

BRIEFINGS ON HIPAA

• Privacy • Security • Transactions • Training

The feds are coming Enforcement is increasing; help protect your hospital from breaches

Healthcare industry analysts say the recent multi-million-dollar fines levied by OCR for HIPAA violations are a wake-up call.

Hospitals and other healthcare organizations may now be wondering how to respond in a charged-up regulatory environment.

OCR shook things up in February when it issued big-ticket penalties for HIPAA Privacy and Security Rule violations. OCR fined Cignet Health of Prince George's County, MD, \$4.3 million and reached a \$1 million settlement with Massachusetts General Hospital (MGH) in Boston.

In the case against Cignet, OCR issued the first civil monetary penalty to a covered entity for violations of the HIPAA Privacy Rule. Cignet violated the rights of 41 patients when it denied them access to their medical records, HHS said. Cignet also failed to respond to OCR's

demands to produce the records and did not cooperate with investigators, HHS said.

MGH, meanwhile, agreed to pay \$1 million to settle allegations that it violated patient privacy laws when a hospital employee left records containing PHI on a subway train.

The hospital also agreed to a three-year corrective action plan (CAP).

Healthcare professionals who shared their insights with **BOH** concur that the sizable fines signal a call to action for the industry and are just the beginning of a trend of increased enforcement. They offer healthcare organizations the following advice:

➤ **Ensure that your organization implements appropriate security and privacy safeguards and best practices.** ARRA, an economic stimulus package that includes HITECH, marked a major shift in the issue of security, says **Catherine A. Allen**.

"The Stimulus Plan and the HITECH Act, combined with the rapid growth of electronic medical records, represent a sea change in the way the healthcare industry looks at the problem of data breaches," says Allen, chair and CEO of The Santa Fe Group, a consulting company based in Santa Fe, NM. It manages the Shared Assessments Program, which evaluates security practices and controls.

"In this climate, it is imperative that the healthcare industry understands the importance of using appropriate security and privacy safeguards and best practices," says Allen.

An in-depth review of these issues is under way, she notes. The American National Standards Institute (ANSI) has partnered with Allen's company as ANSI/Shared

"Electronic health information systems are the nuclear energy of health reform."

—James C. Pyles, Esq.

IN THIS ISSUE

p. 4 HIPAA Q&A
Take a look at tough questions from your fellow privacy and security officers, and check out our expert's responses.

p. 6 Product watch
This product may help you stay compliant with HIPAA privacy and security.

p. 7 Encryption best practices
Is your facility on the right track when it comes to encryption deployment?

p. 10 Seven steps to create a solid defense
Hackers, thieves, and spyware—your facility's infrastructure is constantly under attack. Here are some steps to build a solid protection base and secure patient information.

p. 12 Policy review grid
Sure, you have policies and procedures. But are you tracking them? Here's a sample grid that can help.

HCPPro

The feds are coming

< continued from p. 1

Assessments PHI to explore the financial impact of unauthorized PHI access.

► **When facing legal risks, make security a priority.** The added attention from OCR will bring more fines and lawsuits. “Given HITECH, what looks to be increased enforcement by OCR was inevitable,” says **Chris Apgar, CISSP**, president of Apgar & Associates, LLC, a consulting firm based in Portland, OR.

“I think this should send a clear message to the healthcare industry that enforcement has just started and, per an earlier statement by OCR, the focus will not just be on large organizations,” he says.

Even if OCR does not investigate an organization for an alleged privacy or security breach, patients can still file suit for damages, Apgar says.

“It is time for healthcare organizations to move security to the front burner, especially given the significant legal risk associated with breaches and other security incidents,” he says.

The OCR draft privacy, security, and enforcement rule is not final, but that doesn’t mean OCR won’t enforce rules that have been on the books for years, Apgar notes. For example, in the recent OCR monetary settlements, providers were fined for violating the HIPAA Privacy Rule—which became effective in 2003—rather than HITECH.

► **Creating a compliance program isn’t enough; you must also ensure compliance.** “Putting all of the administrative pieces in place is not sufficient—actual compliance matters,” says **Donald L. Bradfield, Esq.**, senior counsel in the legal department at Johns Hopkins Health System, based in Baltimore.

“My takeaways from the two events, but most particularly the [MGH] event, are that OCR has discovered its teeth and will not hesitate to bite hard,” says Bradfield.

MGH’s problems began when a hospital employee accidentally left records she was taking home with her on the subway, including records of patients with HIV/AIDS. “Human error will not excuse the institution, and once on-site, OCR will not limit itself to the circumstances of the particular event but will range more broadly to other areas of HIPAA compliance,” Bradfield predicts.

► **Implement your own corrective actions.** When you identify risks in your organization, take corrective action right away. “The healthcare organization needs to be in the driver’s seat,” says **James Christiansen**, CEO of Evantix, a risk management software company based in Aliso Viejo, CA.

“The financial impact of the fines to the healthcare companies is just the tip of the iceberg. The real big costs

Editorial Advisory Board Briefings on HIPAA

HCPPro

Group Publisher: **Lauren McLeod**, lmcleod@hcpro.com

Sr. Managing Editor: **Dom Nicaastro**, dnicaastro@hcpro.com

Contributing Editors: **Chris Apgar, CISSP, President**
Apgar & Associates, LLC, Portland, OR
Mary D. Brandt, MBA, RHIA, CHE, CHPS, Vice President of HIM
Scott & White Healthcare, Temple, TX

Jana H. Aagaard, Esq.

Law Office of Jana H. Aagaard
Carmichael, CA

Holly Ballam, RHIA

Corporate Privacy Officer and
Physician Liaison
Beth Israel Deaconess Medical Center
Boston, MA

Kevin Beaver, CISSP

Founder
Principle Logic, LLC
Acworth, GA

Kate Borten, CISSP, CISM

Founder
The Marblehead Group
Marblehead, MA

John R. Christiansen, JD

Managing Director
Christiansen IT Law
Seattle, WA

Ken Cutler, CISSP, CISA

Vice President
MIS Training Institute
Framingham, MA

Rick Ensenbach, CISSP, CISA, CISM

Governance/Risk/Compliance Practice
Manager
Aeritae Consulting Group
Saint Paul, MN

Reece Hirsch, Esq.

Sonnenschein Nath & Rosenthal, LLP
San Francisco, CA

William M. Miaoulis, CISA, CISM

Manager of HIPAA Security Services
Phoenix Health Systems
Montgomery, AL

Peggy Presbyla, RHIA, CHP

Field Operations Director
Infotrak Record Management
Syracuse, NY

Frank Ruelas, MBA

www.hipaacollege.com
Casa Grande, AZ

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 © 2011 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 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.

are tied to implementing the mandatory corrective actions and enduring the ongoing reporting that is typically part of the consent agreement," Christiansen says. "The worst part is the financial and organizational impact of the oversight that lasts for years."

For example, the MGH settlement's CAP will allow oversight by auditors for three years to ensure that the hospital safeguards patient privacy.

"A better approach is implementing a program before an incident occurs, including a plan for handling all the corrective actions," says Christiansen. You can spread the cost of the plan over several years to make it more manageable, he adds.

► **Conduct risk assessments to identify and correct your weaknesses.** "No healthcare organization wants a breach of their patients' information. Without conducting regular risk assessments, all organizations are in jeopardy," says **Rick Kam**, president and cofounder of ID Experts, a Portland, OR-based company that provides data breach solutions.

Documenting risk assessment helps demonstrate HIPAA compliance and effectively addresses patient privacy gaps that might delay or complicate electronic health record implementation and qualification for meaningful use incentives, says Kam.

The ramifications for failure to comply with HIPAA go beyond fines, he says.

They include CAPs, creation and implementation of revised policies, monitoring by government agencies, and potential harm caused to individuals whose information was breached.

► **Protect electronic health information systems and proceed with caution.** "Electronic health information systems are the nuclear energy of health reform," says **James C. Pyles, Esq.**, principal of Powers Pyles Sutter & Verville, PC, a Washington, DC, law firm. "They can bring great benefit if carefully used and controlled, and can be costly and produce catastrophic damage if not tightly controlled."

Electronic health information systems make it possible, for the first time in the history of medicine, to

breach the privacy of millions of individuals at the touch of a button, Pyles says. It's also possible to steal health information without having physical access to it—or even being on the same continent, he says.

► **Educate hospital leaders, including board members, about the risks.** Make your top leaders aware of the consequences of privacy and security breaches, says **Larry W. Walker**, president of The Walker Company in Lake Oswego, OR, and a governance consultant to health-care organizations.

"Based on my experience working with hospital governing boards, the large majority of board members have little or no real knowledge about the risk of patient health information breaches in their organizations," says Walker.

"Nor do they typically know what systems and processes are in place to prevent these breaches. It's not due to neglect—it's simply not a part of their governance thinking, and yet it's a distinctly critical governance accountability that must be understood and addressed by the board."

The safety and security of PHI is a vital trust, and boards must protect this trust through robust policies and careful, deliberate oversight, Walker says. That begins with a boardwide understanding of the vital importance of the issue.

Such an understanding is necessary to ensure that organizations allocate the resources necessary to safeguard patients' information and that their systems and processes work successfully 24 hours per day, 365 days per year to prevent breaches, he says. ■

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.



HIPAA Q&A**Notice of Privacy Practices, HIPAA authorization requirements, inappropriate access**

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

Q We were very familiar with Notice of Privacy Practices (NPP) requirements before the enactment of HITECH. Can you describe any additional requirements that are a result of HITECH?

A Title XIII, the HITECH Act of ARRA, addresses some aspects of privacy but does not replace the HIPAA Privacy Rule.

HITECH does not include any specific NPP requirements. NPPs that meet all HIPAA Privacy Rule requirements are acceptable under HITECH.

HITECH did, however, make significant changes, creating the following:

- Increased penalties
- New breach notification rules
- New rules for restrictions requested by individuals
- New prohibitions on the sale of PHI
- Other rules pertaining to electronic health records (EHR), including accounting of disclosures

Q I've been struggling with HIPAA authorization requirements regarding website postings of patients' healthcare stories. If patients voluntarily post their stories on our Facebook or other social media sites, can we use those stories in other media, such as fundraising brochures, without obtaining specific authorization?

A No. Even though patients sometimes post their stories on an organization's social media website, you should not use these stories for other purposes without the patient's written authorization. Patients

may be willing to share their stories publicly, but they may not want them used for other purposes, such as fundraising.

Q Can I obtain a list of the names of hospital staff members who may have inappropriately accessed my medical records? If all personnel have access to my information, why can't I have access to their names?

A The HIPAA Privacy Rule does not require covered entities (CE) to provide patients an accounting of disclosures for treatment, payment, or healthcare operations.

These are uses for which hospital staff members legitimately access PHI.

However, pursuant to ARRA, CEs that acquire an EHR system after January 1, 2009, must provide an accounting of disclosures for treatment, payment, and healthcare operations by January 1, 2011, or the date on which they acquire an EHR.

CEs that had an EHR in place as of January 1, 2009, have until January 1, 2014, to comply with this requirement.

At this time, many CEs are not required to provide the information you seek. However, if you believe specific individuals inappropriately accessed your medical records, you can file a complaint with the organization's privacy officer. Be prepared to provide the names of the individuals you believe inappropriately accessed your information and why you believe they did so.

Q Posting the surgery schedule has been a recent topic of discussion. Who should receive a copy

of the surgery schedule? Does posting the schedule at nurses' stations as a reference for unit clerks violate HIPAA? Our business office also receives this information, which it requests for workers' compensation issues.

A The minimum necessary standard should govern distribution of the surgery schedule. Specifically, the schedule should be available only to those who need it to perform their jobs, and those staff members should receive only the information they actually need.

Review the current distribution list to determine which individuals or departments receive copies of the schedule. Then contact all of them and inquire why they need the information, what they do with it, and the minimum amount of information they need. You may find that many recipients are receiving the list because they like to know who's having surgery, but don't have a legitimate business need for the information.

Consider creating two versions of the surgery schedule. One version could be the full schedule, including the specific surgical procedures being performed. Surgery staff may need this version for scheduling and room setup; nursing administration may need it to determine staffing ratios.

The second version could omit the specific surgical procedures; staff could use this version in the surgery waiting room to help answer family members' questions and to direct surgeons to the appropriate families for postoperative updates.

Unit clerks and the business office are unlikely to need a copy of the full surgery schedule. Posting the full schedule at nursing stations for anyone to view is unacceptable.

Q Upon receipt of information about a client from another provider of services (such as a

hospital or physician's office), my understanding is that it becomes part of the recipient's record of the individual. May we release information we receive from other providers upon request by a client? I cannot find anything in HIPAA that specifically addresses this issue.

A The HIPAA Privacy Rule does not specifically address redisclosure of health information. However, the American Health Information Management Association (AHIMA) addressed this issue in a 2009 practice brief, *Redisclosure of Patient Information*.

In general, AHIMA recommends that healthcare providers redisclose PHI:

- To other healthcare providers when necessary to ensure the health and safety of a patient.
- To patients when necessary, but only after first encouraging them to obtain the most complete and accurate copies from the originating healthcare provider.
- When necessary to comply with a valid authorization.
- When necessary to comply with a subpoena or court order. In these cases, an organization would redisclose only the information contained within its legal health record.

Note that federal regulations addressing the confidentiality of alcohol and drug abuse patient records generally prohibit redisclosure of health information. Some state laws or regulations may also address redisclosure. ■

Editor's note: Brandt is a nationally recognized expert on patient privacy, information security, and regulatory compliance. Her publications provided some of the basis for HIPAA's privacy regulations.

For more HIPAA compliance-related Q&As, please visit our blog, HIPAA Update, at www.hipaaupdate.com.

Product watch**Backing up your information to move forward**

by Chris Apgar, CISSP

Reliable data backup support can be somewhat elusive because some vendors offer backup support that may not be reliable or affordable. Further, some healthcare organizations have not adopted data backup practices that adequately protect mission-critical data and support fast recovery when data is lost or a disaster occurs.

Mimic Data simplifies the data backup process and significantly shortens recovery time if a server fails, a disaster occurs, or data is corrupted. Mimic Data currently is available wholesale from resellers and from companies that provide outsourced IT support for healthcare organizations. Locating a reseller and evaluating Mimic Data's backup and recovery services is a worthwhile endeavor.

BackSync Backup, one service offered by Mimic Data, is a small but powerful product that backs up everything an organization would expect an enterprise solution (e.g., Microsoft SQL®, Microsoft Exchange®, Microsoft Active Directory®, VMware®, bare metal, and others) to protect, but at a significantly lower cost than other vendors offering backup solutions. BackSync Backup helps healthcare organizations comply with the HIPAA Security Rule and Payment Card Industry requirements. It exceeds National Institute of Standards and Technology (NIST) encryption standards and allows organizations to define retention requirements for live, archived, and deleted data. Also, healthcare organizations can back up data anywhere they choose—locally to a disk or an existing backup server, online, or a combination of locations.

Small medical practices have taken advantage of BackSync Backup and its secure electronic data retention capabilities. Many healthcare organizations use electronic data retention methods that can be unreliable, such as storing data on tapes and external drives located on-site, as part of their data backup process. This can result in

data retention problems related to limited storage space for the backup medium. It can also result in unsecure backup storage, which can lead to difficulty recovering data in the event of a data loss. Some healthcare organizations, for example, store backup tapes on top of the server that has the source data. If a disaster occurs, this arrangement can lead to breach and loss of the backup medium. Additionally, some options for online backup are costly or do not guarantee that backed-up data will be available if data is lost or a disaster occurs. BackSync Backup addresses all of these issues.

Mimic Data's other services, BackSync Protect and BackSync Archive, offer healthcare organizations expanded data backup options. The former is an on-site server that provides a bare-metal backup of an organization's entire server throughout the day. If the organization's server experiences a major hardware failure, BackSync Protect can launch the last backup as a virtual or online server in a very short amount of time, significantly expediting the recovery process. This ensures that the organization can continue to address mission-critical operations with minimal loss of data. The virtual server continues to be backed up until a new server is available or the failed server is repaired. The backed-up data then can be restored to the new or repaired server.

BackSync Archive is a low-cost cloud storage solution that meets HIPAA and NIST requirements. It can accommodate multiple terabytes of an organization's critical data. Healthcare organizations that use BackSync Archive can use industry-standard applications and Internet protocols to back up their data, including secure file transfer protocol and secure Web transmission. BackSync Archive can be configured like a network drive to share files, back up old data that needs to be archived securely, and supplement ongoing data backup by storing another copy of data at a remote location.

Reliable data backup is critical from a business, clinical, and regulatory perspective. Mimic Data

effectively addresses the need for secure backup storage and timely recovery through cost-effective backup solutions that support small to medium-sized organizations. Each of these backup support applications or services can be bundled depending on organizational needs. You can access more information by visiting www.mimicdata.com. ■

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

Best practices

Encryption: Critical for protecting PHI

Healthcare organizations must reconsider their encryption policies, experts say.

If organizations don't encrypt their ePHI, they need to review their practices, said **Dan Steinberg, JD, CIPP/G, PMP**, lead associate at the consulting firm Booz Allen Hamilton, based in Rockville, MD.

Encrypting a message converts it to a form that only the intended recipient can read. It is therefore undecipherable to all but the intended recipient, Steinberg told the audience at the recent 19th National HIPAA Summit in Washington, DC.

Thus, if a staff member leaves a laptop computer on a subway train or a thief steals a desktop computer from an office, the ePHI it contains is protected if it's encrypted.

If Steinberg needed reinforcement for his message, he got it from OCR officials at the HIPAA summit.

"You can learn from the pain of others to do things right," said **Susan McAndrew, JD**, OCR's deputy director for health information privacy.

Encryption is a very simple solution that can help healthcare organizations avoid some of the major causes of large breaches being reported to HHS, McAndrew said. Laptop computers, desktop computers, and portable electronic devices are among the top media types responsible for major breaches, she added.

With encryption, you're faced with the loss of property rather than the loss of data, said McAndrew. You might not be able to prevent thieves from breaking in to offices, homes, or vehicles, but you can encrypt your PHI.

The theft or loss of PHI accounts for two-thirds of all the major breaches involving 500 or more patient records reported to HHS, said **David Holtzman, Esq.**, OCR's health information privacy specialist.

"This is astounding. This is a no-brainer," Holtzman said. "We need to encrypt."

Encryption used for millennia

Cryptography is the science of methodologies for encrypting and decrypting data, Steinberg said. Encryption relies on complex algorithms of numbers, such as the highest known prime numbers and elliptical curves, he explained.

Encryption has been a method for protecting information for millennia, said Steinberg. For example, the "Caesar cipher," in which each letter is shifted forward in the alphabet by a fixed number of letters, is one of the most basic ciphers. A cipher is a secret code used by two parties to communicate.

Encryption mitigates the risk of interception—that an unintended party will receive the information. It accomplishes this by ensuring the information's confidentiality.

Two kinds of cryptography can protect confidentiality; each has advantages and disadvantages, said Steinberg.

The first type is symmetric cryptography, also known as private or shared-secret cryptography. It allows two individuals to share information accessible only to them. Establishing the code requires a secure exchange.

> *continued on p. 8*

Best practices

< continued from p. 7

The second kind of cryptography, asymmetric or public cryptography, is the slower of the two methods. With asymmetric cryptography, one individual has a way of proving his or her identity to another individual. Anyone evaluating a product should probably ensure that it uses one of these algorithms, Steinberg said.

Common symmetric key algorithms include DES, Triple DES, AES, and Blowfish. Common asymmetric key algorithms include RSA, El Gamal, DiffieHellman, and EC-DSA. Common hash functions include MD 1, MD 5, and SHA series.

In simple terms, the biggest difference between symmetric and asymmetric cryptography is whether the sender and receiver have the same or different keys, Steinberg said.

What HIPAA says about encryption

HIPAA does not require healthcare organizations to use encryption.

Instead, it requires covered entities (CE) to consider whether encryption—for data at rest as well as in transit—is reasonable and appropriate in their environment, and to adopt encryption if that is the case, Steinberg said. If encryption is not reasonable or appropriate, CEs—and now business associates (BA) of CEs—must consider the intent of encryption and implement an equivalent control.

If no other control exists that would be reasonable and appropriate, then and only then may CEs or BAs decline to implement encryption—and even then, they must document the rationale, Steinberg said. The accuracy of that determination can be complex.

Encryption is invoked indirectly twice in the HIPAA Security Rule, Steinberg said. 45 *CFR* §164.312(a)(2) (iv) addresses access control and implies the encryption of data at rest. 45 *CFR* §164.312(e)(2)(ii) addresses transmission security and implies encryption of data in motion. A study by the Ponemon Institute reveals that after experiencing a privacy or security breach, 61% of organizations mitigate the problem with encryption, said Steinberg. The Ponemon Institute, based in Traverse City, MI, conducts independent research.

Determine whether encryption is reasonable and appropriate in your environment by considering the elements of an addressable specification, said Steinberg. In particular, consider the following four components:

- **The size, complexity, and capabilities of your organization.** Remember that even smaller organizations have information worth protecting, so this element should not be the only consideration, Steinberg said.
- **Your organization's technical infrastructure, hardware, and software security capabilities.** These

BOH Subscriber Services Coupon				
<input type="checkbox"/> Start my subscription to BOH immediately.				
Options	No. of issues	Cost	Shipping	Total
<input type="checkbox"/> Print & Electronic	12 issues of each	\$349 (BOHPE)	\$24.00	
<input type="checkbox"/> Electronic	12 issues	\$349 (BOHE)	N/A	
Order online at www.hcmarketplace.com . Be sure to enter source code N0001 at checkout!		Sales tax (see tax information below)*		
		Grand total		
For discount bulk rates, call toll-free at 888/209-6554.				
		*Tax Information Please include applicable sales tax. Electronic subscriptions are exempt. States that tax products and shipping and handling: CA, CO, CT, FL, GA, IL, IN, KY, LA, MA, MD, ME, MI, MN, MO, NC, NJ, NM, NV, NY, OH, OK, PA, RI, SC, TN, TX, VA, VT, WA, WI, WV. State that taxes products only: AZ. Please include \$27.00 for shipping to AK, HI, or PR.		
		Your source code: N0001 Name _____ Title _____ Organization _____ Address _____ City _____ State _____ ZIP _____ Phone _____ Fax _____ E-mail address <i>(Required for electronic subscriptions)</i> <input type="checkbox"/> Payment enclosed. <input type="checkbox"/> Please bill me. <input type="checkbox"/> Please bill my organization using PO # _____ <input type="checkbox"/> Charge my: <input type="checkbox"/> AmEx <input type="checkbox"/> MasterCard <input type="checkbox"/> VISA <input type="checkbox"/> Discover Signature <i>(Required for authorization)</i> Card # _____ Expires _____ <i>(Your credit card bill will reflect a charge to HCP Pro, the publisher of BOH.)</i>		
Mail to: HCP Pro, P.O. Box 3049, Peabody, MA 01961-3049 Tel: 800/650-6787 Fax: 800/639-8511 E-mail: customerservice@hcpro.com Web: www.hcmarketplace.com				

factors can be built into the requirements-gathering stages, Steinberg said.

- **The cost of security measures.** Compare the cost of the measures with the cost of a breach and multiply them by the likelihood of such an event. If the cost of the measures is less than the probability multiplied by the cost of mitigation, the measures are very likely worth it.
- **The probability and criticality of potential risks to ePHI.** The probability is always greater than zero, and even seemingly noncritical or nonsensitive PHI may be exploitable, Steinberg said. "I'd put the probability of an eventual security incident, of some type or another, at 100%," he said. The Ponemon Institute estimates the cost of a breach at \$214 per compromised medical record, he noted. "That's a concrete number you can work with."

HITECH's impact

HITECH's breach notification requirements have given encryption new significance, Steinberg said.

HITECH requires CEs to notify affected individuals and BAs to notify CEs upon discovery of a breach of unsecured PHI.

It defines unsecured PHI as PHI not secured through the use of technology or methodology specified by the HHS Secretary in guidance.

A breach notification interim final rule issued by HHS August 24, 2009, provides a safe harbor from breaches when PHI "is rendered unusable, unreadable, or indecipherable to unauthorized individuals." Access the interim final rule at <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>.

HHS also released guidance specifying encryption for data at rest that meets National Institute of Standards and Technology (NIST) Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*. Access this publication by selecting "Special Publications" at csrc.nist.gov.

Data at rest includes data in databases, file systems, flash drives, memory, and other structured storage, Steinberg said.

Both the initial guidance and the interim final rule establish that data in motion must also conform to certain NIST standards to receive the equivalent of a safe harbor.

Data in motion encompasses data moving through a network, including wireless transmission, whether via e-mail or structured electronic interchange.

And don't forget state laws, Steinberg cautioned.

At least 46 states and the District of Columbia have breach notification laws, and not all of them exempt encrypted information. ■

Facing three encryption challenges

Encryption can be a safe harbor that eliminates the need to send data breach notifications, but healthcare organizations still need to be aware of various risks. Organizations should take note of the following concerns associated with encryption, said **Dan Steinberg, JD, CIPP/G, PMP**, lead associate at Booz Allen Hamilton, based in Rockville, MD:

- **Wireless encryption.** Staff members might be using personal devices as a security work-around, which can be difficult to detect, Steinberg said. Individuals need to know the risk this creates, and a covered entity needs to know whether staff members are using personal devices.
- **Mobile devices.** This includes laptop computers, flash drives, telephones, and tablets. Don't forget about

access management and automatic logoffs, along with security awareness and training. Dispose of these devices carefully and ensure that they are wiped clean of any PHI.

- **Encryption of database fields and partial encryption.** HIPAA sets out standards for "de-identification" of records. De-identified records no longer contain information that can be characterized as PHI. However, the remaining data may be used for data mining or breaking the encryption code.

Finally, remember that encryption needs to be part of a larger, robust privacy and security program, said Steinberg.

Use this checklist to ensure compliance

Seven steps to achieve HIPAA security

“There is no such thing as a 100% secure environment. No one can deliver that. What we can try to do is to deliver a resilient enterprise.”

That was the message that **Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)**, brought to his audience at the 19th National HIPAA Summit in Washington, DC.

When it comes to protecting information infrastructure, organizations are under relentless attack, said Pabrai, CEO of ecfirst, a company based in Waukee, IA, that delivers IT services to the healthcare and financial industries.

Constant threats exist, said Pabrai, who specializes in information security and regulatory compliance. An attack on an organizational information infrastructure occurs every 1.5 seconds; that’s 60,000 times per day, he said, quoting statistics from companies such as Trend Micro and IBM.

Every three seconds—20 times per minute—an individual’s identity is compromised, he added. “Now that’s a significant threat.”

Healthcare organizations need to consider these threats as they lay foundations to make their systems more secure and protect the PHI they contain, Pabrai said.

HITECH’s meaningful use incentives include a core objective requiring risk analysis. Therefore, it is all the more important for healthcare organizations to ensure that this activity is not limited to electronic health records, but includes all ePHI that is processed, managed, or transmitted by the entity, he said. This is a big challenge for healthcare organizations.

Organizations must take certain steps to help ensure security and resiliency. “I think it comes down to these seven steps,” Pabrai said. “You can’t skip any of these steps.”

► **Step 1: Assign security responsibility.** It’s required by law, Pabrai said. The HIPAA Security Rule requires covered entities (CE) to appoint a security officer with responsibility for the security of health information.

There’s no reason to hide this individual’s name, said Pabrai. Put him or her on your organizational chart. If a security incident occurs, every member of your workforce needs to know who to contact.

Don’t bury this position in your hierarchy, Pabrai added. A dotted line on your organizational chart should link your security officer directly to a senior executive; ideally, this link should be to the CEO, president, chief financial officer, or chief operating officer. “The buck stops right there,” he said.

The security officer is the individual in your organization who will fight for budget dollars and resources that will facilitate an annual risk analysis to help ensure security. Remember, the attackers are out there, said Pabrai.

► **Step 2: Conduct a risk analysis.** “You’ve got to do it,” Pabrai said. “That’s what’s going to establish the security baseline.”

When was the last time you completed a risk analysis? Ensure that this task is budgeted and that it occurs on a regular basis. Your risk analysis process should include completion of a comprehensive technical vulnerability assessment, he said. This enables you to discover points of vulnerability that can be exploited externally by hackers and internally by individuals with malicious intent, Pabrai said.

► **Step 3: Update your security strategy and policies.** Review your security policies and develop contingency plans, said Pabrai. Your security plan must identify the rules that affect your organization. Updates are necessary to ensure continued compliance with changing rules, such as HITECH, state regulations, and the Red Flags Rule.

Update all necessary documentation—your security system plan, policies, procedures, contingency plan, and disaster recovery plan—as part of this step, he said.

Further, ensure that you develop a system security plan that establishes the security priorities of the

organization and is supported by senior executive management, Pabrai said.

➤ **Step 4: Remediate your weaknesses.** This is your corrective action plan (CAP)—your risk management plan, said Pabrai. You must decide how to correct vulnerabilities and weaknesses identified during the risk analysis process. Use your CAP to establish priorities and budget for improvements.

Implement security controls and deploy encryption for your laptop computers, backups, and removable media, he said.

Pabrai also recommended that organizations consider deploying a single sign-on (SSO) solution, at least for clinicians and the IT department. Further, ensure that biomedical devices are also secured if they store or transmit ePHI.

Many hospitals have implemented strong password requirements to protect ePHI across multiple systems and applications. This can frustrate clinicians who need to access patient information, Pabrai said. The typical clinician working in a hospital today needs to know eight usernames and passwords to access complete information about his or her patients, he said.

On the other hand, he noted, “I see too many organizations with generic accounts” that have common usernames and passwords and that when investigated further do provide access to ePHI. This prevents organizations from tracking an action to an individual user.

The solution is an enterprise SSO, Pabrai said. This allows access control of multiple related, but independent software systems. A user logs in once and gains access to all systems without having to log in to each system separately.

“There is no reason with today’s technology not to budget and implement an enterprise single sign-on to unify user passwords,” said Pabrai. An SSO solution might cost a hospital between \$35 and \$100 per user depending on product features and capabilities, especially integration with some form of strong authentication, such as fingerprint authentication, he said. Organizations should also activate audit capabilities to manage and

track access to ePHI and schedule regular scans of their infrastructures, he said.

➤ **Step 5: Secure your third parties.** “The world is small and getting smaller,” said Pabrai. Organizations may be working with business associates (BA) located across the globe. Pabrai has visited India several times recently and expressed amazement about the number of mushrooming businesses with one target—the United States—and one market segment—healthcare—in mind. These BAs provide services such as coding, billing, transcription, and chart review.

Note that CEs are working with many BAs these days. “Make sure your BA agreements are airtight and your BAs are not the weak link in terms of processing your PHI,” said Pabrai.

➤ **Step 6: Provide training.** Every organization must provide security training and awareness.

“Every member of your workforce must be trained on regulations that impact your organization and the policies of your organization,” said Pabrai. A 10- to 20-minute HIPAA training program done on an annual basis is a waste of everyone’s time, he said. “Better not to do it.”

A vibrant training program that actually ensures employees understand organization policies and the rules they must follow is very important, Pabrai said.

➤ **Step 7: Evaluate your security.** Establish an evaluation process that measures organizational performance during a 12-month cycle, said Pabrai.

Your security strategy must be risk-based, proactive, and integrated, he said. Create a dashboard to grade your compliance.

ecfirst, which runs the HIPAA Academy, uses such a dashboard to assess an organization’s state of compliance. Use HIPAA mandates to grade your organization with respect to policies, training, controls, skills, technical vulnerabilities, executive priority, and data center. Would you rate your organization as good, average, or below average? What would your overall grade be?

Establish goals and a time frame for completion. For example, ecfirst establishes a CAP with items that require completion between 90 and 180 days. ■

Sample HIPAA Policy Review Grid

Old policy number	New policy number	Policy name	Recommendation	Status
100.01	800.04	Facility directory and clergy list opt-out	Archive – Incorporated into 800.04	Scheduled for presentation to policy committee – June 2010
100.02	800.03	Request for amendment to billing Records	Archive – Incorporated into 800.03	Scheduled for presentation to policy committee – June 2010
100.08	800.04	Minimum necessary	Archive – Incorporated into 800.04	Scheduled for presentation to policy committee -- July 2010

Source: Julie Agris, PhD, JD, LLM, CHC, CIPP, CCEP, director of compliance and privacy officer, North Shore-Long Island Jewish Health System (LIJ), Great Neck, NY. Reprinted with permission.



Privacy & Security Primer

**A training tool
for healthcare staff**

June 2011

Tips from this month's issue

Protect your hospital (p. 1)

1. Ensure that your organization has implemented appropriate security and privacy safeguards and best practices.
2. When facing legal risks, make security a priority.
3. Remember, even if OCR does not investigate an organization for an alleged privacy or security breach, patients can still file suit for damages.
4. The OCR draft privacy, security, and enforcement rule is not final, but that doesn't mean OCR won't enforce rules that have been on the books since 2003.
5. Creating a compliance program isn't enough; you must also ensure compliance.
6. When you identify risks in your organization, take corrective action right away.
7. Implement a compliance program before an incident occurs, including a plan for handling all the corrective actions.
8. Spread the cost of the program over several years to make it more manageable.
9. Conduct risk assessments to identify and correct your weaknesses.
10. Understand that documenting risk assessment helps demonstrate HIPAA compliance and effectively addresses patient privacy gaps that might delay or complicate electronic health record implementation and qualification for meaningful use incentives.

11. Breaches can have more ramifications than just fines—including corrective action plans, creation and implementation of revised policies, monitoring by government agencies, and potential harm caused to individuals whose information was breached.
12. Protect electronic health information systems and proceed with caution.
13. Educate hospital leaders, including board members, about the organization's risks.
14. Make your top leaders aware of the consequences of privacy and security breaches.

Encryption best practices (p. 7)

15. Analyze your encryption policies.
16. If organizations don't encrypt their ePHI, they should review their practices.
17. Encrypting a message converts it to a form that only the intended recipient can read. It is therefore undecipherable to all but the intended recipient.
18. Encryption is a very simple solution that can help healthcare organizations avoid some of the major causes of large breaches being reported to HHS.
19. With encryption, you're faced with the loss of property rather than the loss of data.
20. Organizations should consider whether encryption—for data at rest and in transit—is reasonable and appropriate in their environments, and

adopt encryption if that is the case. If encryption is not reasonable or appropriate, covered entities (CE)—and now business associates (BA) of CEs—must consider the intent of encryption and implement an equivalent control that achieves the same result.

21. If no other control exists that would be reasonable and appropriate, then and only then may a CE or BA decline to implement encryption—and even then, the organization must document its rationale for doing so.
22. Know that encryption is invoked indirectly twice in the HIPAA Security Rule. 45 *CFR* §164.312(a)(2)(iv) addresses access control and implies the encryption of data at rest. 45 *CFR* §164.312(e)(2)(ii) addresses transmission security and implies encryption of data in motion.
23. Determine whether encryption is reasonable and appropriate in your environment by considering the elements of an addressable specification.

Consider the following four components:

- The size, complexity, and capabilities of your organization. Remember that even smaller organizations have information worth protecting, so this element should not be the only consideration.
- Your organization’s technical infrastructure, hardware, and software security capabilities. These considerations can be built into the requirements-gathering stages.
- The cost of security measures. Compare the cost of the measures with the cost of a breach and multiply them by the likelihood of such an event. If the cost of the measures is less than the probability of a breach multiplied by the cost of mitigation, the measures are very likely worth it.
- The probability and criticality of potential risks to ePHI. The probability is always greater than zero. ■

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 2011.*