Report on
Patient Privacy

Volume 10, Number 1 • January 2010

Practical News and Strategies for Complying With HIPAA

Contents

Go to www.AISHealth.com *for summaries of the latest House and Senate health reform bills.*

Five narrative sections at www.AISHIPAA.com *have now been updated to reflect new requirements contained in the HITECH Act, and a brand-new section on Security Breach Notification has been added. If you don't have a Web site 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

'Loose Lips' Can Get CEs in Trouble, Now That Verbal Gaffes Must Be Reported to OCR

The caseworker probably thought she was doing the right thing by sharing with the patient's daughter that the woman had become increasingly paranoid. But when the daughter confronted the mother with knowledge of her decline, the mother was rightfully outraged — the daughter was not authorized to receive protected health information about her.

The mother filed a complaint with the hospital where she was an outpatient. And the privacy officer must now report this incident to the Office for Civil Rights, under the breach notification requirements contained in the HITECH Act provisions of the Recovery Act *(RPP 9/09, p. 1).*

The hospital is also investigating the incident, taking action against the caseworker, and will formally report to the patient that she was the victim of a breach in the privacy and security of her PHI — as there is no doubt that the patient was "harmed" by the release of information, the privacy officer, who requested anonymity, tells *RPP.*

"This kind of stuff happens way more often at every hospital than a server being hacked into or a laptop being stolen. And when a verbal release like this happens, it almost always causes harm because it is to a friend or family member, or someone who knows the patient," the privacy officer says.

continued on p. 8

HITECH Act's Marketing Provisions Build on Prior HIPAA Regulations, Restrict Incentives

The HITECH Act's marketing provisions, which become effective Feb. 17, 2010, will take HIPAA restrictions up a notch by further limiting the types of communications that are acceptable without prior patient authorization.

With few exceptions, covered entities and business associates will no longer be able to issue marketing communications for which they receive payment, which some experts say leaves little room for anything more than prescription drug reminders.

And while the rule clarifying the statute has not been released — nor has HHS pinned down a date for its release — CEs and BAs will be expected to comply next month. That leaves organizations with a healthy amount of guesswork regarding how to comply with the intricate provision.

The HIPAA privacy rule currently states that marketing using protected health information (PHI) requires a patient's prior written consent. The two types of marketing that do not require authorization are face-to-face communications — an obvious exception, since it would mean getting a signature before having a chat with your doctor — and communications that involve products or services of nominal value, such as giving new mothers free formula as they leave the maternity ward.

Furthermore, a communication is not considered "marketing," and consequently does not require authorization, if it falls under one of the three HIPAA exceptions

for treatment, payment and/or health care operations (TPO):

(1) It describes a health-related product or service (or payment for a product or service) that is provided by, or included in a plan of benefits of, the CE making the communication;

(2) It is made for treatment; or

(3) It is made for case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

Under the HITECH Act passed in February 2009 *(RPP 2/09, p. 1),* communications that fall under TPO and are already permissible without HIPAA authorization must now pass another litmus test: The CE cannot have received payment for the communication.

However, the HITECH Act makes three exceptions here as well. If the CE did receive payment for the communication, authorization is still not necessary when:

(1) The communication describes only a drug or biologic currently being prescribed for the individual, and the amount of payment received for making the communication is reasonable;

(2) The CE making the communication has received a valid HIPAA authorization from the individual; or

(3) The communication is made by a BA and is consistent with the terms of its BA agreement.

The first exception is the biggest change for providers, says HIPAA security consultant Chris Apgar. Physicians "can't receive payment from pharmaceutical companies for getting patients to try new medicines," he explains. They can still receive incentives for giving out samples (of "nominal value") to see if a patient tolerates a certain drug, and for sending out prescription reminders for a drug that a patient is already on. But recommending different medicines is no longer allowed — even if the recommendation is for a new version, such as a time release capsule, of a drug the patient is currently taking, according to Apgar, with Portland, Ore.-based Apgar and Associates.

Rebecca Fayed, a Washington, D.C., attorney with Sonnenschein Nath & Rosenthal LLP, points out that the second HITECH exception is superfluous, because the "whole point of the exception is avoiding the authorization." The third exception, she says, clarifies that "if a business associate makes a communication for you, the mere fact that you pay the business associate to make the communication does not make it marketing." For instance, it's acceptable for a doctor who wants to recommend an alternate treatment to pay a third party to send a brochure about it — as long as the doctor has not received an incentive for making the recommendation in the first place.

Statute's Intent Is Unclear

Some experts say that the statute's vague language and the current lack of guidance muddle the intent of the law. Bob Gellman, a privacy and information policy consultant, contends that "some of the language can be read to prohibit any kind of advertising, even on a covered entity's Web site," since that can be a source of revenue. The wording in the HITECH Act could be interpreted as pertaining to "any advertising that generally encourages the use of goods or services, not tied to use or disclosure of PHI," says Gellman, although "it doesn't make sense to prohibit advertising for anything that isn't based on a patient's identity or health records."

According to Gellman, "the only thing pretty much allowed are prescription drug reminders — nothing else is favored.…The safest thing to do is not engage in any marketing activities" until the HHS secretary offers more guidance.

continued

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.

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

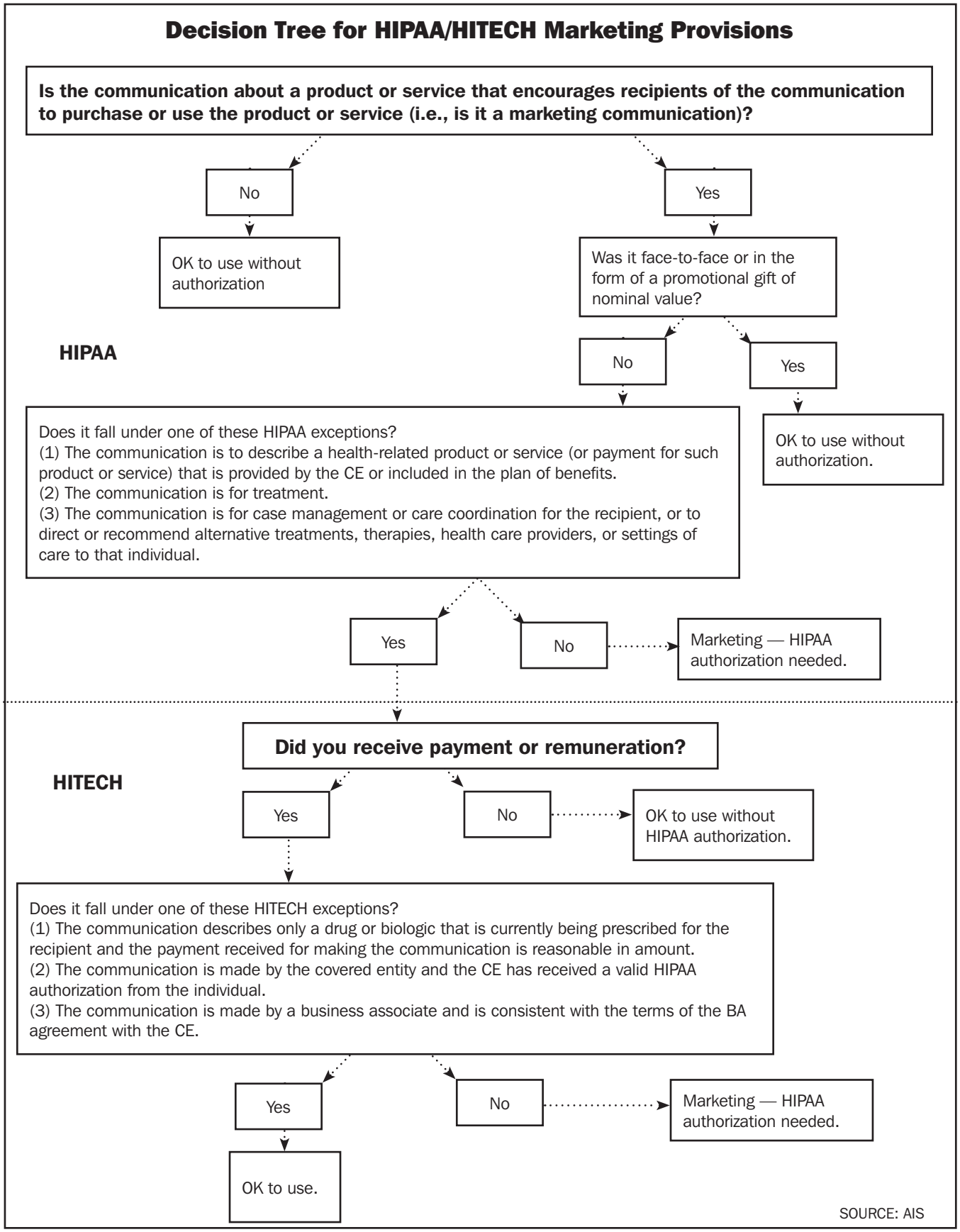
(3) Staple your business card to this form and mail it to:
AIS, 1100 17th St., NW, Suite 300, Wash., DC 20036.

Payment Enclosed* ❑ $429

Bill Me ❑ $404

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

Decision Tree for HIPAA/HITECH Marketing Provisions



SOURCE: AIS

Kirk Nahra, an attorney in Wiley Rein's Washington, D.C., office, says it's tough to define the intent of the law at all. "I'm not sure I see the problem that is trying to be fixed. The effect is to cut back on certain kinds of communications," including those about value-added products such as discount fitness-club memberships, he says. "Were health insurance members complaining about getting discounts? I understand the not-making-a-profit part of it, but I'm not sure this is fixing a privacy issue."

In addition, Nahra says, it's hard to nail down what is meant by a payment. "What if a fitness company will pay for postage for a mailing?…How closely connected to the communication does the payment have to be? Hopefully the rule will answer that" when HHS issues its guidance on HIPAA marketing.

Provision Shouldn't Be Taken Lightly

Enforcement of the provisions will be a challenge, says Apgar, and will require clear communication from compliance officers. "The drug reps come in and talk to physicians one-on-one," he says. Many physicians end up "receiving tickets or dinner out or other forms of compensation, and that's where you need to be careful." Although it's not exactly clear what constitutes payment, since HHS has yet to issue the final rule, compliance officers should take a conservative approach, says Apgar, and tell doctors to steer clear of anything that could be construed as payment. "Don't take those tickets, don't take that free dinner, don't take that $100 gift certificate to Macy's," he says.

Apgar notes there's a lot of anxiety in the industry about the new marketing provisions, which could be quelled with some simple advice. Compliance officers should tell doctors that "the biggest thing they need to focus on is to make sure they're not getting money back for pushing new drugs and new devices."

Fayed, on the other hand, says compensation through football tickets and the like is no longer much of a problem because the majority of "reputable pharmaceutical companies have already been slapped on the wrist [for this]. There's a bigger issue than privacy there — providers are more concerned about kickback issues that arise than privacy.…You're more likely to see high monetary penalties in fraud and abuse than in marketing."

But with enforcement only a month away, privacy and security experts agree that providers should not take this provision lightly. Gellman says that any activities that could be seen as having "marketing intent ought to be on the block for review and probable termination, except prescription drug letters" that remind patients to get refills (though switch letters are no good).

Since marketing is a way for CEs to use PHI for personal gain, Fayed says "it's one of those regulations that the government would be most likely to make a big case out of failure to comply with.…This is one area where I tell clients, don't misunderstand the rules."

But experts also generally agree that until further guidance comes out, understanding the provision is not an easy task. Gellman says that the statute seems like a product of "midnight drafting. There are a large number of problems with the language…. You can take the words and read them one way or another." Nahra says that HHS has a "difficult task in writing the rule and trying to figure out what Congress intended."

Regarding the rule's release, Nahra hears it was supposed to be out by the end of 2009. "They've talked about putting out a mega-rule that covers a bunch of topics — all of the HITECH issues where they didn't have deadlines for the rule," he says. HHS did not return a request for comment on when the rule will be published.

Contact Apgar at capgar@apgarandassoc.com or (503) 977-9432, Fayed at rcfayed@sonnenschein.com or (202) 408-6351, Gellman at (202) 543-7923 and Nahra at Knahra@wileyrein.com or (202) 719-7335. ✧

Human Error With E-PHI Creates Breaches, Need for IT 'Firewall'

An impatient patient, a harried medical-records clerk and the pervasiveness of e-PHI collided recently at Mammoth Hospital in California in a breach that highlights the pros and cons of an electronic environment.

Rushed by the patient for two copies of his MRI results, the clerk properly copied one image onto a CD. But she made the second CD without verifying that the same MRI image remained on the computer screen. As a result, another patient's MRI results landed on the second CD. When the patient got home, he realized the second CD didn't capture the MRI of his foot. It was obvious; the CD had a picture of a head and another person's name. Fortunately, he returned the CD right away and the hospital launched an immediate investigation. As required by California's security breach notification law, Mammoth Hospital informed the state and the patient of the breach and "jumped through hoops for 24 hours," says Greg Young, director of privacy and information security officer.

The state investigated the breach, but was satisfied by the hospital's mitigation and closed the case. The hospital no longer allows employees to release PHI except through the medical records department (though

out-of-towners can obtain their PHI from the emergency department), and Young has shared the lessons learned from the incident in training and in an article in the employee newsletter.

With the possibility of human error, poor judgment and intentional theft, electronic medical record (EMR) systems require careful monitoring and adjustments. Fortunately, they provide the tools to make this easier, since it's very hard for anyone, except perhaps an IT expert, to access an electronic chart without leaving a footprint. But no matter how fancy the technology is, HIPAA compliance still rests heavily on managing behavior and common sense.

"When people think of security, they think of techno-geeks in the corner. They think of things like encryption and firewalls and wireless security. But that's not the biggest risk," says Chris Apgar, president of Apgar and Associates in Portland, Ore. "You can have the best technical security system," but it won't mean much if a person walks out with a laptop loaded with PHI or with a database burned to a CD, Apgar says. That's why training and reinforcing policies and procedures are so important.

NIST Recommends Separating IT Duties

Checks and balances are an effective way to prevent PHI abuses in all areas of the organizaation, including clinical, the business side and information technology.

The National Institute of Standards and Technology (NIST) recommends a separation of IT duties to minimize the risk of improper uses and disclosures of e-PHI (see publication 800-66), says Washington, D.C., attorney Robert Hudock. For example, the IT employees who maintain servers should not be the same employees who conduct security audits. "The person capable of doing the bad act should not be capable of covering up their bad act," Hudock says. That way, if an unscrupulous system administrator steals 5,000 Social Security numbers from a database, it will show up in an audit log, and the bad act will be identified because the system administrator is blocked from modifying audit logs. Only a conspiracy between the two employees could circumvent this safeguard. The idea, he says, is to "firewall" the employees.

Covered entities can get very granular with this separation of duties. "You can start creating divisions within roles within the staff," Hudock says. For example, the person who maintains e-mail doesn't maintain back-up tapes. "The more you divide up responsibility, the more complex it would be for one person to engage in a bad act. The bigger a conspiracy gets, the easier it is to detect," he notes. However, Apgar adds, "this type of granularity only works for larger organizations."

While IT employees present more risk because they are the men and women behind the curtain, Hudock doesn't see them as more likely to engage in identity theft than anyone else. Front-line employees who handle credit cards — in registration, the gift shop, cafeteria — are a bigger threat, he says. To minimize the risks posed by front-line employees, Hudock suggests installing video cameras in vulnerable spots and letting employees know they will be caught if they mishandle credit card information.

And it's been his experience that "when you have a rogue IT person," he or she will engage in destruction, not theft. For example, a disgruntled IT employee who believes he's about to get canned is more likely to unleash a virus than steal PHI, he says.

Carelessness May Be Biggest Risk

Apgar agrees that IT people don't pose that much risk. "It's not even maliciousness like identity theft. The most significant risk is careless staff not adhering to rules," he says. Covered entities are put in the path of HIPAA violations most often by employees and physicians who are reckless with electronic PHI. There are employees who send unsecured e-mails to their friends; surgeons who text anesthesiologists about a procedure without encrypting the PHI-laden message (often because encryption of messages between two people using the same mobile carrier on a secure network is not common); quality assurance staffers who repeatedly send faxes to the wrong number before taking corrective action; and physicians who log in to their practice's EMR system at Starbucks using the Wireless hotspot, oblivious to nearby coffee drinkers who are shoulder surfing and could be learning juicy tidbits about their friends and neighbors. Apgar also points to laptops left in plain sight in vehicles, which he notes is explicitly forbidden by the Oregon Department of Human Services.

"It is these types of things" you have to worry about, Apgar says. "Yes, you will have theft of information because of curiosity or greed. But if you don't secure your facility," it's more likely that people's bad habits will bring you down.

Because behavior is so integral to HIPAA compliance, Young reinforces the concept of a "web of security" to Mammoth Hospital employees. It has to be "the foundation if we are going to have any security," he says. This means employees have to keep an eye on each other. If a colleague is behaving out of the ordinary or does something inappropriate (e.g., pulls a memory stick from her purse and downloads data from a company computer), report the person to the security office. "It's not tattling. It's making sure we do the right thing and that creates a web of security," he says.

To overcome resistance employees might have to turning in a fellow employee, Young explains that everyone is tainted by the bad behavior of one employee. "If I

work with [John] and he stretches the rules, pretty soon I get associated with stretching the rules even though I'm not," he says. Beyond the background checks and the electronic flags and the VIP and random audits, "we are relying on individuals." It's analogous to security at a top-secret facility, where employees never work alone. Mammoth Hospital employees are trained to think on behalf of both themselves and co-workers, according to Young, who is a former police officer. "Not only are they doing things right for themselves, but making sure [co-workers] are doing the right thing as well." If not, their supervisor or the information security office must be informed.

Employees Must Report Each Other

The effectiveness of this approach was demonstrated recently when one employee turned in another for accessing and printing out her own medical records in violation of Mammoth Hospital policy. The woman needed her own PHI for a referral to the doctor so she printed it out and faxed it. "Her co-worker found out and told us," Young says, and now the offender will be retrained. HIPAA permits covered entities to require written requests for medical records for several reasons (e.g., sometimes charts contain notes or other information that were provided with the promise of confidentiality), and by law some lab-test results can only be disclosed by physicians. Mammoth Hospital also implements the policy to ensure employees don't tinker with charges. HIPAA even grants covered entities the authority to deny access to patients for a reason allowed by the privacy rule. Young says there's no cause for employees to access their own medical records; they can get their medical records the same day through proper channels. Because of her apparent impatience, Young says, the employee who printed her medical records "now has had doubts cast on her own integrity." But if it weren't for her co-worker's integrity, the violation may never have been detected.

The strength of electronic medical record systems is that they allow better controls, says Savannah attorney Diana McKenzie. "You can see every nurse and physician who accessed" John Smith's medical records, she notes, and get a red flag when an employee who typically prints 15 medical records at a time suddenly prints 500. But "you have to be thoughtful as to who gets access to what and why they get access to it." She agrees that IT employees could wind up with too much access, but has often found the reverse to be true. "Folks tend to restrict access that can impede a diagnosis," McKenzie says.

For example, with a lot of EMR systems, radiologists are denied adequate access because they don't need it to read images, she says. That's problematic because interpretations vary depending on medical history. "There are certain diseases that create abnormalities that can be misdiagnosed without a fuller picture, so restricting radiologists' access to medical records impedes medical care," she says. But these kinks are being worked out, says McKenzie, with the law firm of Hunter, Maclean, Exley & Dunn.

In the end, Apgar believes that "the two most important pieces to prevent bad things from happening" are policies and procedures. "A lot of organizations have the right practices, but they don't document them." Training should ensure that employees understand the policies and procedures and understand the general privacy and security requirements of the organization and related regulations. For example, some covered entities require employees to sign e-mail policies, which typically require them to encrypt PHI in e-mail and forbid inclusion of sexually explicit material, among other things. By signing, employees are pledging that they understand the policy and will abide by it.

Contact Young at young@mammothhospital.com, Hudock at rhudock@ebglaw.com, Apgar at capgar@apgarandassoc.com and McKenzie at dmckenzie@huntermaclean.com. ✧

Medical Identity Theft Is Low-Tech, High-Risk and Rapidly Growing

With many legislators, law enforcement officials, and privacy experts now calling it the fastest-growing type of crime, medical identity theft has emerged as a forefront issue for health care providers.

And while ID theft may conjure images of hackers overriding systems with sophisticated technology, the reality is that stealing health care information is generally a low-tech endeavor. Stepping into 2010, health care providers should be vigilant about the physical safekeeping of portable tech equipment and take a hard look at their employee hiring and training practices.

Harry Rhodes, director of practice leadership for the American Health Information Management Association (AHIMA), says there are several factors driving the rise in medical identity theft. The recession could be pushing more people toward seemingly low-risk, high-profit crime. It's less dangerous that the drug trade, Rhodes says, and more lucrative than regular identity theft. "Credit limits are usually a couple thousand dollars, while the lifetime benefits on a medical insurance policy go into the millions," he says. The credit card industry has built in safeguards over the last few years, too. For instance, credit card companies will call consumers when they notice abnormal spending patterns, and many gas stations now ask for a cardholder's zip code at the pump.

There are four types of medical ID theft, Rhodes explains:

(1) One-off: An insured individual gives his or her insurance card to a relative, and the relative accesses medical services under that person's name. Or an individual sells his or her insurance card on the street.

(2) Insider: An employee at a health care organization who has the ability to process bills files false claims. Often the employee sets up a bank account and has the payment sent directly there.

(3) Organized crime: Insiders steal and sell patient information, or pay off beneficiaries to give it to them. The organized crime unit sets up a sham medical business and files false claims.

(4) Drug seeking: People buy or steal others' insurance information for the purpose of obtaining narcotics.

In one recent case, says Rhodes, an organized crime unit in Miami trained young women to work as receptionists, and helped them become insiders at clinics. Targeting patients with Alzheimers and dementia, the women would photocopy patient information, and drop the copies into their large handbags. The crime ring would then either file false claims through a sham equipment provider or find "deadbeat docs who were willing to weave in claims," says Rhodes. They kept claims at $9,999, knowing that OIG does not tend to investigate claims under $10,000. "The girls would stay at the clinics for 90 to 120 days, and get out before they were discovered.… No one suspected them because historically clinics have high turnover," Rhodes explains. "It's amazing how really low-tech it was…just girls and purses — nobody hacked in, there were no listening devices."

Laptop Thefts Top the Breach List

And while it's possible to put a few reams of paper in a purse and walk away, it's even easier to slip a two-inch thumbdrive — which can hold confidential information for hundreds of thousands of people — in your pocket. "Anything portable, a smartphone, a laptop, a thumbdrive…losing that one tiny thing can cause gigantic headaches," says Elizabeth Johnson, an attorney with Poyner Spruill LLP in Raleigh, N.C. "That's less true about hard copy."

Rhodes analyzed a list of data breaches from the Privacy Rights Clearing House that occurred between January 2005 and October 2009. Of the 127 incidents in which computer equipment was stolen, 99 were laptops, 20 were backup tapes, three were memory sticks, one was a Blackberry and one a computer server. There were also 11 incidents of lost computer equipment, four of which were memory sticks, and the rest CDs. The list included only seven incidents of stolen paper records.

The majority of laptop thefts occur when people take the equipment home or on a trip, says Rhodes. The computers are snatched out of cars, off mass transit, or from hotel rooms. There are also cases in which thieves work the arriving flight lanes at airports, swiping laptop bags off curbs and tossing them to accomplices in getaway cars.

The Privacy Rights Clearing House data list 12 situations in which employees or business associates exposed PHI over the Internet. Rhodes says that it's "usually someone moving [data] to an unprotected Web site to work on it more easily." Perhaps an employee wants to avoid signing on and off or is trying to override a glitch in the software, so he or she transfers the data to a Web site — which happens to be publicly accessible. Again, confidential information is up for the taking, no hacking needed.

The data also showed 21 cases of improper disposal of PHI, most of which were due to old files being left unshredded. Rhodes says this is common, and that "usually the janitor turns them in. He calls the radio or TV station to report people." In one egregious case, boxes of health records were sold to a school teacher for scrap paper. Most often, file boxes were dumped in the trash or left behind in an office building.

Rhodes found only five instances of external hacker attacks in the almost five-year period.

EHR Conversion Poses a Risk

One major technology risk-area on the horizon, says Ed Goodman, chief privacy officer at Identity Theft 911, is the conversion to digital health records. The government is incentivizing organizations to make the switch, which necessitates "low-level data entry to start converting over," says Goodman, who is based in Scottsdale, Ariz. "There will be lots of lower-paid individuals and there are not always background checks being done. It's pretty easy to abscond with Social Security numbers, credit card numbers or other identifiers." Many organizations are hiring outside vendors to do the work for them. "There could be identity thieves working for the health care vendors," Goodman notes. "That info's like cash, it's like gold."

And in a waning economy, budgets tend to drive decisions. Goodman warns that CEs "don't always know who they're doing business with. They need to make sure they're not going with a cut-rate fly-by-night solution."

The Hungry Beast Feeds Itself

With the government upping enforcement efforts, through the new breach notification rules and upcoming stiffer civil monetary penalties, CEs and BAs have little room for error. Enforcement recoveries are now being funneled back into enforcement, which Goodman calls "the hungry beast that keeps feeding itself." The Federal Trade Commission's Red Flags Rule, enforcement of which has been postponed four times but is slated to begin June 1, also requires health care organizations that

do their own billing to have identity theft mitigation and detection programs.

Privacy and security experts agree that, above all else, employees pose the biggest fraud risk. Whether due to negligence, a lack of understanding or a decision to break the law, one employee can undermine an entire organization's security and put thousands, even millions, at risk for ID theft. "Preventing medical identity theft comes down to staff training, education and awareness," says Rhodes.

Here are some things CEs and BAs can do to prevent medical ID theft:

(1) Examine your privacy and security policies and procedures. Are you encrypting data? Requiring password-protected log-ins to access PHI? Address any weaknesses. "Obviously super mega-breaches that are high-tech grab the headlines. But they arise from poor security practices," says Goodman.

(2) Implement background checks when hiring new employees. Inquire with business associates about their hiring practices.

(3) Limit access on a need-to-know basis — an approach that is required by the role-based access of HIPAA's minimum necessary standard. A receptionist in charge of scheduling patients probably does not need access to much more than the schedule. Goodman calls this a "layered approach" to access.

(4) Consider double-checking patients' identities, according to Johnson, because "it's not hard to have someone else's insurance card." When given an insurance card, confirm the patient's address or ask for a second form of ID, such as a driver's license.

(5) Train employees on identifying and reporting breaches, proper disposal of PHI, secure vs. unsecured Internet networks, and other areas of possible breaches. Make education ongoing and document the trainings.

(6) Emphasize the new enforcement provisions under the HITECH Act. Rhodes explains that "in the past, employees were exempt. But now the way the rule is rewritten, employees can be found guilty and fined or imprisoned. The ante is going up." Make sure employees know they are personally at risk.

Privacy officers should keep in mind that employees can do just as much to reduce risk as they can to increase it. Johnson, who specializes in privacy, points out that "employees are also your first line of defense. If someone is attempting to steal data, it's going to be employees who are in the best place to realize what's happening and either prevent it or notify people in a timely fashion."

With well-thought-out policies and staff training, "this is a crime you can actually do stuff about," says Rhodes. "And the things you can do to protect yourself are not necessarily very high-tech or costly."

Contact Rhodes at Harry.rhodes@ahima.org, Goodman through Christopher Bacey at cbacey@identitytheft911.com and Johnson at ejohnson@poynerspruill.com. ✧

Verbal Releases of PHI Are Common

continued from p. 1

This scenario is probably not what most compliance officials think of when they ponder the new breach notification requirements. But this kind of incident, even though the breach was verbal, must be reported to OCR, if there is a significant risk of harm and if the daughter was not involved in the mother's care nor authorized to receive the information, says Richard Campanelli, former OCR director who is now in private practice in the Washington, D.C., office of Baker & Daniels LLP.

The privacy officer is increasingly frustrated that verbal gaffes like this one still occur nearly seven years after the privacy rule went into effect. And she believes that most health care organizations may not realize they must include this incident in their annual log of breaches that is submitted to OCR.

She also worries that health care workers and compliance officers are placing too much emphasis on "electronic" breaches. She argues that although they have the potential to expose more individuals' data, electronic breaches are fairly infrequent. Also, studies have found they rarely result in harm to the patient.

No 'Shut Up' Software

Experts *RPP* consulted feel the privacy officer's pain. They say that verbal slip-ups are a tough nut to crack but agree they must be addressed, as the stakes are far higher now that penalties have doubled for violations of all kinds of misuses of PHI.

"People are not computers, and we have to remember both the protection of orally communicated information and paper-based information implicates the privacy of the patient, and we must continue to focus on all those protections," Campanelli tells *RPP.* "While the emphasis on electronic breaches is justified, we still need to focus on the personal aspects of protecting information, and that requires training, diligence and leadership so that there is a culture of compliance."

Jeff Drummond, a partner in the law firm of Jackson Walker LLP, based in Dallas, says such verbal slipups "are probably harder to stop because there's no technical fix for it. You can't buy `shut-up' software like you can buy encryption hardware, and you can't audit employees' verbal activities like you can audit their electronic access."

Reece Hirsh, a partner in the San Francisco office of Morgan, Lewis and Bockius LLP, points out that while the privacy rule allows "incidental disclosures," which may occur by accident or are unavoidable, unauthorized disclosures like the caseworker made are not OK.

"Because there is some flexibility in the law regarding incidental disclosures, there is a tendency to think that inappropriate verbal disclosures aren't going to get you in trouble. But they definitely can," Hirsch says.

Abner Weintraub, president of the consulting firm, The HIPAA Group, says he has always taken issue with the term incidental disclosures, saying it "tends to minimize" the importance or impact they can have, and makes CEs less accountable.

Prohibited 'Verbal Leakage' Is Common

During site visits related to his consulting work, "we see [verbal breaches] constantly," but he adds, "it is easier to change technology than to change people." Weintraub says he hopes that the increased penalties for all kinds of breaches will prompt more CEs to place a greater emphasis on preventing and controlling what some refer to as "verbal leakage."

Hirsch adds that this particular situation points out the thorny issues that can arise when disclosures by workforce members involve family members and sensitive problems, like behavioral health disorders.

"It is challenging for the privacy official to get that message across so that [family] disclosures really are appropriate and they understand who a patient's personal representative is," defined as the individual who can receive a family member's PHI, Hirsch says. Personal representatives are usually defined in state laws.

Be Vigilant and Send a Message

To clamp down on verbal breaches, CEs will have to periodically retrain workers, send reminders, and act swiftly and publicly to punish offenders, Drummond says.

"CEs should be vigilant in [providing] continuous education," Drummond says. "Most aren't. The more you can do to educate your staff, the better. It is particularly effective if loose-lipped employees are corrected when they foul up, particularly in a way that sends a message to everyone else. You don't necessarily want to publicly embarrass them, but that might be a fitting way to make sure the lesson is learned, not just by that employee but by the others as well. And if someone egregiously breaches privacy, like a snooper, they should be terminated with as much fanfare as you can stomach — you don't want to get sued for it, but you want to make it an object lesson to the other staff that privacy violations will cost you your job."

Some verbal breaches should be dealt with in the same fashion as electronic infractions, with sanctions and retraining, says Drummond. The penalty should depend on the severity of the incident.

"If the breach is intentional, or intentionally careless, it deserves harsher action," Drummond says. "If the breach is more damaging, it deserves harsher action. Equally blameworthy breaches, one verbal with little risk to the patient and one electronic with many patients affected, should be treated differently, with the electronic breach getting harsher punishment. But that doesn't mean you shouldn't still punish, or at least educate, the verbal breacher."

Training the workforce "just once and then forgetting about it" isn't going to protect the CE, Campanelli says. "And the privacy officer should be given the kind of

authority and gravitas to be able to help create that culture…at all levels of the organization." This is important because sometimes doctors are the offenders, and employees may have a difficult time challenging their behavior.

He adds that, under the HITECH Act, the clock to address and report on breaches starts ticking as soon as the CE — or its workforce members — knows or should have known of them. So employees also must be trained to alert the privacy official or their superior ASAP whenever there is an incident that might be of concern.

Six Additional Compliance Tips

Experts interviewed by *RPP* identified these additional steps CEs can take to prevent such breaches:

(1) Emphasize in workforce training materials and educational sessions that a verbal breach is a real breach that can subject them to all the same penalties and sanctions as electronic breaches and other inappropriate disclosures, as specified in the facility's policies and procedures.

(2) In training, include examples, such as the caseworker inappropriately talking to a family member, so the workforce members can better understand what types of infractions may occur. Explain how these differ from incidental disclosures.

(3) Remind the workforce that the covered entity will now have to report breaches to patients immediately, and to OCR either immediately or annually depending on the extent of the breach. Just that knowledge may help spur fewer thoughtless or careless disclosures.

(4) Consider revising or adding new sections to training materials or modules, to better define "breach" to involve the verbal or oral communication of verboten PHI. Specifically insert the words "verbal" or "oral" in the materials.

(5) Walk through the facility and see what PHI can be heard and seen. Make notes of inappropriate disclosures and share them with the individuals at fault. Take action when necessary.

(6) Because business associates are also responsible for reporting breaches to the CE, and the CE to OCR and the patient under some circumstances, CEs may wish to revise their business associate agreements to ensure that oral and verbal breaches are spelled out *(RPP 12/09, p. 4).*

Even while tweaking compliance programs in this way, the bigger picture must remain in focus. Says Drummond, "Don't let your electronic PHI compliance efforts lead you to take your eyes off the non-electronic compliance issues. The fact that you're focusing on one doesn't give you the right to forget about the other. Annual — or more often — HIPAA education is really necessary."

Taking steps such as "tightening policies, modifying training and adding privacy reminders" is essential, says Weintraub. "Those can change attitudes, but it is going to be a slow process."

OCR itself could make a simple change to help CEs enforce the notion that verbal breaches are worthy of attention. OCR recently created an online form that CEs can use to report breaches; those that affect 500 or more individuals must be reported right away, while any

under that number can wait until the annual report is filed, due two months after the close of the calendar year.

OCR's online filing form does not have a category for oral or verbal breaches, so presumably these would go under "other." That should change, says Weintraub.

"I think that shows an institutional bias toward electronic breaches, and a failure to equate verbal breaches with them," he says. "I would absolutely recommend that OCR make that change. Until that is done, the workforce isn't going to consider these significant."

Contact Campanelli at Richard.campanelli@bakerd.com, Hirsch at rhirsch@morganlewis.com, Drummond at jdrummond@jw.com and Weintraub at Abner@HIPAAgroup.com. ✧

PATIENT PRIVACY COURT CASES

This monthly column is written by Rebecca Fayed 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 Fayed at rcfayed@sonnenschein.com.*

◆ **The Michigan Supreme Court will decide whether HIPAA permits *ex parte* interviews of treating physicians by defense counsel in medical malpractice cases.** The plaintiff filed a wrongful death medical malpractice action alleging that the defendant physician failed to diagnose or treat the plaintiff's decedent. During the course of this action, the defendant physician sought to interview the decedent's treating physicians. Although the plaintiff authorized the disclosure of the decedent's medical records, the plaintiff refused to authorize the oral communications. The defendant physician attempted to obtain a qualified protective order to permit the *ex parte* communications with the treating physicians, but the Michigan Circuit Court denied the defendant's motion. In November 2008, the Court of Appeals of Michigan reversed the lower court's decision and held that the defendant physician was permitted to conduct an *ex parte* interview with the decedent's treating physicians if a qualified protected order, consistent with the requirements of the HIPAA privacy rule, was put in place. According to the court, the HIPAA privacy rule permits disclosure of protected health information during the course of a judicial proceeding under certain circumstances, regardless of whether that protected health information is in written or oral form. Thus, because the HIPAA privacy rule permits a covered entity to disclose protected health information if a qualified protective order is in place, an *ex parte* discussion with the decedent's treating physicians would be appropriate. In May 2009, the Supreme Court of Michigan granted the plaintiff's motion for an appeal. According to the Supreme Court of Michigan, one of the issues to be addressed is whether HIPAA permits *ex parte* interviews by defense counsel with treating physicians pursuant to a qualified protective order. Oral arguments began in November 2009. *(Holman v. Rasak)*

◆ **An Ohio Court of Appeals held that redacted non-party medical records are not discoverable.** While a patient at St. Elizabeth Health Center, Carol Bednarik overheard one of the nurses tell another nurse that Bednarik's roommate had a highly infectious disease. Shortly after being discharged, Bednarik was rehospitalized because she had contracted this infectious disease. As a result, Bednarik filed a medical negligence action against the hospital. During discovery, Bednarik requested the redacted medical records of the non-party patient with whom she had shared a room. However, the hospital refused to disclose the medical record and filed a motion for a protective order arguing that the record was privileged. Although the lower court ordered the hospital to provide redacted copies of the non-party patient's laboratory results, the Court of Appeals of Ohio recently overturned that decision holding that a non-party patient's privileged medical records, redacted or not, are not discoverable. The court acknowledged that many courts have relied on precedent to allow discovery of a non-party patient's redacted medical records where disclosure is necessary to protect or further a countervailing interest that outweighs the patient's interest in confidentiality. However, the court ultimately relied on a more recent Ohio Supreme Court decision that stated that this exception regarding disclosure of medical records to protect a countervailing interest merely provides a defense to liability for unauthorized disclosure of confidential medical information, but that it does not create a litigant's right to discovery of confidential non-party medical records. *(Bednarik v. St. Elizabeth Health Center)*

PRIVACY BRIEFS

◆ **HHS and CMS closed 2009 by issuing two rulemakings to implement the electronic health record provisions in the American Recovery and Reinvestment Act.** In a proposed rule, CMS set out a definition of "meaningful use" that providers would have to meet to receive incentive payments for EHR technology. The rulemaking proposes criteria, which increase over a three-stage process and are based on specific objectives. The first stage has 25 objectives for professionals and 23 objectives for hospitals; Stage 1 would begin in 2011. The second rulemaking, an interim final rule, sets out the initial standards, implementation specifications, and certification critera for EHR technology. Both rulemakings will be published in the *Federal Register* on Jan. 13 and have 60-day comment periods. They are posted on the *Federal Register* Web page, www.federalregister.gov/inspection.aspx#special, under "Special Filing."

◆ **Administrators at University Medical Center (UMC) in Las Vegas discovered on Nov. 19 that confidential information — including names, birthdates and Social Security numbers — for at least 21 patients had been breached, but they had yet to inform patients of the leak as of Dec. 10,** according to an article in the *Las Vegas Sun*. A source for the Sun alleges that the patient information was being sold over a period of months or even years to ambulance-chasing attorneys. Kathy Silver, UMC's CEO, was called before the state's Legislative Committee on Health Care after the Sun wrote a series of articles about the alleged breach. Silver contends that the hospital has 60 days to make the disclosure. The FBI is also investigating the HIPAA violation. UMC will provide a year of free credit monitoring for affected patients once the hospital notifies them. See the article at http://tinyurl.com/yaue2kl.

◆ **Two new studies in the *Journal of the American Medical Informatics Association* show that U.S. doctors support the use of electronic health records (EHRs) but are concerned about patient privacy breaches, especially in the area of mental health,** according to *USA Today.* One study, which surveyed more than 1,000 family practice and specialist doctors in Massachussetts, found that 86% believe a health insurance exchange (HIE) would improve the quality of care, and 70% believe it would cut costs. However, 16% are "very concerned" about privacy breaches and 55% are "somewhat concerned." None of the doctors surveyed want to pay a $150 monthly HIE fee, while half are not willing to pay a fee at all. The second survey, which included 56 psychiatrists, psychologists, nurses and therapists at an academic medical center, found most believe EHRs are clearer and more complete than paper records, though not necessarily more factual. In addition, 63% are less willing to include highly confidential information on an EHR than a paper record, and 83% say as a patient they would not want their mental health records routinely accessed by other health care providers. See the article at http://tinyurl.com/yjcn7ok.

◆ **The University of California San Francisco (UCSF) announced Dec. 15 that it notified 600 individuals that an external hacker may have obtained access to e-mails that contained their personal health information.** In September 2009, a faculty physician at the School of Medicine provided his/her e-mail username and password in response to an e-mail that appeared to be from someone updating the security on UCSF internal computer servers, but was actually part of a phishing scam. An audit of the possible security breach revealed that the physician's e-mails — which contained patients' demographic and clinical information, and in a few cases Social Security numbers — may have been exposed. UCSF advised patients to review their explanations of benefits for unusual payments and says it "has provided re-education to workforce members to ensure that they protect their user IDs and passwords." See the press release at http://tinyurl.com/y9jm7tj.

◆ **The Detroit Department of Health and Wellness Promotion announced Dec. 15 that it is investigating two medical record thefts.** In late October, a flash drive containing birth certificate information — including parental health information, addresses, Medicaid numbers and Social Security numbers — for residents in the 48202 and 48205 zip code areas was stolen from a health department employee's car. Then, five computers were stolen from the Herman Kiefer Health Complex during the Thanksgiving break, one of which contained 2008 Medicare and Medicaid seasonal flu billing information. Neither the flash drive nor the computers have been retrieved. Officials from the health department sent letters notifying individuals who may have been affected by the breaches. The Detroit Police Department is also investigating the case. See the press release at http://tinyurl.com/ygggcba.

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.)