White Healthcare, Temple, Texas
		Joanne Finnegan
<hr/>		
Jana H. Aagaard, Esq. Law Office of Jana H. Aagaard Carmichael, Calif.	Reece Hirsch, Esq. Partner Morgan Lewis One Market, Spear Street Tower San Francisco, Calif.	Mac McMillan, FHIMSS, CISSM Cofounder and CEO CynergisTek, Inc. Austin, Texas
Kevin Beaver, CISSP Founder Principle Logic, LLC Acworth, Ga.	William M. Miaoulis, CISA, CISM CISO & HIPAA/HITECH Service Line Leader Phoenix Health Systems Dallas, Texas	Phyllis A. Patrick, MBA, FACHE, CHC Founder Phyllis A. Patrick & Associates, LLC Purchase, N.Y.
Kate Borten, CISSP, CISM Founder The Marblehead Group Marblehead, Mass.	Frank Ruelas, MBA Principal HIPAA College Casa Grande, Ariz.	
John R. Christiansen, JD Managing Director Christiansen IT Law Seattle, Wash.		
Ken Cutler, CISSP, CISA Vice President MIS Training Institute Framingham, Mass.		
Rick Ensenbach, CISSP-ISSMP, CISA, CISM, HITRUST Manager Wipfli, LLP Minneapolis, Minn.		
<p>Briefings on HIPAA (ISSN: 1537-0216 [print]; 1937-7444 [online]) is published monthly by HCPPro, 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 © 2013 HCPPro, 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 HCPPro, 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@hcppro.com. • Visit our website at www.hcppro.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.</p>		

tenants, that would be considered a hybrid entity, part CE and part non-CE, he notes.

Get authorization to share information

If you determine your assisted living facility is a CE, then you are covered by HIPAA. But remember that your tenants are not subject to HIPAA; only your employees and workforce are covered, says Borten.

That said, while assisted living facilities want to be mindful of their tenants' needs, they still must follow the law. "It is difficult. The boundaries blur. I have a lot of sympathy. But you are still obligated to have policies and procedures that protect patient privacy. The law is the law," Borten says.

You must ensure your workforce members follow HIPAA's rules and regulations, she says. They must not share tenants' health information without permission.

Getting that permission isn't necessarily an onerous task. The Privacy Rule allows for what is called the "opportunity to object" under 45 *CFR* 164.510, says Apgar.

"If the facility receives verbal approval or a verbal request to let other tenants and employees of the assisted living facility know about a trip to the hospital, health conditions, and so forth, there is not a need to obtain written authorization," he says.

But Apgar advises you to document that permission regardless. "It is a very good idea to make sure such verbal requests or verbal permission to share health information is documented to avoid problems later for the facility," he says. In order to avoid liability, documentation is a must.

Borten agrees. Caregivers should document that the tenant is of sound mind and has given permission to share his or her information, she says.

Greene says assisted living facilities should obtain a HIPAA-compliant authorization to disclose information to other tenants.

To do this, Borten recommends drafting a standardized authorization form and asking tenants to sign it. This authorization is not meant to be open-ended, so it is a good idea to check periodically to make sure a tenant is

still comfortable with the decision to have medical information exchanged with others.

Also, be aware that while a tenant may give authorization to share information about a particular hospitalization, that doesn't mean he or she will approve of any and all information being shared—a month or two later, the tenant may contract another diagnosis or condition that he or she may not want anyone to know about, Borten says.

The National Center for Assisted Living (NCAL) recommends a facility obtain written authorization from each resident to clarify what information it can share and with whom. Facilities also need to be aware of their state laws that may cover the sharing of residents' information, says **Lisa Gluckstern**, public affairs director at NCAL.

"Though the Privacy Rule is somewhat 'flexible' regarding sharing of information with family and friends involved in care, other federal and state laws may not be," Gluckstern cautions. So facilities need to be sure they are in compliance with Medicare *Conditions of Participation* and more stringent state laws, she says.

Let tenants share

Given the fact that many tenants want to share information with their friends, Borten says assisted living facilities could consider setting up a bulletin board where the tenants themselves can post information. For instance, residents could post that "Jane went to the hospital" or "Fred fell in the parking lot and is recovering in rehabilitation."

As long as the tenants themselves exchange the information, it is outside the scope of HIPAA, she says. "It takes the CE out of it. People decide to share or they don't." ■

Questions? Comments? Ideas?

Contact Contributing Editor

Joanne Finnegan

Email joannef100@hotmail.com

A case study

How one Seattle hospital is ready to respond to data breaches

When it comes to data breaches, it's not a question of if, but a matter of when, says **Cris V. Ewell, PhD**, chief information security officer at Seattle Children's Hospital, Research, and Foundation.

It's with that assumption in mind that Ewell has helped build a model to respond to data breach incidents. "You have to have that expectation [that a breach will occur]," says Ewell, who talked about Seattle Children's incident response process in a webinar hosted by ID Experts.

The statistics back Ewell up. In fact, 96% of hospitals had a data breach in the past year and 60% of hospitals experienced multiple breaches, says **Mahmood Sher-Jan**, vice president of product management for ID Experts in Portland, Ore. OCR, the agency that enforces the HIPAA Privacy and Security Rules, has reported over 500 breaches that affected 500 or more individuals since it began posting the information in February 2010. That represents over 21 million patient records.

Incident management challenges

Hospitals and healthcare organizations face several challenges when it comes to having a strong incident management plan:

► **Organization.** One of those challenges is determining who is involved in a hospital's data breach response. "Who is in charge? Someone has to be accountable," Ewell says. Involve everyone in helping prevent data breaches, he says, from those at the highest level of your organization, such as the board of trustees, down to the help desk staff who field calls about potential incidents.

You may need cultural changes to break down the silos at your organization and allow for a multidisciplinary response and management team.

► **Expectations.** People in your organization, including hospital executives, may have the unrealistic expectation that data breaches can be entirely prevented,

Ewell says. Instead, organizations should expect that a breach will occur, he says.

► **Taking on too much.** You need to figure out what you can handle as an organization, Ewell says. Too often hospitals take on too much when it comes to their data breach response, he says.

You may be able to handle a small breach on your own, but what if a large incident occurs involving hundreds of thousands of patients? Can you set up a call center to field patient questions within 24 hours of the breach? Do you have interpreters who can answer patient questions in six or seven major languages? Can you run forensics to determine the extent of the breach? Many organizations will need outside help.


Plan how you will handle a data breach; ideally, you should have contracts set up ahead of time with the agencies that will provide assistance, Ewell says. Don't be reactive and wait until an incident happens.

Determine breach risk

One of the most difficult parts of breach response is determining the risk to the institution and the patient whose data may be compromised, Ewell says. With all breaches, you need to tell the story, he says. Look at motive and intent. Why did the breach happen? Why did the person responsible for the breach want that information?

The breach notification interim final rule, issued in August 2009, requires covered entities to determine if a breach of PHI poses a significant risk of financial, reputational, or other harm to an individual. You need a process in place to determine that risk, and then you need to document how you arrive at a decision. If you determine that the risk created by an incident is not significant enough to harm a patient, meaning you do not need to notify the individual of the breach, this determination must be documented, he says.

Figure 1



Seattle Children's
HOSPITAL • RESEARCH • FOUNDATION

Corporate Information
Security Management

CISO Investigation Report

Date

Case background

Include

- *Date of incident*
- *Date of discovery of incident*
- *Date incident reported to CISO*
- *General incident background and information*

Relevant findings

Include

- *What information or system was involved*
- *Extent of information involved in the incident*
- *Where information was transmitted or utilized*
- *Information about the individual(s) that had unauthorized access to the information or system*
- *Root cause of incident*
- *Impact of incident*
- *Mitigation steps*

Significant events date

KEY
Important Events
Authorized Activity
Unauthorized Activity
Unknown Activity

*All times are represented as Pacific Daylight Time unless otherwise noted

Time	Event

Summary of risk

Include

- *Notification recommendation*
- *Risk related to incident*

Data included in appendixes

<ul style="list-style-type: none"> Appendix A – Contact information Appendix B – Internet protocol address information Appendix C – Heat ticket Appendix D – SIRT notification Appendix E – Forensic report 	<ul style="list-style-type: none"> Appendix F – Interviews conducted and interview documentation Appendix G – Applicable RCWs or other laws Appendix H – Other
--	---

Source: Cris B. Ewell, PhD, chief information security officer at Seattle Children's Hospital, Research, and Foundation. Reprinted with permission.

© 2013 HCPro, Inc. For permission to reproduce part or all of this newsletter for external distribution or use in educational packets, contact the Copyright Clearance Center at www.copyright.com or 978-750-8400.

A question of culture

Seattle Children's culture of governance and organizational support helps ensure the success of its breach response model. As chief information security officer, Ewell reports to a board-level committee, as well as the hospital's general counsel. The hospital has monthly corporate compliance meetings. Ewell also meets weekly with the information security department to talk about security issues.

Seattle Children's is a risk-based organization that looks holistically at privacy and security issues throughout the entire organization, rather than by individual departments. It has an incident management process that outlines how an incident is handled from start to finish.

The process includes:

- Preparation and planning
- Discovery and reporting
- Analysis and assessment
- Response
- Recovery and remediation
- Post-incident review

As soon as an incident is discovered, the organization does a review to determine if an actual breach occurred. For instance, a laptop computer may have been stolen, but if it contained no PHI, the incident does not represent a breach. With each incident there is a recovery and remediation process, where the designated office looks at what occurred and asks how it can do things better.

Roles and responsibilities

Seattle Children's has designated offices and individuals who are responsible for different types of data. Effective incident response takes teamwork, Ewell notes. "You can't do this alone. This is more than security."

The type of data dictates who will lead the response efforts. Here is the breakdown:

- Privacy office—all incidents involving paper PHI
- Chief information security office—ePHI or personally identifiable information
- Corporate compliance office—corporate compliance issues

- Research compliance office—research compliance issues
- Information services security office—incidents not included above

The hospital has an incident management team. You'll want one at your facility too; be sure to include representatives from various departments, such as operations, legal, human resources, privacy, security, and information services.

Understand HIPAA compliance

When it comes to compliance with HIPAA, you have to know the rules, Ewell says.

As part of the ongoing OCR compliance audits, the audit teams are looking at incident response efforts by healthcare organizations, he says. So, for instance, you need to meet notification time frames if a breach occurs and include all of the required information in a notification letter.

When he worked at a previous organization, Ewell says he was faced with a breach situation that caught staff largely unprepared. "You have to pre-plan this stuff," he says. Finding resources when you are under the gun is not easy.

Another issue you must address is sanctions for workforce members. Have a notification, awareness, and prevention policy. If OCR audits your organization, it will expect to see that you have enacted a sanctions policy and that workforce members understand it. Be consistent in how you apply sanctions, and document any incident. "You can't have enough documentation," Ewell says.

Ewell completes a CISO Breach Investigation Report for every data breach. (See p. 5.) A year or two after an incident, he can go back and re-create what occurred. Keep those reports for a period of time and then destroy them based on your data retention policy.

HIPAA requires you to take preventive measures to ensure a data breach does not happen again. You want to show that you put controls in place and that it helped your security posture, Ewell says. ■

Is the cloud a good place for you?

The cloud has come to healthcare, but is cloud computing for your organization?

It's a question you can only answer after doing some careful homework. Just as you conduct a risk assessment when it comes to other areas of privacy and security, you want to engage in careful consideration before you jump into the cloud, says **Phyllis A. Patrick, MBA, FACHE, CHC**, president of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y.

"Look at this as a business decision. How does going to the cloud fit your business plan?" Patrick says.

Cloud computing can offer scalability, flexibility, and cost advantages for healthcare organizations. But because they manage sensitive PHI, healthcare organizations must ensure those cloud services provide the privacy and security needed for their data, she says.

Healthcare organizations need to ask lots of questions before they move to the cloud, agrees **Elizabeth H. Johnson, Esq.**, a partner at Poyner Spruill, LLP, a law firm in Raleigh, N.C.

But Johnson notes that organizations shouldn't start with the assumption that the cloud will be riskier than what they are doing right now when it comes to their PHI and other data. There could be good reasons to make the switch, such as security, functionality, and availability of data to users.

Organizations should compare what they are currently doing and what will happen when they move to the cloud, Johnson says. Think about what data you may be moving. Is it your patient records? Is it payroll, processing, or billing information? Is it entire systems, applications, and networks?

Consider whether you have some already-existing cloud arrangements or data hosting arrangements, or whether the move will be a brand-new venture for your organization, says Johnson. For instance, if you access email through a Web browser, you are already on the cloud. "We started calling it [the cloud] five years ago, but it's not as new as we think," she says.

What exactly is cloud computing?

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources—for example, networks, servers, storage applications, and services—that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A good resource for healthcare organizations on cloud computing is NIST's Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, released in 2012, says Patrick. You can download a copy at www.nist.gov/manuscript-publication-search.cfm?pub_id=911075.

Cloud computing comes in a variety of service models and deployments, says Patrick. These range from public software-as-a-service models, such as electronic health records (EHR) and email that are accessed solely through a Web browser, to private infrastructure-as-a-service models, such as those where a healthcare provider pools hardware resources to provide departments with access to shared data processing and storage.

A cloud provider is a business associate, so you need to learn as much as you can about cloud services before deciding whether a cloud computing environment is right for your organization, Patrick says. You want to be sure you find a solid vendor who understands the HIPAA Security Rule requirements, she says. Request a copy of the vendor's Statement on Standards for Attestation Engagements 16, which reports on controls at a service organization as reviewed by outside auditors.

Think about how you want to transition to the cloud, Patrick says. Do you want to transfer all of your major systems to the cloud at once, or do you want to run a trial by just transferring one small system?

Entering into an arrangement with a cloud provider requires healthcare organizations to proceed with caution and keep their eyes open, Patrick says. You

need to carefully evaluate data security risks posed by moving applications, systems, and networks to the cloud. Consider factors such as whether the vendor has proper backup and disaster recovery capabilities. What happens if a system goes down? How is your data protected?

Where is data located? Is there one facility or several? Is the data physically secure? Also, consider how you would get out of the arrangement if you want to terminate the contract. It's important to talk with a legal advisor and make sure you have a contract that protects your organization, Patrick says.

Remember that healthcare organizations maintain

the ultimate responsibility for managing their data and complying with legal and regulatory requirements, including HIPAA, Patrick says.

Evaluate a potential vendor on its ability to provide safe, reliable services, but realize that in the end, *you* are responsible for ensuring the confidentiality of the information, she says.

There are tools and resources to help healthcare organizations make decisions about cloud computing. One that Patrick recommends is a toolkit put together by the Health Information and Management Systems Society. You can find it by visiting www.himss.org/asp/topics_PStoolkit_CloudSecurity.asp. ■

Ten points to consider when it comes to cloud computing

When considering whether cloud computing is the right choice, healthcare organizations need to ask lots of questions, says **Elizabeth H. Johnson, Esq.**, a partner at Poyner Spruill, LLP, a law firm in Raleigh, N.C.

Here are 10 points she advises them to consider:

- What kind of data will you put on the cloud, and what laws are attached to that data? If it's the PHI of your patients or employees, be sure to keep HIPAA requirements in mind. If you are putting data on the cloud that contains Social Security numbers, look at your state laws that govern that information.
- Think about whether your data will be on a public or private cloud, Johnson says. If it is public, you are sharing that infrastructure with other people. You want to be sure there is a logical separation, so data can be on the same server without being commingled. With a private cloud, the infrastructure or hardware is yours alone and not shared with anyone else; however, this kind of arrangement is usually more expensive. Whatever you decide, understand how it works so your data integrity is maintained, she says.
- Know whether any other parties or subcontractors are involved.
- Know where your data will be physically located. Is it Texas? Canada? India? There may be a primary location, but there may also be mirrored locations, so know all the physical locations of your data, Johnson says.
- Understand how you can get your data if you change providers, if the provider sells the business, or if there is litigation.
- Understand liability and indemnification caps. How much liability is a vendor willing to accept? Address this topic at the beginning of your discussions. Who's at fault if there is a data breach? What happens if a subcontractor loses a backup tape of your data?
- Ask about insurance coverage. Does it cover a breach incident specifically? Know what kind of insurance and coverage a provider has.
- Do not buy a vendor's argument that the company is not a business associate because it doesn't access the data it stores.
- Complete a risk analysis. OCR has made it clear if you make major operational changes, you must do a risk analysis, Johnson says. This needs to be documented. A risk analysis will not only keep you compliant, it will help you evaluate whether the cloud is the right decision for your organization.
- Be sure that anything a salesperson promises you is actually included in your contract. Make sure the contract contains language that protects your interests. For instance, you may want language that requires the cloud provider to ask you before adding any subcontractors to your arrangement.

HIPAA Q&A**Patient preference, incidental disclosures, and email blasts**

by Chris Apgar, CISSP

Q I work at a teaching hospital affiliated with one of the nation's top universities and medical schools.

Our emergency department staff forgot to return a patient's insurance card and mailed it to the patient via regular first-class mail without notifying her that they were doing so. A few days later, the patient was traveling when she discovered that the insurance card was missing. She called our emergency department and was told the card had been mailed to her home address.

The patient said she understands that mistakes happen occasionally, but that she was far more upset by our failure to contact her and ask her preference for returning the card than by our initial failure to return it while she was at the hospital. The patient said that had we called her, she would have come to the hospital to retrieve it and that she would have done so promptly because of her imminent travel plans.

Did we do the right thing by sending the insurance card via regular first-class mail without calling the patient first? Should we have sent it via certified mail or in some other manner that required a signature confirming receipt?

Also, should our privacy policy address situations like this?

A This amounts to a violation of patient preference versus a violation of the privacy or security of the patient's information. There is no regulatory requirement to contact the patient before sending back a left-behind insurance card.

First-class mail is protected by federal mail tampering laws, so intercepting and fraudulently using another individual's insurance card would amount to a criminal act.

There is no need to change your privacy policy in an effort to comply with state or federal law. HIPAA represents the privacy and security floor—you need to at least comply with HIPAA. You may implement more stringent privacy practices if you wish, and this could include a procedure that requires a call to the patient before sending that left-behind insurance card back. Implementing such a procedure would probably lead to a happier patient, but it's not legally required.

Q Two patients with very similar names see the same primary care provider in our office. They are sisters-in-law whose names are Michele A. Smith and Michelle B. Smith.

Staff members often retrieve the wrong files for these patients, who become aware of the mistake when the physician asks Michele or Michelle a question that doesn't pertain to her but does pertain to her sister-in-law (e.g., a question about diabetes). The sisters-in-law have a friendly relationship and seem to be familiar with each other's health issues.

This has occurred more than once and with both patients. Do these recurring situations violate HIPAA?

A Incidental disclosures of PHI do not represent a HIPAA Privacy Rule violation. On the other hand, repeatedly disclosing one patient's PHI to another patient would likely be seen as a violation.

A better way to look at it is this: What would be the consequences of an ongoing mix-up if it involved two patients who did not know each other? It is important to implement controls to reasonably ensure Michele and Michelle's medical records are not mixed up.

Q A patient of our group practice of primary care physicians, specialists, and allied health professionals recently notified us that she received unencrypted email from a member of our office staff.

We regularly send e-blasts about various wellness programs to our patients. Unlike communication from our clinical staff, these messages are unencrypted. A patient responded to the email address provided in a recent e-blast about a new weight program that we are offering. The patient asked that we call her regarding the program and provided her telephone number. Her email included no specific questions.

One of our staff members responded via unencrypted email that identified the patient's primary care provider, referenced an inaccurate diabetes diagnosis, identified the insurer and indicated the number of covered nutrition visits annually, and provided self-payment information.

Was an unencrypted email response inappropriate in this situation, and if so, what must we do next?

A If the e-blasts are general and do not reveal any PHI about an individual, except for that individual's name and email address, it is not critical for those email messages to be sent encrypted. On the other hand, if patient PHI is sent unencrypted and it includes specific information about the patient (such as, for example, medical diagnosis, insurance information, primary care physician, and covered visits), it can lead to a violation of the HIPAA Security Rule.

It is important to remember encryption is an "addressable" implementation specification, but that does not mean it is optional. The rule requires covered entities implement the controls "as written," implement an equivalent control, or justify not implementing the control. In the case of encryption, there is no real justification for not implementing the control if email will be used to send PHI to patients. Encryption solutions fit budgets of all sizes, and there generally is no problem with interoperability between different solutions. If you have access to a website, you will likely have no problem sending and receiving secure messages.

There also is the issue of breaches of unsecure PHI. If someone intercepts that unencrypted email message, it represents a breach of unsecure PHI. If that happens, business associates are required to notify covered entities, and covered entities are required to notify individuals as well as OCR. Covered entities can assess risk—will significant harm be caused to that individual? If the message is intercepted by an unauthorized individual, from a conservative perspective, it may well cause significant harm. It's advisable to not send any PHI via email unless it's encrypted. The regulatory and practical risks are too high, not to mention the potential for patient harm. ■

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.

Don't miss your next issue!

If it's been more than six months since you purchased or renewed your subscription to **BOH**, be sure to check your envelope for your renewal notice or call customer service at 800-650-6787. Renew your subscription early to lock in the current price.



Briefings on HIPAA 2012 index

Breaches

Are you ready for a HIPAA breach? March, p. 9.

CMS receives failing grade for breach notification.
Dec., p. 6.

Data breaches are happening ... but how? Jan., p. 7.

Data breach experience teaches important lessons.
Oct., p. 4.

Four steps to minimize your data breach risks.
Feb., p. 4.

Free tool can help you determine whether it's a breach.
June, p. 8.

HIPAA awareness POPPs at Boston hospital.
Oct., p. 5.

Latest study shows major increase in data breaches.
Feb., p. 1.

Planning ahead facilitates effective breach response.
Oct., p. 1.

Sample privacy and security incident response policy.
Oct., p. 6.

Steps to help your organization respond to a breach.
March, p. 6.

What you can learn from CMS' breach notification mistakes. Dec., p. 8.

Compliance tips

Audit and monitor your organization's efforts.
Nov., p. 1.

Begin with code of conduct, policies, and procedures.
July, p. 5.

Compliance officer job description. Nov., p. 3.

Convince your leaders to invest their dollars.
May, p. 8.

Do your policies and procedures pass the test?
June, p. 4.

Education and training are essential components.
Aug., p. 6.

Get your HIPAA privacy program in compliance. June, p. 1.

Help workforce learn from the mistakes of others.
Oct., p. 10.

How to improve your training program. Feb., p. 8.

Integrity of PHI at ABC organization. Aug., p. 11.

Know where it goes: Map the flow of your PHI.
Aug., p. 8.

Newsletter keeps HIPAA front and center. April, p. 7.

Rapidly changing world brings new HIPAA compliance challenges. March, p. 10.

Responding appropriately to complaints of noncompliance. Oct., p. 12.

The role of compliance officers and committees.
Aug., p. 10.

Sample privacy and security violations sanctions policy.
Oct., p. 8.

Sample working off-site security agreement. Oct., p. 5.

Test staff knowledge with these scenarios. July, p. 7.

EHRs

EHR security: Why it's everyone's battle. Nov., p. 10.

Privacy, security concerns high in HIEs. July, p. 10.

Stage 2 won't increase HIPAA requirements. April, p. 5.

Enforcement actions

An \$18.5 million HIPAA lesson for healthcare organizations. May, p. 1.

OCR got tough: Heightened HIPAA enforcement in 2011.
Jan., p. 9.

HIPAA Q&A

Copy fees, inquiries about deceased patients. Aug., p. 12.

Digital signatures, minimum necessary standard.
July, p. 8.

Relocating? Taking a new job?



If you're relocating or taking a new job and would like to continue receiving **BOH**, you are eligible for a free trial subscription. Contact customer service with your moving information at 800-650-6787.

Encryption levels, disclosures to BA, employee sanctions.
April, p. 8.

Fundraising, other providers, going out of business.
Oct., p. 11.

Mental health issues; accounting of disclosures.
Jan., p. 11.

Notification of a patient with HIV; HIPAA-mandated
software; unencrypted messages. June, p. 11.

Patients' medical records after physician death; privacy
when patient beds are close. Feb., p. 11.

Patients who receive others' information. Nov., p. 8.

Security cameras, UB-04 forms, unreviewed test results.
Dec., p. 11.

HITECH Act

HIPAA/HITECH final rules, finally? May, p. 4.

Mobile devices

Are your workforce members texting PHI? June, p. 5.

Don't let inadequate security be your downfall.
Aug., p. 8.

Healthcare system develops mobile device checklist.
May, p. 10.

Manage risks associated with mobile devices. July, p. 6.

Mobile devices another PHI challenge. March, p. 1.

Staff newsletter promotes use of checklist. May, p. 12.

OCR audits

The audit is over. The real work begins. Feb., p. 7.

Audits to continue in 2013, OCR process evolving.
Dec., p. 1.

Have these documents ready for a HIPAA compliance
audit. April, p. 5.

Hospital undergoes one of first OCR audits.
April, p. 1.

Important takeaways from OCR audit results.
Aug., p. 6.

Initial OCR audits complete; more to come.
May, p. 6.

An inside look at how one hospital is preparing.
Dec., p. 2.

OCR advises next steps to consider. Aug., p. 2.

OCR HIPAA audit protocol key activities. Aug., p. 4.

OCR protocol information a valuable compliance tool.
Sept., p. 1.

OCR releases data from first 20 HIPAA compliance
audits. Aug., p. 1.

A tight frame for compliance audits. Feb., p. 6.

Timeline of a HIPAA compliance audit. April, p. 4.

Twelve quick tips for audit readiness. April, p. 3.

What you might not know about OCR HIPAA audits.
July, p. 1.

Privacy/security

Five tips to help ensure patient privacy. Dec., p. 8.

HIPAA, hooray for the new year. Jan., p. 8.

Privacy notice—acknowledgement of receipt. Nov., p. 7.

Sample policy: Walk-around security reviews. Dec., p. 5.

Sample privacy notice content and delivery policy.
Nov., p. 5.

Survey shows many organizations experience HIPAA
breaches, remain unprepared for an audit. Jan., p. 1.

What are some of the biggest concerns regarding HIPAA?
Jan., p. 6.

Why do we need a notice of privacy practices?
Nov., p. 4.

Product watch

Avoid a shutdown due to data loss. Jan., p. 10.

Data availability with some caveats. April, p. 10.

Get back to business quickly when disaster strikes.
July, p. 9.

Spectrum offers attractive option for EHR conversion.
Dec., p. 12.

Social networking

Ensure compliant use of social media, networking.
Nov. p. 12.

How hospitals can help physicians meet social media
challenges. April, p. 12.

Teach your physicians, staff proper social media protocol.
April, p. 11. ■

Privacy & Security Primer

**A training tool
for healthcare staff**

January 2013

Tips from this month's issue

HIPAA poses unique challenges for assisted living facilities (p. 1)

1. If a hospital, nursing home, and assisted living facility are one legal entity, then they are a single covered entity (CE) under HIPAA.
2. If the assisted living facility does not conduct any HIPAA-covered transactions electronically, such as electronic billing, then the CE has the option of treating itself as a hybrid entity and can choose whether to include the assisted living facility in the healthcare component that is covered under HIPAA.
3. HHS has a question and answer decision tool on its website, with guidance on how to determine whether an organization is a CE under HIPAA.
4. Tenants are not subject to HIPAA, but it is important to ensure staff members follow rules and the HIPAA regulations, and not share tenants' health information without permission.
5. If tenants give verbal permission to workers to share information about hospital visits, health conditions, etc., with other tenants, written documentation is recommended, but not required, and should be updated periodically.

Seattle Children's Hospital prepares for data breaches (p. 4)

6. In 2012, 96% of hospitals had a data breach and 60% of hospitals experienced multiple breaches. OCR, the agency that enforces the

HIPAA Privacy and Security Rules, has reported over 500 breaches that affected 500 or more individuals since it began posting the information in February 2010, representing over 21 million patient records.

7. Organizations should expect that a breach will occur, and contracts should be set up ahead of time with the agencies hospitals will depend on for help.
8. Organizations should have a process in place to determine risk.
9. The interim final rule, issued in August 2009, requires CEs to determine if a breach of PHI poses a significant risk of financial, reputational, or other harm to an individual.
10. Monthly corporate compliance meetings along with weekly meetings with the information security department to talk about security issues are effective strategies Seattle Children's uses to prepare for and prevent data breaches.
11. Seattle Children's also says audit teams are looking at incident response efforts by healthcare organizations as part of the ongoing OCR compliance audits.

Cloud computing (p. 7)

12. Cloud computing can offer scalability, flexibility, and cost advantages for healthcare organizations, but it is important to do a risk assessment to make sure cloud services provide the privacy and security needed for sensitive PHI.

13. A good resource for healthcare organizations on cloud computing is the National Institute of Standards and Technology's Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, released in 2012.
14. A cloud provider is considered a business associate, and it's important to request a copy of the vendor's Statement on Standards for Attestation

Engagements 16, which reports on controls at a service organization as reviewed by outside auditors.

15. When picking a vendor, one factor to consider is proper backup and disaster recovery capabilities.
16. Even though a vendor provides cloud services, healthcare organizations maintain the ultimate responsibility for managing data and complying with legal and regulatory requirements, including HIPAA.

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. *January 2013*.