Report on
Patient Privacy

Volume 14, Number 11 • November 2014

Practical News and Strategies for Complying With HIPAA

Contents

Looking for a back issue of **RPP**? *PDF issues, plus a searchable article database, are archived on your subscriber-only Web page — all the way back to 2008! Log in at* ***www.AISHealth.com*** *and click on the newsletter title in the gray "My Subscriptions" box on the right.*

Policies, Procedures and Other Documents Will Be Key When OCR Audits Resume

Now that it seems likely the HHS Office for Civil Rights (OCR) audit program won't begin until 2015, covered entities (CEs) should take the next couple of months to get their houses in order before some of them hear an auditor's knock on their door.

Actually, most of the upcoming audits — there may be 300 or more — won't be done in person, so there won't be a literal knock from an auditor, but a letter or maybe an email. OCR is planning "desk audits," consisting primarily of a document review of HIPAA policies and procedures, as a top OCR enforcement official recently explained. Some audits will be on site, but OCR has issued less information about these than it has about the desk audits.

Required under the HITECH Act, OCR first conducted a total of 115 audits in 2011-2012 under a "pilot" program *(RPP 7/12, p. 1)*. Overall, these organizations flunked, racking up some 1,000 findings among them, when assessed for compliance with privacy and security rules, and, to a lesser extent, breach notification *(RPP 3/13, p. 1)*.

Following an analysis of the pilot, OCR planned to launch its permanent audit program this year, but it has been delayed, due most recently to the development of an online survey and portal through which documents can be uploaded *(RPP 10/14, p. 1)*.

continued on p. 9

Hospitals With Ebola Patients Are Under Great Pressure to Ensure Their Privacy

Anne Adams, whose titles include chief compliance officer and chief privacy officer for Emory Healthcare, was glad to "get the call" seeking her participation in a meeting of an "operations team" to discuss how the Atlanta-based health system was going to handle communications related to a patient with Ebola.

Most U.S. hospitals will never care for a patient exposed to Ebola; to date, fewer than a dozen such individuals have sought treatment here. But the strategies employed by Adams and others at Emory — which include sending repeated email reminders about HIPAA to its workforce — are applicable to other types of high-profile patients, such as dignitaries, celebrities or accident victims, particularly those who've already been identified by the media.

In addition to its interviews with managers at Emory, *RPP* also talked to John Burklow, associate director for communications and public liaison for the National Institutes of Health, whose Clinical Center cared for several Ebola patients. Officials from the University of Nebraska, which also has treated Ebola patients, did not return *RPP*'s calls in time for deadline.

HIPAA covered entities (CEs) and their business associates (BAs) need to be more mindful that members of their workforces will be tempted to snoop in these patients' records. *The price of noncompliance can be high:* Just ask Shasta Regional Medical Center. In 2013, its parent company paid $400,000 in state and federal penalties and accepted a three-year corrective action plan with the HHS Office for Civil Rights (OCR). Former

OCR Director Leon Rodriquez called Shasta a "poster child" for bad HIPAA behavior *(RPP 11/13, p. 1)*.

Their misdeed? Executives talked to the media and their employees about a patient who had already been featured in news articles but had never authorized Shasta to share any of her protected health information (PHI).

Similarly, the media had already chronicled the life-and-death-struggle of Emory's first Ebola patient, Dr. Kent Brantly, well before he was spirited to Emory University Hospital from Liberia in August. To date, Emory has successfully cared for four of the 10 patients who have been identified as receiving care in the United States for Ebola.

Emory Faced 'Unprecedented' Press Demands

At Emory, the heightened risk to patient privacy and the need to tightly control information "was recognized right away," Adams tells *RPP*. "I was asked to come to the first communications meeting and [was] able to answer questions and provide guidance" as to what was permitted and prohibited under HIPAA.

The operations team brought Adams together with Emory's CEO; chief medical officer; Vince Dollard, assistant vice president for communications; and representatives of facilities management and other departments. Dollard and Adams spoke exclusively to *RPP* about their experiences.

At Emory, team members, who Dollard says "initially" met twice a week, worked to craft the communications strategy and messages Emory would utilize about these patients, both internally and externally. Dollard and Adams say this team's effective functioning was a key contributing factor in how well Emory was able to handle caring for these patients while maintaining its compliance with HIPAA.

Although the guiding principle under HIPAA hadn't changed — "patient privacy is paramount" — there certainly were added complications. "What was different about this situation was the sheer volume of news media that descended on Emory was unprecedented," Dollard says, and it also was atypical that the media already knew the patients' names.

Additionally, the task of ensuring there was no inappropriate access or sharing of these patients' PHI by Emory's workforce was increased by the sheer size of the group of caregivers who had "appropriate access." Dollard says the Ebola direct care team consisted of five physicians and 21 nurses.

In some respects, the groundwork for special privacy precautions had already been laid, Dollard and Adams explain. All Ebola patients were admitted to Emory's Serious Communicable Disease Unit, which Dollard says was established in collaboration with the Centers for Disease Control and Prevention 12 years ago to treat CDC employees.

By default, the names of individuals in this unit do not get added to the patient directory, and instead are assigned a status of "no information."

"We felt that was the best way to ensure [privacy and] to care for the patient," Adams says. "If anyone calls and asks if [such] a patient is here, we [say] we don't have any information in our system." That means in addition to not providing any information about a patient's condition, Emory won't confirm or deny the patient is being treated there, she explains.

Press Needed to Be Educated

Dollard says Emory asked each Ebola patient what information they wanted released and honored their wishes.

"Our first two patients were both affiliated with large missionary organizations," Dollard says. "While they and the patients' families through the course of treatment…gave interviews and obviously used their names, our patients did not want to come off our formal 'no information' status and we respect their right to privacy," Dollard says. "In talking with the news media we

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.

Editors, Theresa Defino, Francie Fernald; Executive Editor, Jill Brown; Assistant Editor, Lauren Clason; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Tracey Filar Atwood; Production Director, Andrea Gudeon

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.AISHealth.com that include a searchable database of *RPP* content and archives of past issues.

To order an annual subscription to **Report on Patient Privacy** ($524 bill me; $494 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Subscribers to *RPP* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

never used their names, until the news conference" that Brantley gave upon his discharge from the hospital.

Emory's actions weren't always immediately understood — or accepted — by the media. "At the outset, the news media were asking for names and specific treatment information," Dollard recalls. "We remained steadfast even though [reporters] were saying 'But their families are out there'" communicating with the press.

Dollard says he routinely included links to information about HIPAA in email exchanges with reporters.

When information was issued, any details came straight from the patients themselves. For example, one drafted a statement describing his improving condition while still declining to reveal his name, a situation that prompted *The Washington Post* to describe him as the "little mentioned" Ebola patient and Emory as "tight-lipped" (see http://tinyurl.com/oxvj9rc).

To accomplish their companion task of ensuring internal HIPAA compliance, Emory's leadership suggested sending an email "blast" to all Emory Healthcare employees, which was done several times.

Adams says these "gentle reminders" focused on several main themes, including warning against sharing information even if no patient names are used, and especially not on social media.

The email admonished workers to "**NOT** talk about or discuss patient information in public areas (cafeteria, restrooms, elevators, etc.)" and to "**NOT POST ANY** items or information about our patients on any social media site (e.g., Facebook), even if you think it may be de-identified information." (See box below for the email Emory sent to its staff and physicians.)

Emory also activated an additional control on its electronic medical records system, Adams told *RPP*. Workers who try to access Ebola patients' records are stopped by a message that appears on the computer screen, and must affirmatively check a box attesting that they are authorized to view the PHI before the system lets them continue.

continued

Emory Healthcare Email to Its Workforce on Privacy of Ebola Patients

Emory Healthcare in Atlanta has cared for four of the 10 patients treated thus far in the U.S. for exposure to Ebola. As the first was arriving, the system's leaders sent the following message to its workforce staff and physicians to ensure they understood the need to continue "keeping patient information strictly confidential" despite the media frenzy.

Dear Staff and Physicians,

Our expertly trained physicians, nurses and staff at Emory University Hospital safely and securely received a patient with Ebola virus. All standard infection control protocols were followed precisely, and we are so honored to have the privilege to care for this patient. Our deepest gratitude goes out to our care team.

The media, the community and the entire world continue to have great interest in patients with Ebola. You may see numerous media trucks parked along the road. You may also hear reports or speculation regarding the condition of the patient. We continue to respect the privacy of all our patients and are bound by HIPAA compliance rules. So, despite the media attention, we are keeping patient information strictly confidential. Thank you for respecting the privacy of all our patients and their families. As a reminder, we all should:

- **ONLY ACCESS** patient information to complete employee-specific job duties and for job-related functions.
- **ONLY ACCESS** the minimum amount of patient information needed to complete the job at hand.
- **NOT** talk about or discuss patient information in public areas (cafeteria, restrooms, elevators, etc.). Anything said that can identify a patient is considered protected information.
- **NOT POST ANY** items or information about our patients on any social media site (e.g., Facebook), even if you think it may be de-identified information.

In the interest of patient privacy, we don't anticipate sending you a lot of updates, but we will provide information when necessary. To learn more about Ebola, our safety protocols, CDC advisories and tools to help address questions your patients may have, please visit the Ebola information site.

We are so proud of the work you are doing for the patient and all of our patients across the system.

Thank you.

SOURCE: Emory Healthcare.

Running audit trails to see who had accessed these patients' records is another action Emory is taking, and with good reason.

Conducting such audits was also apparently the way the University of Nebraska's medical center discovered two workers had violated HIPAA by reviewing information about an Ebola patient receiving treatment there, one of two it has cared for.

The medical center issued a statement announcing the termination of the two workers, stating it had also taken "other corrective action."

NIH Sent Alerts Before Patients Arrived

NIH, as an arm of the federal government, already operates under a bright spotlight, and one that has intensified since July when several vials of smallpox were discovered unsecured in a refrigerator on its Bethesda, Md., campus.

That discovery led to congressional hearings and a temporary halt to certain types of research, not to mention giving a big scare to, as Burklow puts it, NIH's "literal neighbors" — businesses and a school located nearby.

So with the goal of "no more surprises" in mind, NIH decided to announce internally and externally that it was expecting a patient who had been exposed to Ebola, as well as report that the patient had "safely" arrived, and later when the patient was discharged.

"Part of the process here is to announce to our own staff" when something of this sort is happening, so that they don't first learn of it from the media, Burklow says.

The patient told NIH not to release his name, and neither Burklow nor any of his care team did so. NIH described him as "an American physician who was volunteering services in an Ebola treatment unit in Sierra Leone."

Even though it is not a HIPAA covered entity — the Clinical Center falls under the federal Privacy Act — and the principles are much the same, Burklow tells *RPP*. NIH is also governed by medical ethics practices.

When it received a second Ebola patient, NIH went through the same announcement cycle, but in this case the patient was Nina Pham, the 26-year-old Dallas nurse who contracted Ebola while caring for Thomas Eric Duncan, the only patient in the U.S. to die of Ebola to date.

Before she was to be discharged, Pham told the Clinical Center staff she would participate in a press conference. NIH hastily pulled together the event, at which Pham, joined by NIH Director Francis Collins and others, read a prepared statement. (For more information, see http://www.nih.gov/news/health/oct2014/od-24a.htm.)

Overall, Burklow says NIH experienced few problems in managing communications and privacy for these patients, but he noted it learned from previous experiences handling similar circumstances. And, he says, he even found the press to be "very respectful."

"The first weekend…there were satellite trucks parked in front of the Clinical Center," he says. Officials asked the press if they could "please leave and come back" the following Monday. "And they did."

One consideration important for success is to ensure the appropriate balance is struck between maintaining patient confidentiality and providing information to the press, the public and members of the workforce, Burklow says. "You almost have concentric circles of people affected" and will need to "keep everybody in mind and abreast of developments without compromising patient privacy," he says.

Contact Adams at anne.adams@emoryhealthcare.org, Dollard at vdollar@emory.edu and Burklow at burklowj@od.nih.gov. ✧

CE/BA Compliance Survey Churns Up Countless Problems to Be Solved

Smaller covered entities and business associates want and need more educational and other resources to strengthen their HIPAA compliance. This is one of the findings in a recently released survey on how covered entities (CEs) view compliance by their business associates (BAs). The survey was funded by the California HealthCare Foundation (CHCF), which earlier this year received $500,000 from a $4.1 million settlement with Stanford University and two of its business associates for leaving patient information online for more than a year.

Under the terms of the settlement, CHCF will use the funds to establish educational materials and outreach to increase business associate awareness of compliance with federal and California law *(RPP 4/14, p. 1, 11).*

To prepare for the project, CHCF contracted with Manatt Health Solutions (MHS) to survey CEs and BAs about their compliance practices. MHS, a policy and business advisory division of the law and consulting firm Manatt, Phelps & Phillips, LLP, mailed questionnaires and interviewed 16 covered entities of varying sizes and functions and five business associates that were technology and software vendors and health information networks. It also reviewed the literature on OCR investigations and other government audit findings, private lawsuits, breach statistics compiled by OCR and news reports on the large scale breaches involving business associates. The purpose of the survey was to "assess" and provide an overview of "Business Associates' compliance

with their obligations to protect health information under HIPAA."

Overall, the size of the covered entity and the business associate made a big difference in how the relationships were managed and what the entities believed they needed to do to strengthen their compliance efforts. Another overriding theme was the amount of resources business associate compliance consumes.

Just Counting All the BAs Can Be Difficult

Larger covered entities reported that they often estimated their total number of BAs because it was difficult to maintain a centralized database of all possible vendors. Likewise, for larger business associates, the challenge was maintaining and updating thousands of BA agreements (BAAs). However, for small business associates, the biggest HIPAA challenge was the disparate requirements of their covered entities' BAAs.

To reduce the time spent determining which vendors were business associates, some covered entities had all vendors sign BAAs, even if they would not fall under the definition of "business associate." Some even had other covered entities receiving the PHI for treatment or health care operations sign BAAs, which is not required by HIPAA.

This practice, the report points out, actually conflicts with HIPAA because a BA is required to use the PHI on behalf of the covered entity and return or destroy it when its function is completed. The covered entity using PHI for treatment or its own health care operations was not using it on behalf of the disclosing covered entity and would not return or destroy the PHI. One covered entity reported including in all vendor contracts an obligation to comply with the business associate provisions of the law to the extent the vendor had access to PHI. This, according to the covered entity, "negates the need to re-evaluate the BA status of the vendor every time the scope of work changes."

For a covered entity with thousands of BAs, it is practically impossible to perform due diligence on prospective candidates, according to the survey. Most CEs reported doing little to no due diligence, but larger covered entities made an exception for BAs providing IT services with access to electronic PHI. In this case, CEs viewed these contracts as high enough risk to devote resources to the investigation. Some of the covered entities send prospective BAs a questionnaire asking about various aspects of their HIPAA compliance. CEs then use the data to stratify the BAs into risk categories, which determines how much additional investigation they will perform before signing the contract, as well as the amount of resources to be devoted to monitoring and oversight.

CEs also said they often feel the tension between the need to quickly execute a contract and the need to perform thorough due diligence. To address this, some CEs allow time-sensitive contracts to be signed immediately and conduct due diligence after the signing. The agreement allows the CE to revise the contract if concerns surface during due diligence.

To assess the amount of resources they will devote to monitoring BAs, covered entities said they do a cost/benefit analysis of the resources and generally concluded that the cost outweighed the benefit. Smaller covered entities reported that they rarely have the resources to do any sort of ongoing monitoring. For some covered entities, the one exception, in addition to the vendors that handle electronic PHI, were BAs that sent PHI offshore or themselves were located offshore.

Many covered entities do not allow their BAs to store PHI offshore, but if they do, they engage in a higher level of due diligence, usually performed by their IT staff. The report cites several examples of how covered entities handle BAs who store PHI offshore or who are located offshore: (1) more frequent and stringent on-site audits of the offshore BA; (2) stringent policies and procedures, such as no phones with cameras in the workplace; (3) covered entity executive level approval for use of any offshore BA; and (4) strict limits on the countries in which a BA may be located.

Smaller BAs Are Often Less Reliable

While covered entities contract with all sizes of business associates, from "'mom and pop'" businesses to organizations with national or international operations, not surprisingly they reported that the smaller business associates, or those new to health care and/or unfamiliar with their obligations under HIPAA, "place significant stress on the business relationship between the two entities." If a BA had an individual or an office dedicated to HIPAA compliance (which generally was the case with larger BAs), the covered entity had much more confidence in the BA's compliance capabilities. In contrast, "the absence of any particular person or office at the BA responsible for privacy law compliance is...an early (and often alarming) indication of a lack of sophistication about HIPAA."

The most frequently negotiated provisions in the BAA were the provisions the covered entity added to the HHS/OCR standard BAA, including indemnification, the time frame for breach notification and which party is responsible for breach notification and costs. If the business associate wants to negotiate provisions in the contract, some covered entities believe the BA is "paying attention" to its HIPAA obligations. The report noted that larger business associates have more bargaining power

than smaller BAs to "dictate the terms of their business and legal agreement."

One area where covered entities still seem somewhat disorganized is the return or destruction of PHI once the BA's use of it on behalf of the covered entity has ended. While all the BAAs include the provision that requires return or destruction, CEs admit that they do not have a process in place to assure that the PHI is indeed returned or destroyed. One covered entity with a process described the steps it takes: (1) the purchasing department notifies the legal/compliance department that a contract is expiring; (2) the legal/compliance department sends a return/destruction form to the business relationship owner; (3) if the contract is not being renewed, the business relationship owner asks how the BA will ensure the return or destruction of the information; (4) the covered entity asks the BA to sign an attestation that the PHI was destroyed, or if destruction is infeasible, the BA must notify the covered entity in writing and state that it will maintain the PHI in compliance with HIPAA.

Breach Notification Is a Concern

Breach notification by a business associate also requires special attention in the BAA. HIPAA allows up to 60 days for a covered entity to notify an individual after discovery of a breach, but most covered entities set a much shorter time frame for the BA to notify them. Not only does a shorter time frame give the covered entity time to comply with its 60-day requirement, but many state laws, such as California, have an even tighter notification deadline. (California requires notification to individuals within five days of a breach of medical information.) In general, covered entities not subject to California's deadline require the BA to notify them within 10 days of discovery; in California, covered entities require immediate notification.

Some covered entities are concerned about how few notifications of possible breaches they have received from BAs. Those that were reported generally were attributed to human error. But, covered entities said, there is no way to reliably determine whether a breach has occurred at the BA that requires notification. Some attributed the low reporting of security incidents to the BA's "lack of awareness of its obligation to report more than a lack of security incidents."

Overall, there was no clear consensus among covered entities of the impact the HITECH requirements had had on BA compliance with HIPAA. A few covered entities said they are probing their BAs' relationships with their subcontractors and are emphasizing that the subcontractors as well as the BAs must execute a BAA. Some covered entities said that direct regulation did not enhance their confidence in BA compliance; others thought compliance would increase over time.

In addition to the number and varying provisions of the agreements they have to deal with, other challenges for BAs include finding staff with HIPAA compliance and security expertise and dealing with the number of audit requests from covered entities related to IT security. Some business associates are having a third party audit them so that they can present the results to the covered entity to fend off an audit request.

Most BAs Have Workforce Training

Most business associates have some sort of employee training. Large BAs have training programs for new hires and an annual mandatory refresher course. Another offers weekly Web-based training. Small BAs may not have such formal programs, but instead refer employees to the readily available OCR training materials available on the Web.

One negative factor identified by business associates was the unwillingness of other BAs to share best practices, primarily for competitive reasons.

BAs that serve small or solo physician practices reported that they worry more about the practice's HIPAA compliance than they do their own. Technical safeguards seem to be the area of concern.

As noted, one purpose of this survey was to identify the educational needs of both covered entities and business associates. While larger covered entities and business associates did not feel they needed additional training resources, smaller covered entities and business associates believed they would benefit from additional education and training, particularly programs that are more "user friendly" or "common sense." Trade associations, such as the county medical associations, and government entities, they said, would be an "appropriate conduit for materials, webinars, and in-person training." "Training modules should be comprehensive and authoritative so that Business Associates can deploy the information to their staff. There should be a go-to person/resource for follow up questions." California CEs highly recommended additional training for BAs on California's breach notification requirements, as well as California protections for sensitive health information, such as mental or behavioral PHI. CEs, however, said they did not want to provide training to their business associates and voiced concern about any liability that could be associated with such training.

One recommendation made by some covered entities and business associates was the development of a third-party certification program for BAs, which if accepted by covered entities could save the BA time and resources. However, some covered entities, particularly

the larger ones, said they would not accept such a certification in place of their own due diligence and oversight. Others noted that it was unclear whether a third-party certification would satisfy the priorities of the government.

Other strategies and themes from the interviewees included (1) standardization of BAAs, due diligence/risk assessments/questionnaires and independent audits and certifications; (2) development of assessment tools to evaluate and manage business associates; (3) resources to perform increased audits or educate covered entities to ask the business associates for their security risk assessment; (4) education about who is and who is not a business associate to overcome the overly cautious approach some covered entities are taking; and (5) participation in a "Compliance Officer Peer Network," like the one operated by the California Primary Care Association.

Some even recommended elimination of the BAA altogether, but others found the BAAs worthwhile because (1) they provide legal protections and recourse for both parties; (2) they assign responsibility among the parties and address various business provisions not included in the required BAA elements; and (3) they reinforce the need for confidentiality of important information. Regardless, one covered entity said the business associate agreements are "a fact of life."

CHCF has not announced what its next steps are to fulfill the mandates of the settlement agreement.

For a copy of the survey results visit http://tinyurl.com/kaxcksw. ✧

Two Calif. Courts of Appeal Side With Covered Entities in PHI Cases

Recent decisions handed down by two California courts of appeal will give California health care providers a reason to breathe easier. Both cases involved the theft of computers from the providers and alleged violations of the California Confidentiality of Medical Information Act (CMIA). The act, among other provisions, allows individuals to bring suit, which HIPAA does not, and provides an individual $1,000 in damages from a provider who has negligently released confidential medical information in violation of the act. The individual does not need to show that he has suffered or was threatened with actual damages.

In the first case, *Eisenhower Medical Center v. Superior Court of Riverside County,* E058378 (Cal. App. 4th, May 21, 2014) (www.courts.ca.gov/opinions/documents/E058378.PDF), the medical center appealed a lower court ruling denying its motion for summary adjudication. The information on the computer stolen from Eisenhower contained over 500,000 individuals' demographic information and medical record numbers but no medical information. The CMIA requires an unauthorized release or disclosure of individually identifiable information *and* medical information. The CMIA defines "medical information" as "any individually identifiable information... regarding a patient's medical history, mental or physical condition, or treatment." Individually identifiable information is any information that would allow identification of the individual, such as name and address.

The case focused on what constituted "medical information," as defined in the law, which, if improperly disclosed, would violate the statute. The lower court ruled that the mere presence of a patient's name in hospital records was "medical information," but the appeals court reversed. It held that "medical information cannot mean just any patient-related information," such as demographic information; it must include information on the patient's medical history, diagnosis or care. "The mere fact that a person may have been a patient in the hospital at some time is not sufficient."

In the second case, *Sutter Health v. Superior Court of Sacramento County,* C072591 (Cal. App. 3rd, July 21, 2014) (www.courts.ca.gov/opinions/documents/C072591.PDF), the stolen computer clearly contained medical information in the form of the medical records of four million individuals. The issue before the court here was whether the plaintiffs needed to prove actual viewing by an unauthorized person. The lower court had ruled against Sutter, but the appeals court reversed. According to the court, "the mere possession of the medical information or records by an unauthorized person was insufficient to establish breach of confidentiality if the unauthorized person has not viewed the information or records." The law, the court said, "does not provide for liability for increasing the risk of a confidentiality breach [such as would be the case with the theft]. It provides for liability for failing to 'preserve the confidentiality'" of the medical records. And there is no breach if no unauthorized person has viewed the records. The plaintiff must allege a breach of confidentiality, which it had not done in this case, not just a loss of possession. The decision

includes a discussion of another recent case, *Regents of University of California v. Superior Court*, 220 Cal. App. 4th 549 (2013), in which the court also held that there must be an actual breach of the information, although it reached its decision based on a different analysis than the court of appeals in this case.

The whistleblowers in both cases appealed to the California Supreme Court, but the court refused to hear either case.

As a result of these two rulings, a U.S. district judge dismissed CMIA allegations against Alere Home Monitoring in a case where a laptop with 116,000 patient names was stolen from an employee's car in 2012, according to the whistleblowers. The plaintiffs put forward a number of allegations, including the CMIA allegations, but the court, in an order granting Alere's motion to dismiss, denied all the allegations because the plaintiffs did not allege actual viewing of the records. The court did give plaintiffs leave to amend to "allege additional facts that would remedy the...dismissed claims." Plaintiffs, however, may not allege unjust enrichment because California has no cause of action for unjust enrichment. *Falkenberg v. Alere Home Monitoring, Inc.*, No. 13-cv-00341 (N.D. Calif., Oct. 7, 2014) (https://ecf.cand.uscourts.gov/doc1/035112244092). ✧

Florida Law Not Preempted by HIPAA, Lower Court Is Reversed

The Court of Appeals for the Eleventh Circuit has overturned a lower court decision that found that HIPAA prempted a Florida statute. The Florida law required the plaintiff to sign an authorization for release of PHI before filing a medical negligence lawsuit. The district court held for the plaintiff, ruling that "because the... authorization form was not voluntary," the provision would result in disclosure of the plaintiff's "HIPAA-protected health information without his consent and without other safeguards in HIPAA and its regulations."

Under Florida law, a plaintiff in a medical negligence lawsuit must give 90 days of notice to the defendant before initiating a lawsuit. Florida statute §766.1065 requires the plaintiff to include with the 90-day notice a signed authorization to disclose "protected health information that is potentially relevant to the claim of personal injury or wrongful death." If the plaintiff does not include a valid authorization, the presuit notice is void, and the plaintiff may not bring the lawsuit.

In the authorization, the plaintiff must list the names and addresses of all health care providers who either (1) examined, evaluated or treated the plaintiff with regard to the relevant injuries or (2) examined, evaluated or treated the plaintiff during the two years prior to the incident at issue, but if these providers have no relevance to the injury, the plaintiff may expressly exclude contact with them. The authorization allows defendants to conduct *ex parte* interviews with the physician, insurer, adjuster, experts or attorneys and with the listed providers, unless they are not relevant. The plaintiff's treating physician does not need to consent to the interview.

In its decision the court reviewed all the requirements of the Florida authorization form and found that it contained all the elements required by HIPAA in §164.508(c) of the regulations. However, the plaintiff challenged some of the Florida elements, including the list of providers not relevant to the lawsuit. The court noted that HIPAA permits an individual to disclose his or her entire medical record regardless of the reason and opined that "it is not a defect that the Florida presuit authorization permits disclosure of some information that may be irrelevant to the plaintiff's medical negligence claim."

The court also held that HIPAA does not require that "the scope of an authorization be commensurate with a specific, legitimate purpose," again pointing to the fact that an individual may release his or her entire medical record. It also explained that the description of the information to be released must be sufficient to allow the covered entity to know which information the authorization references. The law, it said, does not require authorizations to be narrow, only to be specific. It found the Florida authorization language, which stated that the authorization was for the purpose of facilitating the investigation and evaluation of the claim, to defend against any litigation, or to obtain legal advice with regard to the claim, was sufficiently specific to pass HIPAA muster.

The plaintiff also argued that HIPAA only allows compound authorizations, subject to certain exceptions, not authorizations combined with other legal permissions. Here, the court said, HIPAA precludes combining an authorization with another legal permission, not "literally 'any other document.'" The presuit notice, it said, is not a legal permission but merely a condition precedent to filing. The fact that the authorization must be sent out with the presuit notice "does not create an impermissible compound authorization."

Authorizations: Voluntary or Mandatory?

Plaintiff's last argument challenged the "voluntary" nature of the Florida authorization — the argument that had convinced the district court that HIPAA preempted the statute. By requiring him to sign the authorization or forego the lawsuit, the plaintiff maintained, the law is contrary to HIPAA, which, he contends, requires all authorizations to be signed voluntarily. The court of appeals disagreed, stating that HIPAA has "no explicit voluntariness requirement...and the HIPAA regulations

contemplate that HIPAA authorizations may be based on conditions." It pointed to the fact that the covered entities were prohibited only from conditioning medical treatment or receipt of health care benefits on the signing of the authorization. This explicit prohibition, the court said, "implies that there are no implicit prohibitions on requiring HIPAA authorizations in other circumstances." The court went further, concluding that HHS acknowledged that "some coercion is allowed" when it permitted states to require a recipient to sign an authorization before receiving Medicaid benefits.

The court concluded that "conditioning the use of the state courts on compliance with a federal provision (HIPAA) does not conflict with that federal provision.... Had the drafters of the HIPAA regulations wished to preclude a state legislature from conditioning a public benefit — such as filing a lawsuit — on signing a HIPAA authorization, they could have easily done so....The regulations do not do so, and we must give effect to the regulations' silence." *Murphy v. Dulay*, No. 13-14637 (11th Cir. Oct. 10, 2014) (http://media.ca11.uscourts.gov/opinions/pub/files/201314637.pdf). ✧

Step Away From That Subpoena and Review Your HIPAA Obligations

This story was written by Elizabeth Litten, a partner in the Fox Rothschild health law practice in Princeton, N.J., and is reprinted with permission of Fox Rothschild LLP. For more information, contact Litten at elitten@foxrothschild.com.

If you receive a subpoena, discovery request, or even a court order demanding the release or production of documents or files that may contain protected health information (PHI), are you obligated to comply? The surprising answer, in many cases, is "no." Even more surprising may be the fact that, in attempting to comply with what appears to be a valid legal document, you may actually be violating federal law.

HIPAA regulations require, first and foremost, that covered entities, business associates, and their subcontractors protect the privacy and security of PHI they create, receive, maintain, or transmit. HIPAA regulations permit disclosure of PHI only under very specific circumstances, one of which includes disclosures for judicial and administrative procedures. Yet even this specific "judicial and administrative procedures" circumstance contains limits and, notably, *permits,* but does not *require* the disclosure. While other HIPAA regulations require disclosure under specific circumstances, the regulations specific to "judicial and administrative procedures" allow, but do not mandate, the disclosure. Recent inquiries about litigation matters that involve subpoenas, court orders, and PHI prompted me to list a few reasons to step back and carefully consider your HIPAA obligations before responding.

(1) Does the demand or request require you to redact PHI from your response? If so, be sure not only to remove all obvious individual identifiers, but review 45 C.F.R. 164.514 to make certain you have completely de-identified the information. (Beware, for example, of failing to remove geographic identifiers, such as the city in which the individual resides.)

(2) If the demand or request is contained in a court order, can you limit the disclosure to only the information authorized in the order? Do not produce documents or files in response to an order of a court or administrative tribunal if the production might result in the release of PHI that is not specifically identified in the order.

(3) Evaluate the demand or request to ascertain if the PHI demanded or requested is the "minimum necessary" to meet the purpose. Do not produce documents or files in response to an order of a court or administrative tribunal if the production might result in the release of PHI that is in excess of what may be deemed to be "minimally necessary" under HIPAA to achieve the purposes of the subpoena, discovery request, or court order.

(4) If the demand or request is contained in a subpoena or discovery request, you cannot disclose PHI until you receive required assurances. Bear in mind that you "may" disclose PHI in response to a subpoena or discovery request, but only after receiving satisfactory assurances that the individuals affected have been contacted or that a qualified protective order has been sought.

Don't be intimidated by an official-looking legal document or assume that because it demands information in connection with litigation (whether you are a party to the litigation or not), you can ignore your responsibility to protect and secure PHI under HIPAA. Remember that the lawyer who drafted (or sent you) that subpoena, discovery request or court order is not responsible for your HIPAA compliance. ✧

Get Ready for OCR Audits

continued from p. 1

"In all likelihood we are not going to really see the audit program kick into full gear until 2015, rather than 2014 as originally planned," says Adam Greene, a partner in the Washington, D.C., office of Davis Wright Tremaine, who made his remarks during an Oct. 28 webinar offered by the American Hospital Association, "OCR HIPAA Audits...Will You Be Prepared?"

Greene was joined by Mahmood Sher-Jan, executive vice president and general manager with ID Experts, a

breach prevention, assessment and mitigation firm based in Portland, Ore.

OCR officials have released some details about the audit program in speeches at conferences and through a notice in the *Federal Register* on February 24, 2014 *(RPP 3/14, p. 1)*. But the information has been changing, evidence that the program has not yet been finalized.

Greene says OCR had been expected to complete 400 audits, of which 50 would be of business associates (BAs). The actual number has not yet been determined. The audits may be split 65%-35% among CEs, with 65% being of providers and 35% health plans, he says.

"And that's largely because of what they saw in those initial audits," Greene says, with "bigger problems" being reported for providers than other groups.

Greene reviewed how the audits may progress over the first couple of years of the upcoming program. Like the pilot, the desk audits will assess CEs' compliance with the three regulations — privacy, security and breach notification. But Greene believes that, unlike the pilot, OCR will choose just one of the three for each per CE.

For example, if a CE is asked to provide data and information on breach notification, it will not be audited for compliance with the privacy and security regulations.

Within this framework, Greene described the focus of the first batch of desk audits, predicted to begin next year. He also offered to fill in some of the details of what audited CEs can expect.

◆ ***Risk analysis and risk management.*** OCR officials may request "the most recent risk analysis and risk management [plan]. It's possible they may ask for prior versions too, but in all likelihood they'll be focused on the most recent one."

◆ ***Content and timeliness of breach notifications.*** The agency may ask for information on "what breach notifications were made, and to the extent that there were incidents that did not rise to the level of a breach, they're going to want to see your documentation" supporting that decision.

◆ ***Notice of privacy practices and individuals' rights of access.*** Auditors are probably "going to focus on looking at the notice to check that the content is all there, but they are also likely going to want to see documentation that it is posted properly, and that, if you are a health care provider, for example, you are documenting acknowledgment of receipt of the notice by individuals." Access rights could prompt "lots of questions….I think they are going to want to see that you timely provided individuals with access upon request and that you have policies and procedures in place" as appropriate.

The 2016 phase, Greene says, will focus more on security rule compliance, and highlight "device and media controls, transmission security, general privacy safeguards and training on policies and procedures."

As far as the outlook beyond 2016, OCR officials "are initially thinking [about reviewing] encryption and decryption," says Greene. "So think, data at rest; facility access controls [and] what physical security you might have in place."

OCR may modify audit target areas "based on high risk areas identified in [earlier] audits, breach reports and complaints," he adds.

Policies Should Be Ready — and Finalized

Once OCR selects a CE for a possible audit, Green notes that the organization will also be asked to identify all of its business associates, which OCR will use to develop a pool of potential BA auditees.

"So if you're a CE, now's the time to look at your vendor management process. Because you're going to, in all likelihood, have a very small timeframe to produce for OCR, if you are in this initial survey pool, a list of all your BAs. And if you're not able to do so, there's some risk that OCR will essentially open up a compliance review because they feel like you do not sufficiently have BAs under control," he warns.

Greene points out that CEs are likely to have "a matter of days rather than months to respond to the data requests," based on the timeframes in the pilot.

"All documentation must be current as of the date of the request. They will not accept documents that were created after the date of request. It's also valuable, therefore, to have dates on all your policies so that there's no question that the policy was finalized before the data request," Greene says.

Greene adds a further word of caution. "Be careful about policies pending indefinitely, waiting for the CEO or someone else to sign them because that could get you into trouble," he says. "They're not going to be accepting draft policies."

Because auditors will have little or no contact with audited CEs to seek clarifications, "your program has to speak for itself," he says.

"There's not going to be phone interviews. There's not going to be opportunities to provide written clarification, necessarily. Your documents need to be pretty self-explanatory. Throwing in the kitchen sink will not help you," he adds, and providing "a lot of information that wasn't asked for" may produce "a grumpy auditor," something no one wants.

In addition, Greene says, OCR has made it clear that "if you are not able to respond comprehensively, they will potentially send you to one of the regional offices for

a compliance review, with the high probability that [this] will then lead to [a] formal settlement penalty."

Greene summarized the major features of a risk analysis "because this is a big focus area" of the audits. Specifically, a risk analysis should "cover all electronic protected health information, not just your electronic health record."

As a first step, the risk analysis must "identify all reasonably anticipated threats," he says. "That's going to include intentional human threats like a hacker or a malicious insider" as well as "inadvertent human threats."

Examples of these are "a firewall that was accidentally turned off and not turned back on," the sending of an email without encryption, or even the use of a PowerPoint presentation with "PHI embedded" in it.

Don't forget natural threats such as earthquakes and flooding and man-made environmental threats, such as network or power failures, Greene says.

OCR officials "really want to see all these sorts of threats addressed and then identify corresponding vulnerabilities based on what security controls you have in place," he adds.

"So, you can have a hacker, but if there's no vulnerability, there's no risk there," he says. "You have to look at what vulnerabilities you might have that any of these threats might exploit."

Sher-Jan reviewed incident response plans as a necessary component of a breach notification program. Incident response plans are required under the security rule, and are used by CEs to analyze a possible data loss or misuse to mitigate the effect and perhaps keep the event from becoming a reportable breach *(RPP 9/14, p. 5)*.

Sher-Jan also reminded webinar participants that they must be "mindful" of the breach notification requirements imposed by state governments, in addition to HIPAA regulations.

He points out that, compared to the federal regulatory landscape, "state laws change much faster, and keeping up with them is much harder."

Currently there are 47 states and three territories that have data breach notification laws, he says, adding that his firm is "tracking more than 20" jurisdictions that have considered changes this year. It is important, then, "to have a system in place to keep you compliant" with new requirements.

To view the presentation, go to http://tinyurl.com/pvl9w22.

Contact Greene at adamgreene@dwt.com and Sher-Jan at mahmood.sher-jan@idexpertscorp.com. ✧

PRIVACY BRIEFS

◆ **CMS on Oct. 16 released the certification agreement and privacy and security agreement for qualified health plans to sign before doing business on federal exchanges for 2015.** The agreements cover items like health plan obligations to protect personally identifiable information and ensure secure communication links with CMS. The documents also contain assurances from CMS that the agency understands that health plans developed their insurance products based on tax credits and cost-sharing reductions being part of exchange coverage. In a nod to pending litigation that could strip subsidies from federal exchange coverage, CMS said insurers could have cause to terminate the agreements if this happens. The full U.S. Court of Appeals for the D.C. Circuit on Sept. 4 agreed to conduct a second hearing on the controversial *Halbig v. Burwell* case, which could upend health reform law tax subsidies for enrollees on federal exchange. Visit http://tinyurl.com/pkntgy8.

◆ **Seventy percent of health care data breaches in California were due to lost or stolen hardware or media containing unencrypted information,** an Oct. 28 report from the state's Dept. of Justice found. The 25 health care breaches reported accounted for 15% of all breaches in California in 2013, affecting 1.1 million records, or 6% of the total number of records affected. Retail accounted for the vast majority of records affected, thanks in large part to Target Corp., whose breach compromised 7.5 million records in California. Visit http://tinyurl.com/mcfqjza.

◆ **A potential security breach of unspecified origin at the Arizona State Retirement System may have compromised the private health information of 44,000 Arizona retirees enrolled in the state's dental plan,** *The Arizona Republic* reported on Oct. 27. The agency is notifying affected individuals and will pay for 12 months of identity protection for any who request it, which cost the agency an estimated $291,000. Visit http://tinyurl.com/mrdycon.

◆ **Community Health Systems (CHS) is facing another class action lawsuit over its recent data breach,** WBIR reported on Oct. 12. A New Mexico

PRIVACY BRIEFS (continued)

woman is suing the hospital for negligence in the hacker attack that exposed more than 4 million patients' personal information earlier this year. Briana Brito and her attorneys say CHS did not notify affected patients in a timely manner, and plan to join another class action lawsuit against the hospital in Texas. Visit http://tinyurl.com/m6dqbko.

◆ **The Department of Homeland Security is investigating roughly two dozen medical devices and hospital equipment that are potentially vulnerable to cyber-attacks,** anonymous sources told iHealthBeat on Oct. 23. The devices include Hospira's drug infusion pump, Medtronic's implantable heart device and St. Jude Medical's implantable heart device. The sources said there have been no hacking cases to their knowledge. Visit http://tinyurl.com/l5oowfy.

◆ **A printing error compromised 4,000 patients' privacy at South Texas Veterans Health Care System,** KSAT reported on Oct. 8. Letters that the provider mailed to patients concerning a new federal rule on hydrocodone combination were printed double-sided, exposing another veteran's information to the veteran who received the letter. The letters contained names, addresses and prescription drug information. Visit http://tinyurl.com/nvxt58q.

◆ **Cone Health accidentally mailed more than 2,000 patient letters to the wrong addresses,** the provider announced on Oct. 9. Cone said a clerical error is to blame, exposing patient names, physician names and the names of the practices the patients visited. Visit http://tinyurl.com/l98thas.

◆ **Colorado health officials inadvertently violated the privacy of 15,000 people when it mailed out postcards to Medicaid behavioral health patients,** *The Denver Post* reported on Oct. 10. The postcards were mailed as part of a survey to patients receiving behavioral health services. The agency said it has notified the patients and is revising its policy to prevent future mishaps. Visit http://tinyurl.com/pbwy4mr.

◆ **A Penn Highlands Brookville center in Brookville, Pa., may have suffered a data breach through a vendor's access to its server,** the facility reported on Oct. 13. A hacker may have gained access to the server through the vendor, which maintains records for Penn Highlands. Potentially affected information includes names, addresses, dates of birth, driver's license numbers, phone numbers, insurance information, medical information and Social Security numbers. Penn Highlands said forensic experts could not say for certain whether a data breach actually occurred. Visit http://tinyurl.com/lj6535v.

◆ **A "small number" of laptops went missing from several Dallas ambulances between Jan 1, 2011, and Aug. 29, 2014,** *The Dallas Morning News* reported on Oct. 14. The city did not disclose how many laptops went missing or how they disappeared, but did say that on Aug. 15 it discovered one of the software applications the laptops use was not properly protected. The laptops contained patient names, ages, gender and EKG information. Visit http://tinyurl.com/m94opjj.

◆ **Lucia Savage was named chief privacy officer of the Office of the National Coordinator for Health Information Technology (ONC),** *HealthITSecurity* reported on Oct. 14. She was previously senior associate general counsel at UnitedHealth Group's UnitedHealthcare, and succeeds Joy Pritts, who stepped down in June. Visit http://tinyurl.com/oyctzbr.

◆ **A stolen laptop from a Cedars-Sinai Medical Center employee's home contained information for tens of thousands more patients than previously thought,** the *Los Angeles Times* reported last month. Cedars-Sinai initially reported the June burglary affected at least 500 patients, but has now increased the number to more than 33,000, the article said. The hospital changed its estimate after consulting a data forensics firm. The Social Security numbers for 1,500 patients were among the compromised information. Encryption software for the laptop had not been reinstalled after a change in the computer's operating system. Visit http://tinyurl.com/nqjk47n.

◆ **Medical information is worth ten times as much as credit card information on the black market,** a Sept. 24 Reuters article said. Hackers use personal and medical information gleaned from health care databases to purchase drugs and medical devices that can be resold for profit. Security experts said health care systems are an easy target because of their oft-outdated cyber security systems, and also because of the length of time it takes before authorities discover the breach. For more information, visit http://tinyurl.com/lf55pzy.

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 provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — 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.)