

BRIEFINGS ON

HIPAA

• Privacy • Security • Transactions • Training

New study: Healthcare has long way to go to protect patient privacy

“Patient revenue trumps privacy and risk management,” according to the sponsor of a new study that gives healthcare organizations failing grades for not adequately protecting patients’ PHI.

The Ponemon Institute study indicates that protecting patient data is not a priority in healthcare, says **Rick Kam**, president and cofounder of ID Experts, the Portland, OR, company that sponsored the study.

The November 2010 *Benchmark Study on Patient Privacy and Data Security* highlighted healthcare organizations’ shortcomings that result in data breaches despite stronger safeguards required by the 2009 HITECH Act. You can find a copy of the study at www2.idexpertscorp.com/ponemonstudy.

“Our study found that data breaches remain a frequent occurrence at healthcare organizations—threatening patient privacy and leaving healthcare organizations with a heavy financial burden,” the report concluded.

IN THIS ISSUE

p. 3 Strengthen your HIPAA practices
Because of the Ponemon study, we now know what facilities are thinking when it comes to HIPAA compliance. Here’s what we can do about it.

p. 5 HIPAA Q&A
Our expert weighs in on the questions we’ve received from our readers.

p. 6 HIPAA product watch
This tool can help you comply with HIPAA and HITECH, but you must do your due diligence to ensure that it’s the right one for your facility.

p. 7 Breaches are climbing
The OCR website of breaches of unsecured PHI affecting 500 or more individuals has doubled since July.

Not a priority

Data breaches cost the country’s healthcare system billions of dollars each year. Survey respondents reported an economic impact of slightly more than \$1 million annually to their organizations from data breach incidents, says **Larry Ponemon, PhD**, chair and founder of the Ponemon Institute.

But protecting patient privacy is not a top priority for healthcare or-

ganizations, and that won’t change until the federal government undertakes stricter enforcement practices, says **Chris Apgar, CISSP**, president of Apgar & Associates, LLC, in Portland, OR.

“As one person said at a recent meeting I attended, ‘The board of directors is not looking at spending money on security, they are looking at how much they can make off a new MRI machine,’ ” Apgar says. “Yes, it’s very shortsighted, but it’s not unique to hospitals. It’s true of clinics and other healthcare organizations.

“Providers are way behind when it comes to security of patient information. It’s a combination of ignorance and [the fact that] implementing sound security takes away from and doesn’t add to the bottom line, especially given there is still no real increase in OCR rule enforcement.”

The study details

The Ponemon Institute surveyed 65 healthcare organizations. Although the sample was limited in size, the research was in-depth and included interviews with senior-level staff members to collect information about their organizations’ PHI loss and theft experiences, according to the report. Participating healthcare organizations

“Providers are way behind when it comes to security of patient information.”

—Chris Apgar, CISSP

HCP Pro

Patient privacy

< continued from p. 1

were integrated delivery systems that included networks of organizations with a parent holding company (35%) or part of a healthcare network (46%) and stand-alone hospitals or clinics (17%).

Notably, 71% of participating hospitals said the new HITECH rules have not significantly changed patient record management practices. More than half of respondents (58%) said they have little or no confidence that their organizations have the ability to detect all patient data loss or theft.

Noting the small number of healthcare organizations participating in the study, **Frank Ruelas** cautioned against drawing broad conclusions about all U.S.

hospitals. Ruelas is director of compliance and risk management at Maryvale Hospital in Phoenix and principal of HIPAA College in Casa Grande, AZ.

Examining healthcare organizations that haven't experienced a breach and asking about their practices is an important step, Ruelas says.

A call for change

A major reason for supporting the study was creating a call for action to healthcare organization executives, says Kam.

HIPAA privacy and security officers know what their organizations need to do to protect PHI, he says. However, protecting PHI is not a priority, and organizations aren't providing resources to accomplish it, he adds.

"We need to do a better job is basically the message," Kam says.

The study also revealed that lack of preparation and staffing contributed to breaches of patient data. Healthcare organizations cited:

- Inadequate resources (71%)
- Few, if any, appropriately trained staff (52%)
- Insufficient policies and procedures to prevent and quickly detect patient data loss (69%)

The majority of responding hospitals have fewer than two staff members dedicated to data protection management. Information most at risk due to lack of protection includes patient billing information and medical records, according to the study.

Patients typically are the first to detect a significant number of breaches. This suggests that patient data are unknowingly exposed until patients detect the problem, the study says.

"It basically is an issue of inadequate resources," says Ponemon. "A lot of organizations in our study were frankly frustrated they are not getting the resources they need."

He hopes organizations will use it for internal benchmarking, to compare their own practices to what others are doing to try and protect patient data. ■

Editorial Advisory Board Briefings on HIPAA

HCPPro

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

Sr. Managing Editor: **Dom Nicastro**, dnicastro@hcpro.com

Contributing Editors: **Chris Appgar, CISSP, President**
Appgar & 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

William H. Roach Jr., MS, JD

Partner
McDermott Will & Emery
Chicago, IL

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 781/639-2982. 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.

Seven tips to improve your organization

A recent study by the Ponemon Institute indicates that many healthcare organizations need to pay far more attention to their efforts to secure PHI.

The November 2010 *Benchmark Study on Patient Privacy and Data Security* highlighted healthcare organizations' failings that result in data breaches. So what lessons can healthcare organizations draw from the study?

Consider these seven tips for improvement:

➤ **Focus on creating better security.** "Security is the same as an insurance policy. Will physicians and hospitals discontinue their malpractice insurance coverage to save a buck?" says **Chris Apgar, CISSP**, president of Apgar & Associates, LLC, in Portland, OR.

If you haven't done so already, implement safeguards to protect the data in one very high-risk area: transportable devices, such as laptop computers, says **Frank Ruelas**, director of compliance and risk management at Maryvale Hospital in Phoenix and principal of HIPAA College in Casa Grande, AZ.

A lost or stolen computing device was the No. 2 cause of theft or loss of patient data (41%), topped only by unintentional action (52%). See the chart on p. 4 for other leading causes.

"This report on some level may give cause for these organizations [that have not done so] to rethink their position," says Ruelas.

➤ **Be more proactive and robust with respect to auditing.** Notably, 41% of organizations surveyed discovered a data breach as the result of a patient complaint. "Ouch!" says Ruelas. "Detection seems to be more by accident or by notification by third parties, rather than internal detection methods or alerts."

➤ **Take advantage of the study's results when you need to justify the cost of implementing PHI safeguards.** "Breaches are very expensive, and sound security will significantly reduce the number and cost of breaches," says Apgar.

Hackers who attack your PHI from the outside and employees who can do damage on the inside can cause significant financial damage to healthcare organizations, Apgar says, adding that this damage can occur in various ways:

- Data theft
- Infection of systems with viruses
- Advertent or inadvertent data corruption
- Loss of backup tapes necessary to recover from a disaster or data loss

Ensure that your organization's leaders recognize the serious harm to goodwill, reputation, and community standing that can occur as the result of a data breach, says Ruelas. "Often, a positive reputation of a good corporate citizen developed over years can be flushed down at light speed if a breach occurs," he says.

"A good way to drive business away from the hospital is to breach patients' data. It's called lack of trust," says Apgar.

➤ **Continue to build a good internal track record of trying to do the right thing.** Focus on actions such as training staff, updating policies, and internal impromptu reviews of staff compliance, says Ruelas.

➤ **Learn from other organizations' best practices.** Despite the pessimistic picture the survey paints, "realize that some hospitals are getting it right," says Ruelas. Network with peers and develop a rapport with similar organizations to facilitate the sharing of effective practices. Cultivating relationships can lead to genuine lessons learned, he says.

➤ **Be prepared to respond to data breaches beforehand.** This advice comes from **Rick Kam**, president and cofounder of ID Experts, the Portland, OR, company that sponsored the Ponemon Institute study. The company's focus is data breach solutions.

Notably, 60% of survey respondents experienced more than two data breaches during the previous two years, with an average of 2.4 data breaches.

Healthcare organizations need to have an incident response plan and have tools—such as data loss prevention tools, breach detection capabilities, and firewalls—in place to handle a breach, says Kam. A majority of organizations (63%) said it took between one and six months to resolve data breach incidents.

Don't wait for a breach to happen and be forced to scramble to find organizations or professionals to help

> *continued on p. 4*

Seven tips to improve your organization (cont.)

you, Kam advises. "Find your friends early," he says. For instance, if you need to send out letters notifying patients of a breach or set up a call center to answer patient questions, you should already have a process in place.

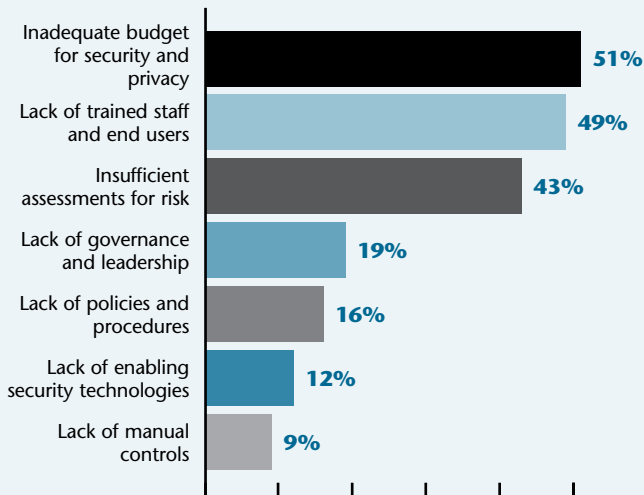
➤ **Conduct a security audit.** There is a growing breach insurance industry, says Kam. These companies

often require healthcare providers to conduct a security audit to help mitigate their risks and get a discount on premiums, he says.

A security audit can help you determine where your organization is most at risk when it comes to data breaches.

The most likely reasons for data breaches

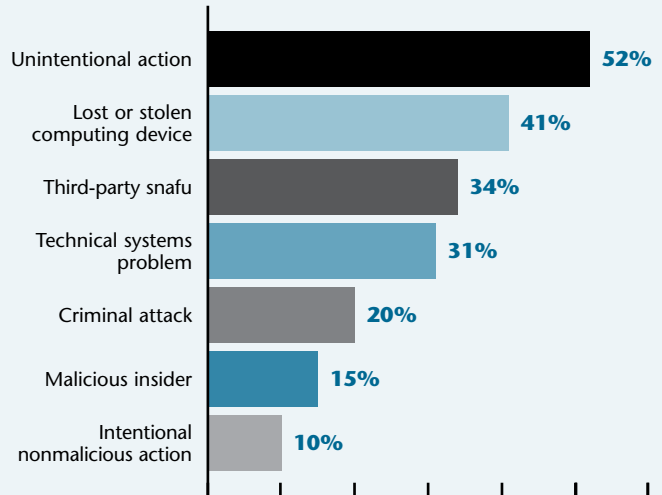
The biggest areas of vulnerability for a data breach to occur:



Source: The Ponemon Institute, Benchmark Study on Patient Privacy and Data Security, November 2010.

The nature or root causes of patient data loss or theft

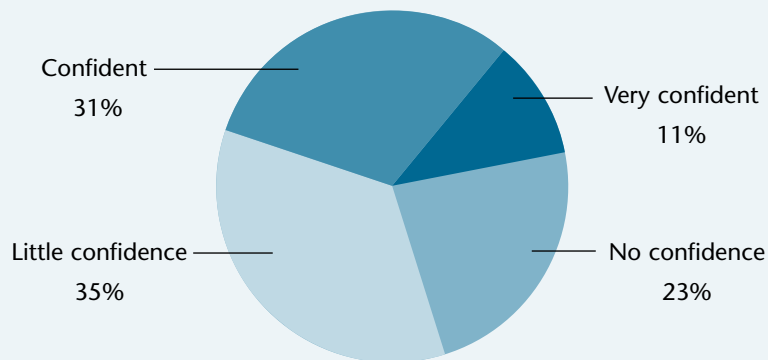
Primary causes of data loss or theft:



Source: The Ponemon Institute, Benchmark Study on Patient Privacy and Data Security, November 2010.

Level of confidence in ability to detect data loss or theft

Level of confidence in an organization's ability to detect all patient data loss or theft:



Source: The Ponemon Institute, Benchmark Study on Patient Privacy and Data Security, November 2010.

HIPAA Q&A**Q&A: Intake and output records; Kaizen events involving the public and inviting them into psychiatric ward**

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

Q Our nursing staff continues to tape patient intake and output sheets outside of patient rooms in our hospital. I have spoken to the director of nursing several times about this situation to no avail. Since only the back side of the form is visible and the forms don't contain patient identification, she believes this is not a HIPAA violation. Also, the nurses put stickers with "high fall risk," "NPO," "NPO for surgery," etc., on the outside of the patient doors. Are these practices acceptable?

A Yes, these practices are acceptable. In the first case, the intake and output records are de-identified since they do not contain patient names or other identification. For a patient in a private room, an observer could certainly assume the form belongs to the patient in the room, but this information does not tell anything about the patient's diagnosis. Stickers with basic information, such as "high fall risk," are also appropriate since they contain the minimum amount of information needed for patient care/safety.

Q During a Kaizen event involving mental healthcare, how can we invite public members of the Kaizen team into the psychiatric emergency and inpatient settings for observation purposes related to the Kaizen?

A Kaizen (Japanese for "improvement") is a philosophy that focuses on continuous improvement of processes. Originally applied to manufacturing and engineering, it has been expanded to healthcare and other industries. A Kaizen event is designed to address a particular issue over the course of a week.

Continuous improvement of processes is important in healthcare, as in other industries, but you must balance the need to involve public members of the team with the patient's right to privacy, particularly in a sensitive area such as psychiatric care.

Some health-care settings adhere to the practice of obtaining written consent from

Stickers with basic information, such as "high fall risk," are also appropriate since they contain the minimum amount of information needed for patient care/safety.

patients for outside observers, but this is not practical in psychiatric emergency and inpatient settings. Instead, you may need to limit actual observation of patients to staff members. Public members of the team could participate in subsequent discussions in which staff describe their observations or even role-play the events they observed. This would allow for broad input into the improvement process without violating patient privacy. ■

Editor's note: Brandt, vice president of HIM at Scott & White Healthcare in Temple, TX, answered these questions. She is a nationally recognized expert on patient privacy, information security, and regulatory compliance, and her publications provided some of the basis for HIPAA's privacy regulations.

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.

Product watch**HITECH Security Advisors offers tool to assess compliance with federal law; providers must analyze their needs first**

by Chris Apgar, CISSP

It appears OCR and state attorneys general will be taking a more serious approach to enforcing HIPAA and HITECH. It's essential that covered entities (CE) and business associates (BA) who haven't begun a security compliance review do so. This is a requirement of the HIPAA Security Rule evaluation standard.

Also, healthcare professionals and hospitals potentially eligible to take advantage of meaningful use stimulus dollars are required to closely examine their security risks as a condition of funding eligibility.

HITECH Security Advisors, LLC, developed a simple but thorough HIPAA/HITECH compliance assessment (evaluation) tool that fits the needs of small to medium-sized organizations. The HIPAA Assessment Toolkit™ is easy to use and addresses the regulatory requirements of the HIPAA Security Rule and new security-related HITECH requirements. It is currently Microsoft® Excel® spreadsheet-based and is expected to move this quarter (first quarter of 2011).

The tool walks users through security compliance requirements; users completing the assessment rank compliance with HIPAA and HITECH security requirements. Compliance is measured as fully compliant, partially compliant, or not compliant. Data collected can be used to develop management reports. Another important use is development of compliance mitigation plans.

This tool addresses security compliance only. A significant advantage of the security assessment tool is it addresses one of the most common and critical compliance failings of CEs and BAs: the generation of required documentation. The assessment tool documents where action is necessary and can help users develop documentation that entities have mitigated compliance violations.

Because the tool addresses security compliance only, it should be used in conjunction with a privacy compliance assessment tool. HIPAA and HITECH privacy requirements for CEs and BAs differ.

The tool includes solid reference information and a crosswalk to the National Institute of Standards and Technology standards. This information is helpful with respect to compliance with various HIPAA Security Rule standards. This is important because a certain level of understanding of security requirements should be mandatory for any security officer.

The assessment tool is cost-effective and easy to use. It has a low price point that fits within the budget of small to medium-sized CEs and BAs. However, it can't accommodate the necessary data collection and analysis required for larger and more complex organizations. The tool addresses federal regulatory security requirements, but it doesn't address state-specific requirements, federal security requirements other than HIPAA and HITECH, or more stringent industry practices.

The tool is not sophisticated enough to fully account for what can be called subsets of the HIPAA Security Rule requirements. Such requirements would include addressing remote access security, encryption of data at rest, multi-factor authentication, and other more stringent or broader requirements that need to be addressed by larger and more complex healthcare organizations.

The tool does not include the level of detail necessary when accounting for differing security practices across a large organization, such as a large healthcare delivery system or health plan. Depending on the organization, differing practices may be appropriate depending on the operational requirements of departments and associated facilities.

This is a simple, cost-effective, and worthy tool for small to medium-sized healthcare organizations interested

in assessing and documenting HIPAA and HITECH security compliance. Taking time for a demonstration before investing in the complete version of this tool is advisable. Healthcare organizations can learn more about the tool at <http://hipaasecurityassessment.com>.

HITECH Security Advisors, LLC, also markets a risk analysis tool and other compliance tools that are separate from the HIPAA Assessment Toolkit. These tools were not evaluated for this month's "Product watch" but are worth checking out. ■

Large patient information breaches double since July 2010

The number of entities reporting breaches of unsecured PHI affecting 500 or more individuals has reached the 200 mark.

As of press time early December, 2010, the number of entities reporting the egregious breaches to the government's HIPAA privacy and security enforcer hit 197.

The number of entities—listed on the OCR breach notification website—has almost doubled since July, when the number hit 107.

In the past five months, 93 new reports have surfaced—an average of 18.6 per month. That's a higher pace than the 15 per month during the first five months after OCR launched the website.

The list is required by HITECH, the American Recovery and Reinvestment Act of 2009 privacy subpart that includes greater breach notification requirements, more public scrutiny, and increased fines for HIPAA privacy and security violations.

The reporting requirement is included in the interim final rule on breach notification, which became effective September 23, 2009, and was still under review as of presstime in December 2010.

Laptops are still the No. 1 location of breach information on the list, accounting for 55 of the 197 reports (27.9%). Other locations in which breaches occurred are paper records (41 reports), desktop computers (32), and portable electronic devices (29).

In addition to filing a report with OCR on breaches affecting 500 or more individuals, the requirements also include:

- Notice to next of kin about breaches involving patients who are deceased

- Notice to patients alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach
- Notice to covered entities (CE) by business associates (BA) when BAs discover that a breach has occurred
- Notice to the secretary of HHS and prominent media outlets about breaches involving more than 500 patient records
- Notices to include what happened, the details of the unsecured PHI that was breached, steps to help mitigate harm to the patient, and the CE's response
- Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecured PHI breaches involving fewer than 500 patient records

The top two breaches with the largest number of affected individuals are:

- **AvMed, Inc., of Florida**
 - Approximate number of individuals affected: 1,220,000
 - Date of breach: December 10, 2009
 - Type of breach: Theft
 - Location of breached information: Laptop
- **Blue Cross Blue Shield of Tennessee**
 - Approximate number of individuals affected: 1,023,209
 - Date of breach: October 2, 2009
 - Type of breach: Theft
 - Location of breached information: Hard drives ■

Social media: Balance the benefits and risks

Social media and networking have created a dilemma for many healthcare organizations: They carry both benefits and risks.

But with people increasingly using social media websites—blogs and social networking sites such as Facebook, Twitter™, and YouTube—for business and personal communications, healthcare organizations can't bury their heads in the sand.

"Any organization that's communicating with the public needs to address social media. It's not something you can ignore. It needs to be part of your strategy going forward," explained **Phyllis Patrick, MBA, FACHE, CHC**.

Patrick and her business partner, **Angel Hoffman, RN, MSN**, cofounders and managing directors of the AP Health Care Compliance Group, which has offices in Pittsburgh and Purchase, NY, spoke about the use of social media at the HIPAA Summit West October 5, 2010, in San Francisco.

A search for balance

Social media is now the No. 1 use of the Internet, author Bill Tancer, general manager of global research at Hitwise, an Internet tracking company, wrote in his book, *Click: What Millions of People Are Doing Online and Why It Matters*.

However, healthcare organizations must balance the rewards of social media with the need to keep medical information confidential, said Hoffman. Healthcare organizations worry about patients' PHI or pictures being posted on the Internet or staff members blogging about patients they cared for, she said.

On the other hand, there are corporate benefits from social media. Organizations are using it for marketing, including advertising, patient relations, and connecting with consumers. There are also human resources uses, such as recruiting new employees and even conducting informal background checks on job candidates by checking sources like Facebook, Hoffman said.

Organizations need to consider the risks of using social media, establish policies, educate staff, and have sanctions in place for violations, Hoffman said. Your employees need to know what is acceptable behavior, and you should write that right into your code of conduct, she said.

Risk scenarios to consider

Organizations should think about several risk scenarios and security issues as they formulate an approach and policies regarding social media, said Patrick. Consider the following:

- E-prescribing
- Patient portals, including direct portals
- Communications with providers
- Provider portals
- Alerts to providers
- Alerts to patients
- Consultation/referral services
- Results delivery, such as from tests or imaging
- Partners/vendors without HIPAA responsibilities
- Public health surveillance systems
- Syndromic surveillance systems
- Public health emergencies
- Bioterrorism events
- Patient consent issues

You should consider each one of these types of communication to be exchanges of health information as you put together your policy and ensure the security of data and resources when it comes to social media, said Patrick.

"Social media should appear on your risk matrix when you do a risk assessment," she said.

Patrick advised organizations to do a reality check in terms of what is happening with social media. Forbidding employees from accessing social network sites may not be the answer. It isn't enough for organizations to say, "This won't happen if we forbid it." That is not going to work—it is happening," she said.

When it comes to restricting or enabling social media use, “I would say you should be looking at ways to enable it,” Patrick said.

In devising a security strategy that fits your use of social media, organizations should keep in mind that growing research, such as that by the 1105 Government Information Group, suggests that many security vulnerabilities are not the result of failures of technology, but failures of human resources and leadership, Patrick said.

Some experts are advising that organizations adopt two policies—one that addresses expectations and boundaries for workforce members, and a second addressing operational guidelines for social media workers and others, such as those in marketing, said Patrick.

For an example of a social media policy, check out the one available on the Vanderbilt University Medical Center website, Patrick said. You can find the policy at <http://tinyurl.com/2w3w7nq>. ■

Social media best practices checklist

When approaching the topic of social media use, there are some important questions healthcare organizations need to answer, said **Phyllis Patrick, MBA, FACHE, CHC**. Patrick and her business partner **Angel Hoffman, RN, MSN**, co-founders of the AP Health Care Compliance Group, put together the following checklist:

- Is your primary interest restricting or enabling the use of social media?
 - Does your organization view social media as a highly effective information gateway?
 - Have you asked your workforce how the organization can take advantage of the benefits of social media and avoid the pitfalls?
 - Have you developed a strong business case for social media use, supported at the appropriate level for each department/functional area, considering the organization’s mission, vision, and values; possible threats; technical capabilities; and potential benefits?
 - Does your IT staff understand that the goal should not be to say “no” to social media, but to follow good security guidance, with effective and appropriate security and privacy controls?
 - Does your organization have a policy addressing social media?
 - Does the policy reflect the viewpoints and needs of various stakeholders (e.g., patient care, research, education)?
 - How does the policy support the mission, vision, and values of your organization?
- How does the policy affect your relationship with business partners and vendors/contractors?
 - How do you conduct training on the appropriate use of social media (on- and off-site)? Are you including appropriate use of social media in your overall security and privacy awareness training program?
 - How will you capture social media traffic and audit, analyze, and use it for security and privacy investigations, as appropriate?
 - Have you reviewed the Financial Industry Regulatory Authority’s (FINRA) Regulatory Notice 10-06, *Guidance on Blogs and Social Networking Web Sites*, to determine its applicability to your organization and how you might use its recommendations to strengthen your organization’s social media program? (**Note:** FINRA provides guidance on the responsibilities of companies to supervise the use of social networking sites. You can find the guidance at <http://tinyurl.com/yexukyv>.)
 - How does your organization plan to use social media to generate new strategies, engage, and learn?

Questions? Comments? Ideas?

Contact Sr. Managing Editor
Dom Nicastro

Telephone 781/639-1872, Ext. 3413

E-mail dnicastro@hcpro.com

Sample policy

The Vanderbilt University Medical Center's social media policy

Editor's note: Consider adapting these policy and procedure guidelines to fit your organization's needs.

Social media policy and guidelines

I. Outcome goal

To provide guidelines outlining how Vanderbilt University Medical Center (VUMC) supports institutional communication goals.

II. Policy

VUMC offers support of institutional communication goals and provides social computing guidelines for VUMC faculty, staff, and students engaging in online discourse and identifying themselves with VUMC.

This policy is not intended for Internet activities that do not associate or identify a faculty or staff member with VUMC, do not use Vanderbilt e-mail addresses, do not discuss VUMC, and are purely about personal matters.

III. Definitions

Content owners, for the purpose of this policy, are those assigned the responsibility of maintaining, monitoring, and moderating a VUMC social media platform. Official communications refer to those done in VUMC's name (e.g., a Vanderbilt Heart Facebook page).

A. Content owner: Assigned by department as the individual responsible for monitoring and maintaining Web content.

B. Moderator: Assigned by content owner and/or department as the individual responsible for moderating comments and postings by internal and external users, including deleting comments and postings that do not meet the criteria set forth in this policy.

C. Social media platforms: Technology tools and online spaces for integrating and sharing user-generated content in order to engage constituencies in conversations and allow them to participate in content and community creation. Examples are Facebook, Twitter™, LinkedIn, and YouTube.

IV. Specific information

A. Official institutional Web 2.0 communications

1. Because of the emerging nature of social media platforms, these guidelines do not attempt to name every current and emerging platform. Rather, they apply to those cited and any other online platform available and emerging including social networking sites and sites with user-generated content. Examples include but are not limited to:
 - a. YouTube
 - b. Facebook
 - c. iTunes
 - d. LinkedIn
 - e. Twitter
 - f. Blogs
 - g. Social media content that is hosted internally and protected by VUNet ID/password

Source: Vanderbilt University Medical Center. Reprinted with permission. For the full form, go to <http://tinyurl.com/2w3w7nq>.

Briefings on HIPAA 2010 index

Breaches

- Are there other risks you need to worry about? Stolen camera creates privacy breach for Arkansas hospital. Dec., p. 5.
- Beware: Laptop computers create a major risk. June, p. 1.
- Case involving breaches of PHI worth watching. April, p. 11.
- Cost of healthcare security; Report: Breaches on OCR website add up to nearly \$1 billion for entities. Oct., p. 1.
- Follow HITECH and state notification requirements. Oct., p. 11.
- Hospital: Former employee had access to current system. June, p. 6.
- Learn from other healthcare organizations' mistakes: Review the top breaches of 2009 and how you can prevent the same at your facility. Feb., p. 3.
- Lesson learned: Protect PHI when staff member leaves. June, p. 7.
- Prepare to respond to breaches of privacy. Dec., p. 1.
- Prepare your organization to respond appropriately if a breach of unsecured PHI occurs. July, p. 6.
- Theft or loss of paper records, desktop computers put organizations at risk. Aug., p. 1.
- When is it a PHI breach or an internal incident? Oct., p. 7.

Business associates

- Ensure that your business associates comply with HITECH security and privacy. March, p. 1.
- HIPAA proposed rule extends compliance to BA subcontractors; BAs liable for subcontractor breaches. Aug., p. 7.
- HITECH compliance deadline one month away. Jan., p. 4.

Case studies

- Cascade official shares lessons learned from CMS HIPAA security audit. April, p. 1.
- Safeguard portable devices with education, policies: Create a training guide for your employees. July, p. 1.

Compliance tips

- Getting it all done when you're a solo act. Sept., p. 1.
- HITECH, major settlements, EHRs, and more: Looking back on 2009, ahead to 2010. Jan., p. 1.
- New regional privacy advisors provide guidance and education for covered entities and business associates. March, p. 4.
- OCR flags copier vulnerabilities, laptop computers. Dec., p. 11.
- Ten tips for training your workforce to be HIPAA ready. Nov., p. 4.
- Use these cost-effective ways to ensure compliance. May, p. 1.

HIPAA Q&As

- Business associate requirements, audit log retention periods, and more. Feb., p. 6.
- Business associates are still business associates; HITECH includes new criminal penalties. Sept., p. 8.
- Census disclosures may violate HIPAA; consider sign-in sheet alternatives in waiting area. June, p. 9.
- Clipboard permissible but not best sign-in option. May, p. 5.
- Compliance with cameras in rooms; requesting donor information; access to records and legalities. Oct., p. 9.
- Give media limited patient information; HITECH protects paper PHI in addition to electronic information. April, p. 8.
- Insurance company requests, privacy practice acknowledgments, and breach notification. Dec., p. 9.
- Physicians, managed care, risk assessments, and more. Jan., p. 10.
- Posting resident names and pictures, disclosing minors' PHI to parents, and unencrypted e-mails. Nov., p. 8.
- Review patient authorization before responding to attorneys; state law sometimes preempts HIPAA. July, p. 9.
- Terminate contract if vendor denies records request; patient also can be liable for lost records. March, p. 7.

> *continued on p. 12*

2010 index

< continued from p. 11

HITECH Act

- Accounting for disclosures from EHRs: What you need to know to comply with HITECH requirements. Sept., p. 11.
- Adapt HIPAA internal sanctions policy to comply with HITECH; consider penalty tiers for violations. March, p. 10.
- De-identification standard moves to forefront at OCR. May, p. 7.
- A final checklist to help meet the HITECH deadline. Feb., p. 1.
- HCPPro survey: Breach notification requirements are top HITECH challenge; BA contracts also a concern. May, p. 10.
- HITECH creates new privacy challenges for healthcare organizations; individuals gain stronger rights. Aug., p. 4.
- Waiting for the final rule? Here's a checklist to prepare. Sept., p. 4.

Medical identity theft

- FTC delays Red Flags Rule enforcement to December 31. July, p. 12.
- Proactive training: Educate staff members, patients in fight against medical identity theft at your facility. Feb., p. 9.

Product watch

- Consider Axway solutions to help secure PHI. July, p. 11.
- Consider SenditCertified to help ensure secure PHI transmissions. Feb., p. 8.
- Look at the fine print to ensure protection backup services; watch for HIPAA-compliant promises. Nov., p. 10.
- Pre-test security application compatibility, effectiveness before purchase; HIPAA compliance at stake: Kaspersky Mobile Security 7. May, p. 9.
- SunGard strong in disaster recovery planning. Sept., p. 9.
- Take a secure trip to Aruba's wireless solution. March, p. 6.

Security

- CMS offers five solutions to help address inadequate HIPAA Security Rule–required policies and procedures. Nov., p. 11.
- Failure to conduct risk assessment is risky business. April, p. 6.
- Use this checklist to help evaluate your organization: How does your information security program stack up? Aug., p. 9.

Social networking

- Assess privacy vulnerabilities for social networking sites. Jan., p. 7.
- Get 'social'—but address privacy concerns. Nov., p. 1. ■

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 (Required for electronic subscriptions) <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 (Required for authorization) Card # _____ Expires _____ (Your credit card bill will reflect a charge to HCPPro, the publisher of BOH.)				
Mail to: HCPPro, 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				

Privacy & Security Primer

**A training tool
for healthcare staff**

January 2011

Tips from this month's issue

Ponemon study (p. 1)

1. Focus on creating better security.
2. Implement safeguards to protect the data in one very high-risk area: transportable devices, such as laptop computers.
3. Recognize that a lost or stolen computing device was the No. 2 cause of theft or loss of patient data (41%), topped only by unintentional action (52%) in the November 2010 Ponemon study.
4. Organizations should rethink their position on their security practices if they haven't already done so.
5. Be more proactive and robust with respect to auditing; 41% of organizations surveyed discovered a data breach as the result of a patient complaint.
6. Take advantage of the study's results when you need to justify the cost of implementing PHI safeguards.
7. Realize that hackers who attack your PHI from the outside and employees who can do damage on the inside can cause significant financial damage to your healthcare organization. Damage can occur in various ways:
 - Data theft
 - Infection of systems with viruses
 - Advertent or inadvertent data corruption
 - Loss of backup tapes necessary to recover from a disaster or data loss
8. Ensure that your organization's leaders recognize the serious harm to goodwill, reputation, and community standing that can occur as the result of a data breach.
9. Continue to build a good internal track record of trying to do the right thing. Focus on actions such as training staff, updating policies, and internal impromptu reviews of staff compliance.
10. Learn from other organizations' best practices.
11. Network with peers and develop a rapport with similar organizations to facilitate the sharing of effective practices. Cultivating relationships can lead to genuine lessons learned.
12. Be prepared to respond to data breaches beforehand; 60% of survey respondents experienced more than two data breaches during the previous two years, with an average of 2.4 data breaches.
13. Healthcare organizations need to have an incident response plan and have tools—such as data loss prevention tools, breach detection capabilities, and firewalls—in place to handle a breach.
14. Don't wait for a breach to happen and be forced to scramble to find organizations or professionals to help you.
15. If you need to send out letters notifying patients of a breach or set up a call center to answer patient questions, you should already have a process in place.
16. Conduct a security audit. Breach insurance companies often require healthcare providers to

conduct a security audit to help mitigate their risks and get a discount on premiums.

17. A security audit can help you determine where your organization is most at risk when it comes to data breaches.

Social media (p. 8)

18. Ask these questions when it comes to creating a social media outlet for your facility:

- Is your primary interest restricting or enabling the use of social media?
 - Does your organization view social media as a highly effective information gateway?
 - Have you asked your workforce how the organization can take advantage of the benefits of social media and avoid the pitfalls?
 - Have you developed a strong business case for social media use, supported at the appropriate level for each department/functional area, considering the organization's mission, vision, and values; possible threats; technical capabilities; and potential benefits?
 - Does your IT staff understand that the goal should not be to say "no" to social media, but to follow good security guidance, with effective and appropriate security and privacy controls?
 - Does your organization have a policy addressing social media?
- Does the policy reflect the viewpoints and needs of various stakeholders (e.g. patient care, research, education)?
 - How does the policy support the mission, vision, and values of your organization?
 - How does the policy affect your relationship with your business partners and vendors/contractors?
 - How do you conduct training on the appropriate use of social media (on- and off-site)? Are you including appropriate use of social media in your overall security and privacy awareness training program?
 - How will you capture social media traffic and audit, analyze, and use it for security and privacy investigations, as appropriate?
 - Have you reviewed the Financial Industry Regulatory Authority's (FINRA) Regulatory Notice 10-06, Guidance on Blogs and Social Networking Web Sites, to determine its applicability to your organization and how you might use its recommendations to strengthen your social media program? (**Note:** FINRA provides guidance on the responsibilities of companies to supervise the use of social networking sites. You can find the guidance at <http://tinyurl.com/yexukyvv>.)
 - How does your organization plan to use social media to generate new strategies, engage, and learn? ■

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 2011.*