

PATIENT PRIVACY

Practical News and Strategies for Complying With HIPAA

Contents

- 3** Stakeholders to OCR: Accounting for Disclosures Will Be a Mess
- 4** OCR: Follow the NIST Standards When Conducting a Risk Analysis
- 6** Beyond PHI or ePHI: Personally Identifiable Information
- 7** UCLA Researcher Gets Jail Time For Viewing PHI With No Financial Motive
- 10** Is Privacy Compliance Increasing? The Signs Are Unclear
- 11** Patient Privacy Court Cases
- 12** Privacy Briefs

Many narrative sections at www.AISHIPAA.com have now been updated to reflect new requirements contained in the HITECH Act, including a recently revised chapter on Business Associates and a brand-new section on Security Breach Notification. If you don't have a website password, call 800-521-4323 or e-mail customerserv@aispub.com. Please whitelist aishipaa@aispub.com to ensure e-mail delivery.

Editor

Liana Heitin
lheitin@aispub.com

Contributing Editor

Nina Youngstrom

Executive Editor

Jill Brown

To Boost Employee Compliance, Asking 'Why' and Understanding Violators Are Key

As any HIPAA compliance officer will admit, the biggest headache is often getting workforce members to do the right thing.

Frank Ruelas, director of compliance and risk management at Maryvale Hospital in Phoenix and a HIPAA consultant, knows his toughest task is making sure employees *follow* the policies and procedures that are put in place to protect the privacy and security of patients.

But after more than a decade in the field, Ruelas has developed a number of strategies that can boost compliance. To help do the job, he has borrowed ideas from other industries and aspects of health care, such as a "root cause analysis," which employs a series of "why" questions when things go wrong.

Placing himself somewhat apart from what he calls "process experts," Ruelas says he's a bit of a maverick because he thinks some of his colleagues place too much blame on processes and procedures. As a result, individual accountability gets short shrift, he says.

"Over the years, I have constantly seen excuses, and never do people say, 'You knew the policy!' I find it very rare that somebody didn't know the policy, and most policies reflect general practices that have developed over the years — and common sense," he says.

continued on p. 8

New Accounting for Disclosures Provision Stirs Up Old Controversy and New Concerns

Words like "unnecessary," "impossible" and "ridiculous" litter the pages of the more than 100 publicly posted responses to OCR's Request for Information (RFI) on the new accounting for disclosures requirements.

Covered entities (CEs) submitted comments that were nearly unanimous in their negativity about the provision, which expands individuals' rights to view disclosures of their PHI (see p. 3). The new provision requires CEs to log even routine disclosures made for treatment, payment and health care operations (TPO) — something covered entities have never had to do.

Many CEs contend that the current HIPAA requirements are sufficient and that very few individuals have ever asked for an accounting. However, one patient privacy advocacy group claims the expanded rights are a "key, critical" consumer privacy protection and that the technology is already in place. OCR says the CE backlash is not surprising but that the office does not have the authority to modify the rulemaking.

Accounting for disclosures has received pushback since the beginning. The HIPAA privacy rule, which became effective in 2003, gave individuals the right to view a list of incidents in which a covered entity disclosed their PHI. The rule did not require the CE to list disclosures for TPO. Covered entities claimed the accounting was both a burden on already busy employees and an unnecessary requirement because patients rarely ask to see the log.

continued

Now, CEs have even more fodder for complaint. Under the HITECH Act, HHS is charged with revising the privacy rule to allow patients to view disclosures made through a CE's electronic health record system — including those made for TPO (*RPP* 5/09, p. 1).

In formulating its new regulations, the HITECH Act requires OCR to take into account “the interest of individuals in learning the circumstances under which their protected health information is being disclosed” and “the administrative burden for accounting for such disclosures.” Accordingly, OCR issued its RFI in the May 3 *Federal Register* and now tells *RPP* it is “trying to issue a proposed rule on accounting of disclosures expeditiously.”

The RFI asked covered entities, individuals, consumer advocates and EHR vendors to answer the following questions, among others:

- ◆ What are the benefits to the individual of an accounting of disclosures, particularly those made for TPO?
- ◆ Are individuals aware of their current right to receive an accounting?

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Copyright © 2010 by Atlantic Information Services, Inc. All rights reserved. No part of this publication may be reproduced or transmitted by any means, electronic or mechanical, including photocopy, FAX or electronic delivery without the prior written permission of the publisher.

Report on Patient Privacy is published with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Editor, Liana Heitin; Contributing Editor, Nina Youngstrom; Executive Editor, Jill Brown; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Gwen Arnold; Production Coordinator, Russell Roberts

Call Liana Heitin at 800-521-4323 with story ideas for *RPP*.

Subscribers to **Report on Patient Privacy** also receive access to **AIS's HIPAA Compliance Center** at www.AISHIPAA.com, with archives of past issues of the newsletter, links to government documents, and 30 searchable narratives written by experts in privacy and security compliance. Subscribers receive e-mail notification when a new issue of **Report on Patient Privacy** is posted on the Web site. Please whitelist aishipaa@aispub.com to ensure e-mail delivery.

To order **Report on Patient Privacy**:

- (1) Call 800-521-4323 (major credit cards accepted), or
- (2) Order online at www.AISHealth.com, or
- (3) Staple your business card to this form and mail it to:
 AIS, 1100 17th St., NW, Suite 300, Wash., DC 20036.
 Payment Enclosed* \$429
 Bill Me \$404

*Make checks payable to Atlantic Information Services, Inc. D.C. residents add 6% sales tax.

◆ How many requests for an accounting have you received from individuals?

◆ Is your EHR system capable of distinguishing between “uses” and “disclosures?”

◆ How much time will it take to update your EHR system to comply?

Cindy Nixon, director of medical records and HIPAA privacy officer for the Cookeville Regional Medical Center in Tennessee, says, “It looks like OCR knew this was going to be an issue the way they phrased the questions.” When asked if the office was surprised by the overwhelmingly negative responses, OCR says it “has received anecdotal information in the past from covered entities about the burden of the current accounting for disclosures provisions, and expected this rulemaking to generate significant interest.”

Provision Has Three Big Problems

There are three major problems with the provision, says Nixon. First, it is too burdensome for a facility to document the exact reason for a disclosure, beyond merely stating T, P or O. Also, most EHR systems cannot distinguish between a “use” and a “disclosure” on an audit trail. Lastly, providing a patient with an audit trail is not meaningful — the patient is unable to tell from the documentation whether the disclosure was legitimate or inappropriate.

Comments posted by other stakeholders reflect many of these same ideas. Pamela McNutt, senior vice president and CIO for Methodist Health System in Dallas, Texas, writes, “It is difficult to imagine a report that could be produced to show the hundreds of touches a patient’s PHI has in the course of [TPO] that would be meaningful or useful.”

She says that EHR systems are not equipped to comply with the requirements. “It is going to be impossible to automate the ‘reason why’ an access or disclosure occurred,” says McNutt.

“To ask all docs to put in a reason every time they look at a chart — that would drive everyone to insanity,” Nixon tells *RPP*. Some physicians are already so encumbered by new regulations coming out that they are quitting or retiring early, she says.

One voice of dissent is Patient Privacy Rights (PPR), a nonprofit health privacy watchdog. Founder and chair Deborah Peel, M.D., in her response to the RFI, says the limitations of current health information technology (HIT) systems are minimal. “Authentication of all users of EHRs and HIT systems is required, so every employee access to every record or piece of PHI is already logged. The login process could be updated to require specific purpose or use, whether

it was a 'use' or 'disclosure,'" Peel writes. And since initially authenticating users requires categorizing their roles in the hospital, generating details on users "automatically would not be a complex or expensive update," she contends.

But McNutt says that people are more inclined to ask about individual disclosures than for a complete log. "The requests we receive are usually very specific," she writes. "Did Doctor X get my charts? Did my neighbor who works at your hospital view my record and why?"

continued

Stakeholders to OCR: Accounting for Disclosures Will Be a Mess

Here is a sampling of comments submitted in response to CMS's May 3 Request for Information on new accounting for disclosures provisions. The complete set of comments can be accessed at www.regulations.gov.

"No one has ever asked [for an accounting], and we cannot appreciate any perceived value to the patient of such disclosures."

— Robert Burney, M.D., privacy officer for the Office of Medical Services, U.S. Department of State

"The 2011 timeline would be very aggressive for electronic health record systems to start reporting on accounting for disclosures."

— Richard A. Mahoney, president of MedPlus and vice president of Healthcare Information Solutions for Quest Diagnostics Incorporated

"Our vendor's audits take 13 hours or longer for one patient's visit. Under this architecture a three-year query could literally take days to sort through the billion[s], if not trillions, [of] detailed audit entries."

— Pamela McNutt, senior vice president and CIO for Methodist Health System in Dallas, Texas

"In the majority of systems that currently fit the definition of EHR, access logs are retained for 90 days. Data storage costs would increase exponentially to retain the information for three years."

— CHRISTUS Health, Irving, Texas

"As a basic measure, PBMs transact 4 to 5 billion prescriptions a year. If such a requirement were to apply, the effect would be an overwhelming administrative burden requiring substantial resources and time. This would involve re-architecture of existing systems and practices, not just software patches."

— Greg Johnson, assistant vice president, federal and regulatory affairs, Pharmaceutical Care Management Association, Washington, D.C.

"We believe ...the average consumer is not familiar with the many permissible disclosures that fall under 'operation' and how many people touch their PHI. Accessing their disclosures for TPO will lead to more questions by the consumer. We will spend a great deal of time explaining these permissible disclosures to the patient, yet the information they obtain in the accounting or from us by way of disclosure will not fully satisfy their real concerns."

— Gina L. Bertolini, assistant general counsel on behalf of The University of North Carolina Health Care System

"I believe that there is a common misconception that most providers operate a single monolithic electronic health records system. And, to comply with HIPAA and the HITECH privacy provisions, the provider simply needs to do some minor programming or push a button. This is generally not the case... This electronic health record environment is extremely complex."

— John Houston, vice president of information security and privacy, University of Pittsburgh Medical Center

"Any level of accounting for treatment, payment and operations portends to be very resource intensive and would also be confusing and concerning to many patients without a tangible benefit... Patient care and other staff are already strained and to accurately accomplish an accounting of disclosures encompassing [TPO] will require significant additional resources for no known patient benefit."

— Lois Dahl, privacy official, Fairview Health Services, Minneapolis, Minn.

"It would be far better to leave it to the courts to determine if, and when, any particular health care organization might be required to make an accounting of its practices associated with its health care operations, all of which practices will ordinarily be of no interest, or benefit, to individual patients... The Department should conduct site visits of health care organizations of various types and sizes... to obtain first hand knowledge of the complexity involved with complying with the proposed regulations."

— Scott Petersen, HIPAA privacy consultant, Multi-Care Health System, Tacoma, Wash.

"The return on investment across the healthcare system appears small. There is little or no real data that quantifies the real/perceived value to the patient of the [accounting of disclosures] that includes disclosures for TPO."

— Healthcare Information Management and Systems Society (HIMSS), Chicago

Many responders also call the provision redundant. Lori Straus, chief corporate compliance and privacy officer for the University of Virginia Health System, writes that patients are informed through the Notice of Privacy Practices that their records may be disclosed to insurers for payment and to business associates for routine health care operations. And, she writes, patients know when a provider receives a record for treatment purposes because they are receiving the treatment.

Few Patients Ever Request Accounting

Most of the responders claim to have received fewer than 10 requests for accounting under HIPAA. Many cited their number of requests in the last seven years as zero.

PPR has not been contacted by any individuals who received an accounting of disclosures under HIPAA, says Peel. However, "since the vast majority of disclosures fall under TPO," the previous non-TPO accounting would be unlikely to "reveal anything meaningful to the individual," she says.

To be beneficial, an accounting for disclosures must "include critical details such as 'who' (i.e., which actual person(s)) actually receive, use, or disclose PHI and the specific purpose or reason for each use or disclosure," claims Peel. She advocates for detailed reporting, stating that "'health care operations' is far too broad a category of use to be transparent or comprehensible to individuals."

Straus argues that under the requirement "health care providers will have to spend large sums to create new or adapt existing systems and interfaces, and devote considerable staffing hours to manual entry of information. These resources, in a time of budget scarcity, would be expended to satisfy only a handful of requests each year, for information that generally is already known to the patient or is so routine and generic as not to be of much benefit."

OCR Is in a Bind

Peel agrees that the survey is leading and says "OCR is asking the wrong questions." Rather than asking how much of a burden the accounting would be, she says, OCR should query organizations on how quickly they can update their information systems to comply.

Whatever OCR's intent in writing the survey, the office will need to draft the rule. "This rulemaking is pursuant to a statutory provision, and OCR does not have the authority to modify the requirements," says OCR.

Dan Rode, vice president of policy and government relations for the American Health Information Management Association (AHIMA), says OCR is in a bind but may have a few options. First, OCR could "go back to Congress with the feedback they're getting out of this RFI...and maybe ask for a modification." Perhaps the

modification would be the creation of a standard code system for recording reasons for accessing an EHR. Another alternative, Rode says, is to move forward with the requirements as they stand and "let the HIPAA entities complain to Congress." Or, he says, OCR could develop a report on the RFI and leave it up to the provider community to mobilize and solve the problem.

OCR does "recognize the burden is quite high," says Rode. "The burden could be high enough to keep some organizations from going forward and getting EHRs. It has the potential to become a barrier to the process."

Responses to the RFI were due on May 18 and are available at www.regulations.gov.

Contact Nixon at (931) 783-2626, Rode through Theresa Grant at theresa.grant@AHIMA.org and Peel through Katherine Johnson at kjohnson@patientprivacy-rights.org. ♦

OCR: Follow the NIST Standards When Conducting a Risk Analysis

HIPAA covered entities (CEs) and business associates (BAs) should be following the recommendations for risk assessments included in guidelines issued by the National Institutes of Standards and Technology (NIST) that typically only apply to federal agencies, according to draft guidance issued on May 10 by the HHS Office for Civil Rights (OCR).

Beyond clarifying specifics, the draft guidance also telegraphs to CEs and BAs that the agency "is taking a more aggressive approach in carrying out its responsibilities under HITECH," says John Parmigiani, a HIPAA security consultant who helped draft the security rule. The draft is a "heads up," he says, that OCR expects risk assessments to happen.

"While the principles discussed in the document should not come as a revelation...[CEs have] not always diligently practiced them," he notes. "The OCR guidance is a quick way of stating compliance expectations and dispelling any 'ignorance of the law' defenses when an organization is not in compliance with federal regulations and industry best practices."

Risk assessments are required under the security rule at section 164.308, which states: "*Risk analysis* (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

What has changed since the security rule came out five years ago, however, is that business associates, by virtue of last year's HITECH Act, are also required to conduct risk assessments. Because this is a new require-

ment for BAs, they may need more assistance in conducting a risk assessment.

Perhaps with this in mind, OCR chose risk assessments as the topic for its first-ever “annual update” on portions of HIPAA, a new task of its own granted by the HITECH Act. OCR, however, stamped the guidance “draft” when it appeared on the agency’s website May 10. It is accepting comments on the document until June 18.

The draft guidance also serves as a strong push to get on the ball to those CEs, especially smaller ones such as physician practices, that never got around to doing a risk assessment in the first place.

And to those that did, the draft guidance drives home the message that once is not enough, and helpfully spells out the circumstances that should trigger a new risk assessment, says Sarah Coyne, a partner and national chair of the health law group of Quarles & Brady LLP in Madison, Wisc.

Risk Assessments Are ‘Foundational’

OCR’s draft guidance seems to imply that at least some CEs and BAs are not at a high enough level of compliance or understanding for anything beyond assistance with basic activities such as a risk assessment.

“Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the security rule. A risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information,” the guidance states.

As with other aspects of the security rule, CEs (and now BAs) must decide for themselves how exactly to comply with the risk analysis requirement as the draft guidance “is not intended to provide a one-size-fits-all blueprint,” OCR says. But NIST documents are valuable resources, it adds.

As OCR explained in the draft, “Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing electronic protected health information. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.”

The mention of NIST should be welcome news for CEs and BAs, Coyne says. “It is good when OCR gives its blessings to something concrete like the NIST standards. One of the good things about HIPAA is that it gives you a lot of flexibility, but that can be frustrating,” she says.

CEs that follow the appropriate NIST standards “can take comfort in knowing” they likely would be in compliance with the relevant HITECH Act provisions, she adds.

Parmigiani, president of John Parmigiani & Associates, LLC, an information security consulting firm in Maryland, says the guidance reiterates basic concepts in the security rule and emphasizes “the sequence of steps that must be undertaken to assure a thorough and useful risk assessment.”

To get started, OCR says, CEs and BAs could ask themselves these questions OCR adapted from the NIST Special Publication 800-66:

- ◆ Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
- ◆ What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
- ◆ What are the human, natural, and environmental threats to information systems that contain e-PHI?

Although the document is guidance, not regulation, and still a draft at this time, OCR uses the word “should” and “must” repeatedly.

Risk assessments must be performed periodically, depending on a number of factors, the guidance states. These may include:

- ◆ As new technologies and business operations are planned;
- ◆ Following a security incident;
- ◆ Upon a change in ownership; or
- ◆ When there is turnover in key staff or management.

Four Steps Should Be Taken

In conducting a risk analysis, the draft guidance says CEs and BAs:

(1) “*Must identify and document reasonably anticipated threats to e-PHI*” and “*must identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI;*”

(2) “*Should assess and document the security measures an entity uses to safeguard e-PHI*, whether security measures required by the security rule are already in place, and if current security measures are configured and used properly;

(3) “*Must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability;*” and

(4) “*Should assign risk levels for all threat and vulnerability combinations identified during the risk analysis.... The output should be documentation of the*

assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.”

The draft guidance, says Parmigiani, “is a reminder for CEs who may have done one or several risk assessments but need to periodically do reassessments” based on the criteria in the draft guidance. “For BAs, it is a new requirement that spells out expectations for regulatory compliance,” he adds.

While the draft doesn’t contain any earth-shaking or seemingly controversial elements, its appearance came as a surprise. The document was not released with any notice to the press or the compliance community and appeared rather mysteriously on the OCR website on May 10. However, it is dated May 7.

The release coincided with a two-day meeting that OCR co-hosted with officials from NIST, but few in the audience were aware it had been released, and no formal announcements about it were made.

Both Parmigiani and Coyne expect few critical comments from stakeholders.

“I would not expect too many comments that would have any fault with the guidance,” he says, “as the points made are acceptable security best practices not only for

the health care industry but also for any protection of sensitive data.”

Parmigiani predicted any negative comments “may cause some slight modifications” from the draft to final guidance.

When finalized, the guidance is likely to be enforceable as regulations, says Parmigiani. He notes that in December 2006, CMS — then the enforcement agency for the security rule — issued guidance on remote access and laptops.

In that guidance, the agency said, “CMS may rely upon this guidance in determining whether or not the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity, and availability of e-PHI, and it may be given deference in any administrative hearing pursuant to 45 C.F.R. section 160.508 (c)(1), the HIPAA Enforcement Rule.”

It is not clear what topic OCR’s next guidance will address, or when it will be issued. But Coyne says it would be useful if OCR could issue more guidance on the specifics of encryption. Encryption is becoming more standard because, in the event of an inappropriate use or

Beyond PHI or ePHI: Personally Identifiable Information (PII)

By Ali Pabrai, MSEE, CISSP

Ali Pabrai is the chief executive of ecfirst and a cyber security and compliance expert. He created The HIPAA Academy and established the CSCS Program, which is focused on global information security regulations and cyber security. Pabrai may be reached at Pabrai@ecfirst.com.

The HIPAA privacy rule emphasized the mandate for organizations to secure all *protected health information* (PHI). The HIPAA security rule focused on *electronic PHI*, and, more recently, the HITECH Act emphasized *unsecured PHI*.

However, there are other regulations that organizations are increasingly required to comply with as well. The Payment Card Industry Data Security Standard (PCI DSS) is an international security standard for organizations that process credit card payments. It emphasizes controls around *cardholder data*, or information that is stored, processed or transmitted by merchants and other organizations. PCI DSS is managed by the PCI Security Standards Council (PCI SSC) and its founders — American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

And 46 states now have regulations that require organizations to protect and secure *personal informa-*

tion or personal data. For example, California’s SB 541 requires breaches be disclosed to the affected patients, while California’s AB 211 includes fines starting from \$2,500 to \$25,000 per violation for organizations that negligently disclose patient records. Massachusetts’ 201 CMR 17.00 requires each covered business to “develop, implement, maintain and monitor a comprehensive written information security program” that applies to records that contain Massachusetts’ residents’ personal information.

Covered entities and business associates cannot limit the scope of their enterprise information security to PHI or ePHI — the risk extends to all personally identifiable information (PII). PII must be secured with “reasonable and appropriate” safeguards. Most organizations already have developed a comprehensive library of information security and privacy policies to comply with HIPAA and HITECH mandates. It’s advisable for organizations to include in their

disclosure, encrypted data doesn't trigger patient, media or OCR notification (*RPP* 5/10, p. 6).

But, as Coyne notes, "encryption isn't explicitly required anywhere in HIPAA or HITECH."

Contact Parmigiani at jcparmigiani@comcast.net and Coyne at sarah.coyne@quarles.com

RPP's subscriber-only website at www.AIShipaa.com includes an exhaustive 62-page section on "Completing a HIPAA Risk Assessment," written by Cornelia M. Dorfschmid, Ph.D., of Strategic Management Systems, Inc. If you need your password, call 800-521-4323 or e-mail customerserv@aispub.com. ✧

UCLA Researcher Gets Jail Time for Viewing PHI With No Financial Motive

This story was adapted from the May 10, 2010, issue of AIS's Report on Medicare Compliance.

A former University of California at Los Angeles Health System employee is the first individual to be sentenced to prison for improperly accessing protected health information (PHI) in violation of HIPAA without having used the data for personal gain.

Huping Zhou accessed celebrities' and other patients' records hundreds of times but did not attempt to sell the information. His defense that UCLA had failed to adequately train him about HIPAA was not enough to spare him jail time.

Zhou, who is licensed as a cardiothoracic surgeon in China, pleaded guilty just prior to a trial in January to four misdemeanor counts of violating HIPAA. He was sentenced late last month to four months in prison and a \$2,000 fine; he faced a maximum prison term of four years.

"Zhou is the first person in the nation to be convicted and incarcerated for misdemeanor HIPAA offenses for merely accessing confidential records without a valid reason for authorization," the DOJ said in a statement, although a guilty plea is not a conviction.

His lawyer has indicated he will appeal the sentence, calling it "harsh." In the sentencing memorandum, Zhou asked for probation, noting the stress to his family, the loss of his job, and the possibility that he may not be able to become a physician in the U.S.

On Oct. 29, 2003, Zhou, employed as a researcher by UCLA's School of Medicine, was notified he would be fired for job performance issues, according to DOJ.

continued

Beyond PHI or ePHI: PII (continued)

definition of "sensitive information" or "confidential information" not just PHI or ePHI, but also PII.

Organizations have to ask themselves: How prepared are we to secure PII, including PHI, ePHI, cardholder information and personal data or personal information?

Examples of PII that must be secured include:

- ◆ Name, such as full name, maiden name, mother's maiden name, or alias;
- ◆ Personal identification number, such as Social Security number, passport number, driver's license number, taxpayer identification number, or financial account or credit card number;
- ◆ Address information, such as street address and e-mail address; and
- ◆ And personal characteristics, including photographic images, fingerprints, handwriting and other biometric data.

Getting Started: Your Checklist

Targeted checklists are simple and provide for consistent actions and results. Looking ahead, orga-

nizations need to conduct a risk analysis — a HIPAA mandate — and ask themselves:

- ◆ Have we clearly identified all PII residing in the enterprise?
- ◆ Have we categorized PII?
- ◆ Are we applying appropriate safeguards based on confidentiality impact level?
- ◆ Is the collection and retention of PII limited to what is strictly necessary?
- ◆ Have we developed an incident response plan to handle a breach of PII?
- ◆ Has the organization established a "forum" to enable close coordination between privacy officers, CIO, security officers and legal counsel?

Make sure to re-visit your privacy and information security policies and update those to go beyond PHI or ePHI. Moving forward, policies and controls must be founded on PII.

For more information on PII, go to <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>. To learn more about PCI DSS, visit <https://www.pcisecuritystandards.org/index.shtml>.

That night, he accessed and read his supervisor's medical records and those of other co-workers. Apparently his curiosity continued, as Zhou moved on to access and read health records belonging to various celebrities, reportedly including Sharon Osborne, Tom Hanks and Leonardo DiCaprio.

Over the next three weeks, Zhou accessed UCLA's patient records system 323 times. However, the U.S. attorney's office said Zhou never disclosed any of the information or tried to sell it, unlike the circumstances in previous HIPAA cases that have been prosecuted.

Accused Researcher Blames UCLA Training

Zhou's attorneys contended there were problems with the way UCLA was training its employees and that he did not know he was violating HIPAA.

UCLA officials, who initiated the investigation after learning of the inappropriate access, told investigators that HIPAA training at that time consisted of a training module (i.e., manual), a six-question quiz and a certificate showing that the employee completed the course, according to court documents.

Employees could take the test without reading the manual first, and they could take it on-line or in person, the officials said. During the quiz, employees were given three chances to answer a question correctly, after which they would be shown the correct answer. In-person HIPAA training courses were an option, though not a requirement.

Robert Ellis Smith, a Providence, R.I.-based attorney, author and expert witness in privacy rights cases, says "Online training is not bad in and of itself and it's not unusual... But somehow [Zhou] didn't get the message. Any good privacy officer will tell you you've got to continuously tell people" what HIPAA says about disclosing PHI. Some hospitals have signs in elevators cautioning people against talking about patients, Smith says, and such constant reminders are critical to compliance.

After the sentencing, the UCLA Health System issued a statement saying Zhou's access should have been terminated sooner, and that changes have been made to ensure that now happens without delay when the jobs of workforce members are terminated.

In addition, UCLA said it had "put in place a number of safeguards to help ensure patient confidentiality," including:

- ◆ Expanding their information system's auditing capabilities and doubling the number of people audited;
- ◆ Evaluating their clinical information systems to reduce the risk of security violations; and

◆ Implementing a "mandatory and expanded HIPAA training and certification module required for all physicians, staff and students."

Past HIPAA guilty pleas or convictions involved individuals who profited or sought to make money using PHI, often to obtain credit card accounts or defraud Medicare. In cases involving celebrity patients, defendants sold information to tabloid news outlets. In 2008, UCLA fired 13 and suspended seven workers for snooping in celebrities' files.

In a July 2009 case in Arkansas, a physician and two hospital employees pleaded guilty to improperly accessing the records of a local news anchorwoman who was beaten to death. Because they did not use or sell the information, they were sentenced to fines and probation, not jail time (*RPP 11/09, p. 10*).

Smith says it's interesting that the people involved in the Arkansas and California cases were both trained physicians. "I'm not sure all medical [professionals] are aware of the consequences of disclosing medical information. Ironically, we have this tradition and respect for patient confidentiality, but it's breached very often. It's good that we have one case with prison time to act as a deterrent."

According to Reece Hirsh, San Francisco-based HIPAA attorney with Morgan, Lewis & Bockius LLP, the ruling is likely to be an indication of what's to come from DOJ. "The sentence in the Zhou case definitely reflects a much tougher approach to HIPAA enforcement than we've seen in the past. It could be a harbinger of a more aggressive enforcement strategy in the wake of the HITECH Act's heightened penalties and enforcement-related incentives."

Visit www.justice.gov/usao/cac. Contact Smith at (401) 274-7861 or ellis84@rcn.com and Hirsch at (415) 442-1422 or rhirsch@morganlewis.com. ◆

Employees Must Follow Policies

continued from p. 1

Too much "time, effort and resources" are devoted to understanding the technical or other features of a breach without looking at the actual behavior of the person at fault, he says.

Understanding why workers violate policies is essential to preventing future problems. Once these reasons are understood, strategies to enhance compliance can be developed to target these failures.

When faced with a suspected violation or a complaint, Ruelas talks to the employee and walks him or her through what led to the suspect activity. Skillful questioning can produce revealing information.

Another key to cultivating strong adherence to privacy policies among workers is to delve into whether the violation, in Ruelas' terms, was an "oops" or whether the person is a "chronic" violator who has finally gotten caught.

Ruelas employs a questioning strategy known as "the five whys," a process similar to that used when hospitals investigate "sentinel events" as required by the Joint Commission. The concept actually began at Toyota but has been adopted by some businesses as a quality control strategy.

Asking why something happened, then further investigating why the preceding event happened, and so forth, is a "simple process that is not adversarial in nature," Ruelas says.

When he is conducting an investigation, Ruelas tells the employee, "Help me understand why you did what you did because I need to understand this before we can come up with any actions to prevent a recurrence."

Peer Pressure Is One Cause

"Whenever there is a deviation from process, one way to investigate that is to determine the root cause by asking why. By the time you have asked the fifth why you have usually gotten to the root cause," he explains.

The series of questions might also reveal that employees more broadly violate the policy and that the individual who was caught was not the only transgressor, which would present a different scenario than if just one worker were involved.

Among the reasons for noncompliance are "knowledge deficiencies," such as individuals who truly didn't know what was required. But that is rarely the case, in Ruelas' experience.

He cites peer pressure as one cause. If a policy is roundly ignored, even a newly hired and newly trained employee might end up violating it, he says. This happens when the workers who are used to not following the procedure correct the newcomer and say, "we don't bother doing those steps."

Yet another reason is "willful noncompliance," such as when the worker thinks, "I know what I am supposed to do, but I am doing it my own way anyway," Ruelas says.

Between a "knowledge deficiency" and "willful noncompliance" is a middle ground, which Ruelas terms as "open to many descriptions," and he sometimes categorizes the issue as one where the worker lacks "competency" to follow the policy. "It can be poor judgment.... They know what the policy was, but there was some factor that involved them following another path," he says.

When he is collecting facts about an incident, Ruelas is also determining whether the violation was an "oops"

by a well-meaning worker, or the product of chronic violations.

Chronic violators "have a pattern of behavior and might have a history of problems," Ruelas says.

Chronic Problem Versus 'Oops'

When beginning an investigation, he tries to view the possible violator as being in the "oops" category. "I am an optimistic person and I try to be unbiased. Maybe the person is just 'not getting it,'" he says.

Ruelas probes further with an audit on the worker's access activities, if appropriate. Sometimes he will uncover a pattern, and "that is disappointing because I think I could have helped the person earlier," he says.

He sometimes discovers that there have been previous problems, but they were not documented. He recommends that covered entities (CEs) maintain a central file containing all problems an employee has had, so that the compliance officer would know if individuals have had problems in other areas of their jobs, beyond privacy. "There might be different policies they are also violating," he says.

And this is where he believes the value of verbal warnings — with documentation — comes into play. A big mistake some supervisors make is to have a chat when there's a privacy or security issue and offer some verbal chastisement that is not reported in the employee's personnel file.

The Role of Retraining

If the employee then slips up again, and the previous times were never documented, it will be difficult to make a case for stronger disciplinary action. Documenting the verbal warning should have a greater deterrent effect — helping prevent the person from committing a violation in the future, Ruelas says.

"In my experience, a verbal warning is really a misnomer. I call it a verbal warning, but to me it is really a documented meeting" with the worker.

A "common theme" behind lack of compliance is lax enforcement by CEs, Ruelas says. Most organizations have a tiered disciplinary process to deal with infrac-

Introducing:

AIS's Health Reform Week

Helping savvy business leaders in health care understand what the enormous changes mean to them ... and what they can do about it.

Go to www.AISHealth.com

tions, with punishments based on the seriousness of the violation, and should make better use of it.

While to Ruelas there isn't much difference between a verbal and written warning, he says the written warning "might have a bit more sticker shock."

Chronic violators should be subject to greater disciplinary actions than an "oops" worker. This might be the difference between termination and counseling, he adds.

Ruelas also supports the idea of retraining workers, and he doesn't believe it is done often enough. "You are giving the employee a message to follow the policy in the future," he says. "You are holding them accountable and helping them understand. The value of retraining is [the workers] get to keep their jobs," but the hospital or other CE also shows it is willing to take disciplinary action.

He says sometimes entities say they will retrain an errant worker, with the implication that they had trained the person previously, which might not be the case. When the retraining of an individual is done, it should be documented, as with the verbal/written warning, Ruelas says.

Obviously, CEs must periodically remind their workforce of which policies and procedures are in place. The frequency, job duties targeted, and media chosen for training programs vary widely from one CE to the next. But employees can't be expected to follow policies they were trained on in 2003 and not reminded of since.

Finally, to improve compliance, take a look at patterns. Be open to the possibility that there *is* a problem with a policy or procedure, says Ruelas, especially if it is violated a couple of times. Employees might violate a

Is Privacy Compliance Increasing? The Signs Are Unclear

Since the privacy rule went into effect in 2003, the nation is supposed to have a better system in place for protecting patient privacy. But is it working?

Whether compliance is improving over time is not an easy question to answer. Some say compliance has gotten better, as employees have become more familiar with HIPAA's requirements. Yet, breaches continue, although it is unclear whether the incidents themselves are on the rise or related publicity is increasing.

At an institutional level, it may be possible to get a sense of whether compliance has improved by tallying the number of complaints that are forwarded to the privacy or compliance officer. But that, too, really doesn't present a complete or accurate picture, since violations may be going undetected or unreported internally, or greater emphasis on compliance may lead to greater reporting.

A number of rolling challenges might depress compliance rates. Keeping up with technology is one: each new piece of diagnostic or treatment equipment, for example, may store PHI, and portable devices — such as flash drives — that once were the purview of only top-level executives are now more commonplace. They are more prevalent and harder to safeguard. Meeting new and modified requirements — such as encryption — are another roadblock.

Vulnerabilities and opportunities for breaches continue to multiply, even as compliance officers tighten their policies, improve training and hunt for violators.

Heightened awareness, if not actual greater enforcement, no doubt results from the HITECH Act's

doubling of penalties and the new requirement to report breaches to affected individuals, the media and the government.

And the number of complaints to OCR has risen every year, with 6,534 reported in 2004, peaking at 8,701 in 2008. Only 2009 saw a drop, to 7,515. But complaints from the first three months of this year put the numbers back on track to perhaps exceed the 2008 total.

Is There a 'Pandemic' of Breaches?

Surveys provide another clue as to the state of compliance, although those run by vendors can be misleading. One recent survey concluded that "only 15% of hospitals feel they are in compliance with the HITECH Act, which went into effect in February 2010," and 30.5% are only at the "evaluating options stage."

The survey claimed that "hospitals are in the final stages of compliance; however, they are nearly two months behind the enforcement deadline." In fact, OCR is not enforcing anything except for the penalty and breach notice provisions, as *RPP* reported prior to OCR's official announcement (*RPP* 4/10, p. 1)

Hospitals were asked, "how many data breach incidents does your organization investigate each year?" The surveyors then used this number to reflect the number of breaches that *occur* each year, which is obviously not the same thing.

The survey said that "new regulations on hospitals are not curing the pandemic of data breaches and medical identity theft." But ... is this really a "pandemic," or is it part pandemic and part marketing hype?

policy because it is “outdated and no longer practical,” Ruelas says.

“Policies tend to get overlooked,” as privacy folks “are always in a fire-fighting mode. A lot of times policies are in place that don’t apply anymore,” Ruelas says.

For example, faxes are now often sent electronically by fax servers, versus through stand-alone fax machines that may have been described in a CE’s early policies.

“You have to look at the policy to see if it is still applicable, whether it reflects current practice,” he says. “If there has been a policy breakdown,” the CE’s leadership “may have ownership.” If this is the case, the policy should be scrapped or rewritten.

When patterns do emerge, make employees aware of them, and hammer home the solutions. Ruelas sends at least monthly e-mails to all department directors. Using a common subject line, such as “FYI Patient Privacy Info,” or “Information Security,” he shares stories from the media, such as the recent case of a radiologist who used pilfered passwords of former colleagues to contact patients after he moved to another facility (*RPP* 4/10, p. 12).

“I am really trying to capture lessons learned,” Ruelas says. “I use them to motivate employees and promote compliance.”

Contact Ruelas at frank@hipaabootcamp.com ✦

PATIENT PRIVACY COURT CASES

This monthly column is written by Kayla Tabela of the Washington, D.C., office of Sonnenschein, Nath & Rosenthal LLP. It is designed to provide RPP readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Tabela at ktabela@sonnenschein.com.

◆ **The New Hampshire Supreme Court issued instructions regarding hospitals’ compliance with search warrants for privileged medical records.** On May 6, 2010, the New Hampshire Supreme Court issued an opinion outlining the procedure that hospitals and medical providers must follow when presented with a search warrant for privileged medical records. Under this ruling, the procedure for any search warrant for privileged medical records shall be as follows: (1) The order must require the hospital or medical provider to produce the records, within a reasonable amount of time, under seal for *in camera* (“in private”) review by the trial court; (2) The trial court must then determine the manner by which the patient is provided notice that the records were produced, and give the patient and hospital an opportunity to object; and (3) Upon objection, the state must demonstrate that the information is not available from another source and that there is compelling justification for its disclosure. In the case at issue, the defendant, Exeter Hospital (the “hospital”), appealed a Nov. 24, 2008, order of the Portsmouth District Court requiring the hospital to turn over the medical records of an individual pursuant to a search warrant. The hospital had treated the individual after a car accident. The individual had appeared intoxicated at the scene of the accident, and was soon thereafter charged with several offenses in connection with the accident, including aggravated driving while intoxicated. The search warrant application sought the toxicology reports and medical records generated during the in-

dividual’s treatment at the hospital. The hospital complied with the warrant, but sought clarification from the court regarding its future obligations to produce a patient’s medical records, without the patient’s authorization or consent, in response to a search warrant. On appeal, the hospital argued that the trial court erred in requiring it to produce the records because the hospital has statutory and ethical obligations to protect its patients’ confidential medical records. The hospital maintained that the issuance of such a warrant deprives the hospital and its patients of notice and an opportunity to contest the production of such records. The hospital further argued that such search warrants place the hospital in a position where it must either violate its obligations to its patients, or refuse to provide the records and face charges of contempt. The state countered, arguing, in part, that under New Hampshire law physicians must report any injury the physician believes to have been caused by a criminal act. The court, however, rejected this argument. The court reasoned that while New Hampshire’s physician reporting statute places a duty on a physician to report, it does not provide the state with the authority to subpoena privileged records when it suspects medical providers have breached their reporting obligations. Nevertheless, the court affirmed the district court’s ruling upholding the search warrant; but balanced “protections afforded by the physician-patient privilege” with “the well-established law governing search warrants” by issuing the above procedure. (*In re Search Warrant for Medical Records of C.T.*)

PRIVACY BRIEFS

◆ **The Federal Trade Commission announced May 28 it will delay enforcement of the Red Flags Rule again until Dec. 31, 2010.** Developed under the Fair and Accurate Credit Transactions Act, the Red Flags Rule requires creditors, including physicians who do their own billing, to implement safeguards against identity theft (*RPP 11/09, p. 12*). The FTC says it is postponing enforcement to allow Congress time to consider legislation limiting the scope of business covered under the rule. This is the fifth such postponement since the rule became effective on Jan. 1, 2008. On a related matter, the American Medical Association (AMA), American Osteopathic Association and the Medical Society of the District of Columbia filed a federal lawsuit May 21 to block the FTC from extending the Red Flags Rule to physicians. Legislation clarifying who is covered under the rule could prevent further lawsuits. See the FTC statement at <http://www.ftc.gov/opa/2010/05/redflags.shtm> and the AMA statement at <http://tinyurl.com/3xf5c6v>.

◆ **A study commissioned by the California Health-care Foundation (CHCF) found that two-thirds of the public remain concerned about the privacy and security of their health information, but the majority of people who use a personal health record (PHR) are not worried about the privacy of that information.** *Consumers and Health Information Technology: A National Survey*, released in April, was conducted by Lake Research Partners between Dec. 18, 2009, and Jan. 15 and looked at responses from 1,849 individuals. It found that one in 14 people have used a PHR — twice as many as a separate study found the previous year. Most PHR users and non-users stated privacy concerns should not keep people from learning how health information technology can improve health care. See the survey at www.chcf.org.

◆ **The Medical Center at Bowling Green notified 5,418 patients their protected health information may have been breached when computer equipment was stolen from the facility.** The unencrypted equipment contained information on patients who underwent bone density testing at The Medical Center between 1997 and 2009, according to the hospital's press release. The breached information included patients' names, dates of birth, medical record numbers and physician names. Some of the breached records also included Social Security numbers and height and weight measurements. The Medical Center, which

discovered the breach April 1, says "We will now archive data to a secure network, which will allow us to eliminate the need for use of a hard drive like the one that was stolen." The facility encourages patients to monitor their credit reports. See the statement at www.themedicalcenter.org/pdf/Breachv12.pdf.

◆ **A flash drive with personal information for 24,600 patients went missing from Our Lady of Peace Hospital in Louisville, Ky.** According to the public media notice, the hospital discovered the breach April 1. An investigation revealed that unsecured information dating back to 2002 — including patients' names, room numbers, insurance, and admission and discharge dates — was stored on the missing flash drive. The information did not include treatment information or Social Security numbers. The hospital recommends patients monitor their credit reports. Contact Barbara Mackovic at barbara.mackovic@jhsnh.org.

◆ **The computer server at Silicon Valley Eyecare Optometry and Contact Lenses (SVE) was stolen on April 2,** according to a public notice on the facility's website. The server contained patients' names, addresses, confidential medical information and Social Security numbers and was password-protected but not encrypted. SVE is recommending that patients place a fraud alert on their credit files and review their credit reports. SVE says, "We have been informed that a suspect has been arrested. The posting on the OCR website says approximately 40,000 were affected by the breach. See the statement at <http://sites.google.com/site/sve-publicnotice/>.

◆ **Patients at the University of Washington Medical Center (UW) in Seattle were upset to learn that HIPAA allows the hospital to use their health records for fundraising purposes,** according to the *Seattle Times*. Steve Finn, once a patient at UW, received a phone call from the hospital on his unlisted number requesting a donation. Finn told the paper he was surprised that his phone number had come from his records. Under HIPAA, patient information cannot be used for commercial purposes; however, a hospital can use a patient's name, address, contact information, dates of admission, gender, age and insurance status to fundraise. The newspaper reports that UW had not received complaints about the practice until this year, when 150 of the 6,000 patients who were solicited opted to have their names removed from the fundraising list. See the article at <http://tinyurl.com/327emy7>.

**IF YOU DON'T ALREADY SUBSCRIBE TO THE NEWSLETTER,
HERE ARE THREE EASY WAYS TO SIGN UP:**

1. Return to any Web page that linked you to this issue
2. Go to the MarketPlace at www.AISHealth.com and click on “newsletters.”
3. Call Customer Service at 800-521-4323

**IF YOU ARE A SUBSCRIBER AND WANT TO
ROUTINELY FORWARD THIS PDF EDITION OF
THE NEWSLETTER TO OTHERS IN YOUR ORGANIZATION:**

Call Customer Service at **800-521-4323** to discuss AIS's very reasonable rates for your on-site distribution of each issue. (Please don't forward these PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)