Report on
Patient Privacy

Volume 16, Number 7 • July 2016

Practical News and Strategies for Complying With HIPAA

Contents

Editor
Theresa Defino
tdefino@aishealth.com

Associate Editor
Lauren Clason

Executive Editor
Jill Brown

New Settlement Over Stolen Phone Shows OCR Is Serious About Business Associates

In a new $650,000 settlement full of "firsts," the HHS Office for Civil Rights (OCR) has slapped a business associate (BA) for the theft of an unencrypted phone that contained protected health information (PHI) of fewer than 500 nursing home patients.

This first settlement with a BA should give a boost to CEs who struggle to convince their BAs that they, too, will face enforcement action for noncompliance, and the two-year corrective action plan reads like a virtual checklist to ensure the appropriate policies and procedures are in place (see box, p. 10).

But the agreement with Catholic Health Care Services (CHCS), a division of the Archdiocese of Philadelphia, will reverberate in other ways, too. The seventh OCR settlement to be announced so far this year brings the agency's 2016 haul to a record $9.3 million, topping its previous record of $7.94 million set in 2014. And it's only July.

The settlement, announced June 30, was prompted by the theft of an iPhone, which, *RPP* has learned, occurred sometime in 2013. CHCS owned six nursing homes at the time of the theft.

OCR said it received "separate notifications from each of the six nursing homes regarding a breach of unsecured electronic protected health information (ePHI) at CHCS" in February 2014, and that it began its investigation on April 17, 2014. But, as in most, if not all, of OCR's settlements, the agency found widespread noncompliance once it started digging.

Although OCR has had the authority to bring enforcement action against CEs for more than 10 years — including for lack of a business associate agreement and for misdeeds by BAs — BAs are relatively new to being held fully liable for compliance.

continued on p. 9

Ohio Respiratory Therapist Is Convicted on Rare Criminal Charges Under HIPAA

A federal jury in Ohio on June 23 convicted a 26-year-old respiratory therapist on misdemeanor charges of unlawfully obtaining individually identifiable health information under HIPAA. The case is a rare criminal conviction for a HIPAA violation, especially considering there are no accompanying charges of fraud or identity theft.

Jamie Knapp, a former certified respiratory therapist at ProMedica Bay Park Hospital in Oregon, Ohio, was convicted of accessing nearly 600 records outside the scope of her job between April 2013 and April 2014. Knapp, who has yet to be sentenced but faces the possibility of one year in jail, claimed she received permission from a superior to study the records in preparation for an upcoming clinical simulation that July, but the supervisor denied doing so.

Then, in two incidents in March and April 2014, coworkers became suspicious of Knapp after seeing her with a sharps container, which holds used needles and medication vials, *The Blade* reported. On the second occasion, Knapp was asked to empty her

pockets, revealing a needle and tourniquet. Knapp then refused to take a drug test and quit.

But David Goldstein, Knapp's attorney, says Knapp passed a polygraph test on the question of whether she had received permission to view the files — a fact that was excluded from the trial because polygraph tests are not admissible in court — and that it's common for hospital workers to keep things in their pockets. Knapp also told *The Blade* that she refused a drug test because she was afraid that nicotine would show up, which she said could be grounds for termination.

Knapp also claimed she was reviewing records because she had been told that some patients had been receiving the wrong medications because of spotty documentation, which Goldstein says accounted for her activities from the time of her exam in July up until her resignation in April 2014.

"She understands now that the law is much more complex and much more difficult than she probably imagined at the time. But I don't think she had any criminal intent or bad intent in doing what she did," Goldstein tells *RPP*, adding that he's disappointed in the verdict. "She just made some bad choices."

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, Theresa Defino; Executive Editor, Jill Brown; Associate 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** (**$554 bill me; $524 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.

Although the prosecution insinuated that Knapp was accessing records in order to obtain drugs, no drug-related charges were levied against her. In fact, local police initially decided not to pursue any charges at all because they couldn't gather enough evidence. Her eventual conviction stems from a subsequent investigation by the FBI.

Other Cases Involved Malicious Intent

Although cases like Knapp's are rare, hers is certainly not the first. For example, in May 2015, a drug dealer in Alaska was sentenced to the maximum of 10 years apiece for two separate HIPAA violations involving people he had injured, one of whom he had kidnapped and tortured *(RPP 4/16, p. 5)*. His friend, who worked at the hospital where the victims sought care and who texted him information about the victims' conditions, received two years in prison. In February 2015, a Texas hospital employee pleaded guilty to criminal HIPAA charges after being discovered with patient information in an apparent attempt to use the data for financial gain *(RPP 8/14, p. 4)*.

And in 2004, an employee of a Seattle cancer clinic was the first individual to be convicted on criminal HIPAA charges, when he went on a $9,000 shopping spree with a patient's credit card information. That case eventually prompted the Department of Justice, through the use of an advisory "opinion memorandum," to broaden the law's scope to include employees of a covered entity, as well as individuals who don't work for a covered entity at all, as in the Alaska drug dealer case.

"The bit of good news for HIPAA covered entities and business associates is that these criminal cases have not been brought with respect to your wrong interpretations of the law — wrong but well-meaning," says Reece Hirsch, partner in San Francisco office of Morgan, Lewis & Brockius LLP. "They've really been brought when bad conduct is occurring — serious, egregious misuses of personal information."

But Knapp wasn't arraigned on any charges of identity theft or fraud, which makes her case even more unusual, even though authorities occasionally take the HIPAA route when other crimes have been committed, too. Jeff Drummond, a partner in the Dallas office of Jackson Walker L.L.P, noted that, in the case of the Texas hospital employee, prosecutors could have pursued any number of fraud charges, but instead opted for HIPAA. "They could have gone after him for all kinds of things," he says, "and they went after him for HIPAA."

Changes in the HITECH Act of 2009 made it easier to bring a criminal case against individuals under HIPAA and memorialized the DOJ memorandum *(RPP 7/11, p. 1)*. Drummond says the language of 42 U.S. Code §1320d-6 is unclear, and that the HITECH Act

was a "hastily" and "sloppily" written statute. He says he hopes future defendants will challenge the law's wording.

"When it comes to criminal law, where one's property or liberty can be removed by the state, there cannot be a 'well, you know what I mean' quality to it," he tells *RPP*. "Criminal statutes in particular must be clearly and precisely written. If there is any ambiguity, and there certainly is here, the benefit of the doubt must go to the accused."

Goldstein says he hasn't discussed the option of an appeal with Knapp, but says that, if she does appeal, she likely will have to request a court-appointed lawyer for financial reasons. Knapp faces up to one year in prison and a fine of $50,000.

Michael Bossenbroek, a partner in Michigan-based Wachler & Associates, P.C., says that while it's "pretty unusual" for a case like Knapp's to proceed to a full jury trial and conviction, he believes the penalty is appropriate in instances of criminal intent.

"Here, it could be the case that the defendant wasn't brought to trial simply for inappropriate access to PHI, but that she [may have had] bad motivations for doing so, even if she wasn't separately charged for those other activities," he says.

But Goldstein says the possible penalty is "absolutely" too harsh in Knapp's case, and hopes she will receive a sentence less than the maximum of one year in prison..

"I'd like to say no," Goldstein says, but adds that he can't predict what the judge will do. "I would think not."

Contact Bossenbroek at mbossenbroek@wachler.com, Drummond at jdrummond@jw.com, Goldstein at davidgoldstein.law@gmail.com and Hirsch at rhirsch@morganlewis.com. ✧

When Asked, Covered Entities Must Give Patients Records by Email

Raise your hand if your organization prohibits workers from emailing protected health information (PHI) outside your walls. You've probably spent oodles of money on software, IT fixes and training to make sure this doesn't occur, right?

Keep your hand up if you know that patients who request their medical records by email — unencrypted no less — can receive them this way.

Did your hand just go down? Not if you work for Carolinas Healthcare System, which operates hospitals in North and South Carolina. Carolinas makes it easy for patients to request their medical record by email. It even gives them an option of "other" to fill in how they want their records, if an email, CD or snail mail package won't do.

But judging by record request forms posted on the Internet, Carolinas is in the minority. Many covered entities (CEs) haven't yet come to grips with the fact that, since September 2013, the final rule implementing the HITECH Act has mandated that patients can receive test results, health information and other documents from their designated medical records set by email.

The time is now to make policy and IT adjustments to allow this. In recent guidance, the HHS Office for Civil Rights (OCR) has made it clear that this is a patient's right and that putting obstacles in a patient's way "must change."

Deven McGraw, OCR's deputy director, tells *RPP* in an interview that while she "very much appreciates the steadfastness of security teams" who oppose unsecure email as a way to send records, the requesting patient "gets it in the way she wants."

It doesn't matter whether the CE has a policy against emailing to patients; if the CE has the capacity, McGraw stresses, then it must comply. "We assumed in every institution there is a capacity" to send PHI unencrypted via email, McGraw says.

She also states that allowing unencrypted emails with PHI upon patient request isn't a "slippery slope."

"We are trying to make it as easy as possible [for people] to exercise their HIPAA rights in a way that works best for them. But it is not meant to be a sort of blanket, 'Get Out of Jail Free' card on security," says McGraw.

She acknowledges this is a distinction that "some people haven't quite grasped."

Guidance Is Clear on Email

Earlier this year, OCR addressed fees as well as what kinds of information patients could receive through records access requests *(RPP 6/13, p. 3)*. It states that a CE "must provide access in the manner requested by the individual, which includes arranging with the individual for a convenient time and place to pick up a copy of the PHI or to inspect the PHI (if that is the manner of access requested by the individual), or to have a copy of the PHI mailed or e-mailed, or otherwise transferred or transmitted to the individual to the extent the copy would be readily producible in such a manner."

In addition, the guidance mentions email as an option in several instances (emphasis added below):

◆ CEs "are not then permitted to require individuals to purchase a portable media device from the covered entity if the individual does not wish to do so." In such cases, the person may "opt to receive an alternative form of the electronic copy of the PHI, such as through *email*."

continued

◆ CEs can allow individuals to use an electronic means to request access to their medical records, "e.g., *e-mail*, secure web portal."

Of course, policies must be communicated to patients. CEs need to let patients know that email is an option, and should provide some flexibility on request forms to ensure compliance with the form and format requirement. They can list email as an option, provide an "other" category, or do both, as Carolinas does.

It also provides a series of choices to help narrow down what information the patient is seeking, with categories for facilities, clinical offices and behavioral health. Patients can also choose whether they want a CD, email, paper copy or other, and then they select the mode of transmission — mail, secure email, fax or ask the system to "prepare them to be picked up by" a person of their choosing.

For more information, see www.carolinashealthcare.org/for-patients-visitors/medical-records.

For Some, This Is a 'Nightmare'

But CE "are between a rock and a hard place" on this issue of emailing records, says Patricia Wagner, a member of the law firm of Epstein, Becker & Green, P.C.

Wagner says meeting the requirement for access by email could be a "compliance nightmare." At a minimum, "policies have to be revised" at CEs who have forbidden PHI from being emailed.

Focusing on the requirement to provide records access by email, if requested, might give CEs a chance to hone their email policies.

David Holtzman, vice president of compliance strategies for CynergisTek, says there really isn't a "state of the art" yet on standard email practices, calling CEs "all over the place" with regard to policies and safeguards.

"Some organizations have sophisticated technologies that will automatically identify communications based on preset characteristics, and, once identified, will encrypt or otherwise secure the PHI in transmission," Holtzman says. "Others have taken the approach of behavioral and administrative controls that prohibit the sending of PHI via email."

He adds that those that "rely on administrative and behavioral approaches can probably comply with these requests more easily," but they will have to "manage the process" carefully.

Management doesn't come easy, as a major Pennsylvania health system experienced first hand. In 2010, a gastroenterologist with Geisinger sent a single unencrypted email to his home computer that contained data about patients to do follow-up work at home.

The action violated two policies. The system banned the sending of emails from work accounts to personal accounts, whether they contain PHI or not. It also mandated that any emails containing PHI that are sent from Geisinger email accounts must be encrypted; employees had to individually activate by inserting a command in the subject line. The physician was terminated and Geisinger had a reportable breach of data for 2,928 patients on its hands *(RPP 2/11, p. 1)*.

There Are Many Practical Considerations

Whether the CE will provide secure or unsecure email transmissions is another factor it must consider. A secure email that makes it difficult, if not impossible, for patients would draw OCR's rebuke, as McGraw indicates to *RPP*.

"In my opinion, I don't think the guidance prohibits securing the [email] transmission," Holtzman says. "I think what is prohibited is creating barriers for individuals to access the information, so if you have a security program that is unobtrusive or does not require action by the individual to retrieve or view their email or the attachment, I think that complies," he says.

Holtzman notes that CEs may be able to utilize "technologies that secure [the email], encrypt and decrypt it without any action by the recipient."

Once new policies are in place, the challenge for CEs is to ensure that workers understand the communication with patients and other individuals making such requests is really a "narrow exception," Wagner says.

Emailing unsecured PHI for other purposes is still verboten, unless the CE's risk analysis shows some other method of security is in place, likely a doubtful situation.

Policies for fulfilling records requests need to address "when it is okay to email the file and when it's not," Wagner says. Policies still can stress that secure communication can occur through a portal, if the CE has one, but as the guidance makes clear, a portal is not a substitute if the patient doesn't want to, or can't, use one.

For CEs that have a blanket prohibition on emailing PHI and can't, or don't want to, make IT adjustments, McGraw suggests that designating a single employee or several who have special authorization to email PHI.

Another requirement is to ensure that those requesting the records are entitled to them, and that their identities and their correct email address are verified. Furthermore, CEs also have an obligation to warn patients of the inherent risk in email communications. Carolinas provides a document listing these concerns, which is available at http://tinyurl.com/jjemrex.

"We have always advised our clients to make sure the patient understands [email] is not secure," Wagner adds.

After the access guidance came out, the Medical Group Management Association sent its members a recap of patients' access rights and requirements for physicians, says Rob Tennant, MGMA's health information policy director.

He encourages providers to talk to patients directly about their request so it "becomes a negotiation." In some cases, "you can't use standard approaches," Tennant says. "People come in their own media" that they want the CE to put the records on, yet these may present an unacceptable security risk and a possible HIPAA violation.

USB Flash Drives Are an Option

One option is to purchase USB flash drives, which have dropped considerably in price over time. Organizations can buy them in bulk and have their logo imprinted on them, and patients seem to like them, he says.

Tennant says MGMA stresses imposing minimal fees and "really trying to hone in on what the patient wants."

These strategies can help make the records request process smoother for both the provider and the patient, and ultimately stave off every privacy officer's nightmare — a conflict that can spur a complaint to OCR.

Wagner called patients' desire for health data "a shifting landscape, with privacy officials — and providers — along for the ride.

"Patients want communication through email, they want more mobile access, and it is something CEs have been struggling with for a while. They are going to have to get comfortable [with more sharing] and figure out where the boundaries are," Wagner says.

Contact McGraw at Deven.McGraw@hhs.gov, Wagner at pwagner@ebglaw.com, Holtzman at david.holtzman@cynergistek.com and Tennant at rtennant@mgma.org. ✧

Uncle Sam 'Needs You' (to Share Information on Cyberthreats)

Last month, the U.S. government announced the availability of the Automated Indicator Sharing (AIS) system to better equip both federal agencies and private organizations to thwart and mitigate cyber attacks.

AIS — no relation to Atlantic Information Services, publisher of *RPP* — is part of the implementation of the Cybersecurity Information Sharing Act (CISA) of 2015, which also called for a taskforce to focus solely on health care. The taskforce holds its second meeting this month.

In joint guidance, the Departments of Homeland Security (DHS) and Justice (DOJ) explained how threats could be shared. HIPAA security officers should review the processes for sharing threats as well as receiving intelligence — all of which is available at no cost.

"The more information like this is shared, the better for targets of cyberattacks," says David Harlow, principal with the Boston health care law and consulting firm The Harlow Group, LLC. Covered entities "may be motivated to share information in order to try to reduce the effectiveness of cyberattacks first experienced in one location, before it can be spread to many."

The guidance also explains that "while there is liability protection for those who file reports, there is also an obligation on the reporting entity to ensure that no PHI is reported, since the threat indicators and defensive measures" may be publicly shared, he says. "Failure to de-identify will result in the loss of the liability protection."

He notes that reporting about threats to others is protected; "otherwise competitors sharing information like this might be considered an antitrust violation."

But they are likely to be torn, he adds. Most CEs "are loath to report that they have been attacked, and may fear that the detail associated with the report will provide clues to potential attackers about their systems and existing defenses and vulnerabilities."

However, the government promises anonymity for those who desire it.

HHS "embraces the recently released DHS/DOJ guidance," HHS Acting CIO Beth Killoran told *RPP* in an email. "The Administration, and HHS, believe strongly that rapid information sharing across the private sector and between the private sector and government is an essential element of effective cybersecurity, because it enables U.S. companies to work together, and work with the federal government, to quickly identify, protect against, and respond to cyber threats," Killoran said.

There Are Three Ways to Share

The new guidance offers three ways to share a threat with the federal government and lengthy explanations for all of them: web submissions, the AIS system and emails. The government prefers the AIS system, which "allows bidirectional sharing of cyber threat indicators," meaning users "will not only receive DHS-developed indicators, but can share indicators they have observed in their own network defense efforts, which DHS will then share back out to all AIS participants."

continued

This method of sharing threats is "strongly preferred since it encompasses a real time, machine-to-machine exchange that supports a higher volume of cyber threat indicators and defensive measures."

Participants Will Be Anonymous

DHS promises that those "who share information through AIS will not be identified as the source of those indicators to other participants unless they affirmatively consent to the disclosure of their identity."

As the agency clarified, "you are anonymous unless you want us to share your name." Cyber threat indicators and defensive measures it receives will be "analyzed, and sanitized" and then shared "with all AIS participants."

But there is a little bit of buyer-beware. What is passed along will "not be validated by DHS as the emphasis is on velocity and volume: our partners tell us they will vet the indicators they receive through AIS, so the Department's goal is to share as many indicators as possible as quickly as possible."

But DHS says it may assign a "reputational score… when the government has useful information about an indicator, "although it does not explain what this means.

Data received by web submission and email "will be forwarded to DHS cyber threat analysts to determine if there is valid cyber threat indicator or defensive measure information, and after review (including a review to determine whether the cyber threat indicator or defensive measure contains any personal information of specific individuals or information that identifies specific individuals that is not directly related to the cybersecurity threat)."

For more information, visit www.us-cert.gov/forms/share-indicators.

The government asks that if the submission is about malware that a different form be used (see http://malware.us-cert.gov/MalwareSubmission/pages/submission.jsf).

Contact Harlow at david@harlowgroup.net. ✧

Health Care Leads All Industries in The High Cost of Data Breaches

Data breaches cost health care organizations worldwide an average of $355 per record and U.S organizations $402 per record, leading other industries by a hefty margin, according to a June 15 report sponsored by IBM Security and conducted by the Ponemon Institute, LLC.

Education was the second leading industry, globally speaking, trailing health care at $246 per record, a significant $109 differential, according to the *2016 Cost of a Data Breach Study*. Data breach costs increased from $3.79 million worldwide in 2015 to $4 million in 2016, with organizations spending an average of $158 per record, marginally up from $154 last year. On the whole, the cost of data breaches increased 5.4%, while the per capita cost ticked up 2.9%.

Of the 12 countries included, the U.S. ponied up the most for each compromised record, paying $221 on average, or $7 million per organization, while Germany paid $213 per record and $5 million per organization. According to the report, health care pays a higher price in part because of the industry's heavy regulations — which result in more fines — and because the industry suffers from a bigger loss of customers when a security incident occurs.

But U.S. customers aren't as sensitive to breaches as customers in France, Italy and Japan, which reported the highest loss of business following an incident. Still, the U.S. paid the highest price for lost business, with an average of $3.97 per record. U.S. organizations also had the highest percentage of indirect costs, at 66%, and paid the most in terms of notification costs, averaging 59 cents per record. India, by comparison, paid the least for notification costs at 2 cents per file. But the U.S. paid among the least for detection and escalation costs at 73 cents per capita, while neighboring Canada had the highest expense at $1.60.

Causes Vary by Country

From January 2015 to March 2016, Ponemon surveyed 383 companies in 12 countries across the globe, all of which had experienced a data breach of approximately 3,000 to 102,000 records. Interestingly, India led the world in the average number of breached records at 31,225, while the U.S. came in third at 29,611.

While the majority of incidents were malicious in nature, that wasn't true for every country. The "Arabian cluster" (Saudia Arabia and United Arab Emirates) experienced the most criminal attacks at 60%, while the U.S. fell somewhere in the middle at 50%. South Africa reported the lowest incidence of malicious breaches at 37%, and the highest incidence of human error at 37%.

The nature of the breach factored into the subsequent expense — malicious attacks cost $170 per capita, on average, while system glitches and human error cost $138 and $133, respectively. In the U.S., those costs were much higher, as American organizations shelled out $236 per record on average for criminal attacks, $213 for system glitches and $197 for human error. One important component of the associated costs is the time it takes to identify the exposure after the incident occurs, which is much shorter in instances of glitches or human error.

Other factors impacted the total cost as well. The rising overall cost of data breaches was attributed to a 3.2% increase in the number of compromised records and a 2.9% increase in the amount of lost business. The use of incident response teams, however, resulted in a $16-per-record decrease, totaling $400,000 in savings, on average. In the U.S., the savings were even larger, with incident response saving nearly $26 per record. Increased encryption also made a significant difference, accounting for a $13-per-record decline overall and a $19 savings for U.S. companies.

Download the Ponemon Institute's full report at http://tinyurl.com/py4l96s. ✧

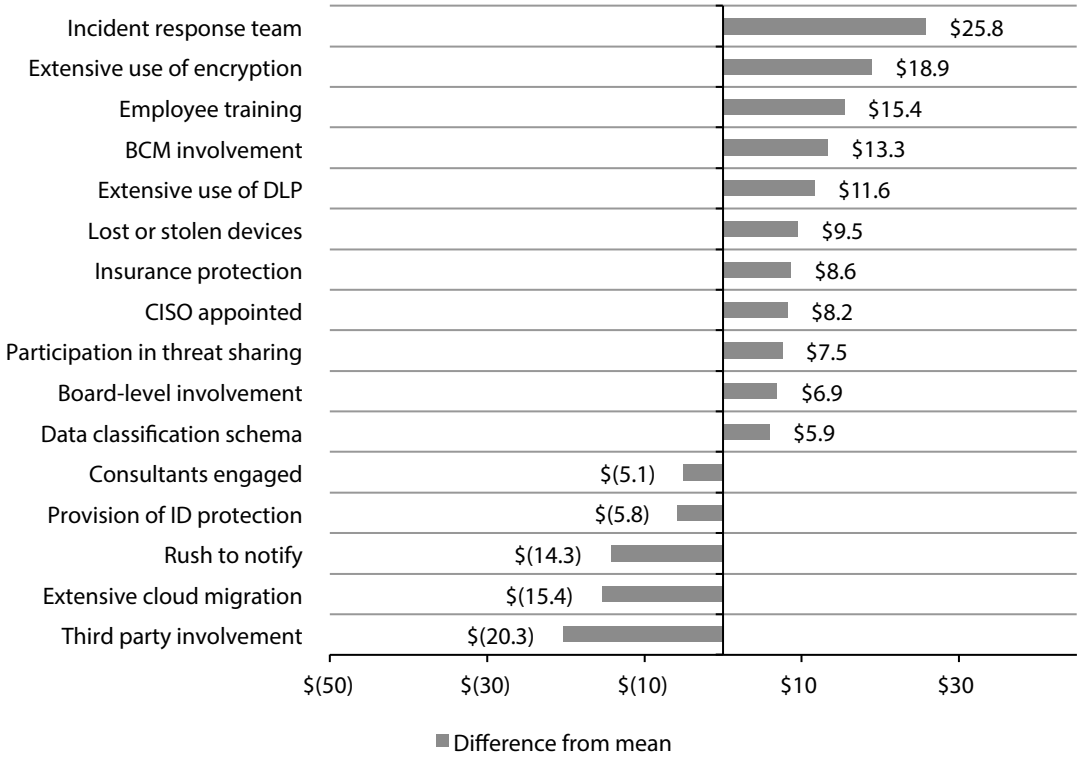
States Update Breach Notice Laws To Include Biometric, Login Info

As the health care industry continues its glacial conversion to digital records, states are amending data breach notification laws to expand the definition of "protected information" and tighten reporting deadlines. The laws come as the use of biometric identifiers continues to grow, with health care organizations using them as a means of authentication in the waiting room. One state — Tennessee — even removed the encryption safe harbor protection afforded by HIPAA. Below is a round-up of recent actions.

◆ ***New York:*** Bill A10475, currently pending in the state assembly, would update the definition of "private information" to include biometric data used for authentication purposes, such as eye scans, voice identification or fingerprints, as well as email addresses or usernames in combination with passwords or answers to security questions. In the event that a combination of those data is leaked, organizations would be required to notify consumers about the breach through means other than email, since their email accounts could be compromised.

continued

Impact of 16 Factors on the Per Capita Cost of Data Breaches



SOURCE: Ponemon Institute's *2016 Cost of Data Breach Study*, sponsored by IBM

The law would also include protected health information from covered entities, and increase the penalty for each failure to notify from $10 to $20 per person, upping the maximum fine from a total of $150,000 to $250,000. Additionally, organizations would be required to provide relevant contact information for identity theft response and credit monitoring, and provide a template of the notice to the state attorney general. If the breach affects more than 5,000 residents, organizations would be required to alert credit monitoring agencies as well. The changes would take effect Jan. 1, 2017. Read the bill at http://tinyurl.com/jkvcjwe.

◆ ***Illinois:*** In May, Gov. Bruce Rauner (R) approved HB 1260, which amended the state's Personal Information Protection Act by clarifying that there is no safe harbor protection for breaches of encrypted data when the decryption key is likely exposed as well. Effective Jan. 1, 2017, the law also defines "health insurance information" to include any unique patient identifiers used by insurers, as well as any information in the patient's application or claims history, including appeals. Medical information now includes data supplied to a website or mobile app, and biometric data used for authentication purposes are now considered protected information, as is login information.

Interestingly, the law specifically allows organizations to omit the number of affected people in their notifications to customers. Additionally, it allows them to report the breach to local media only, rather than statewide media, if the breach affects individuals within a specific geographic area. At the very end, the law states that organizations in compliance with HIPAA or HITECH will be deemed compliant with the state law, as long as they notify the attorney general within five days of notifying OCR. For additional information, read the law at http://tinyurl.com/zx94lo7.

◆ ***Nebraska:*** Gov. Pete Ricketts (R) in April enacted LB835, expanding the definition of "personal information" to include usernames and email addresses when exposed along with passwords or security question answers. The law also clarifies that there is no safe harbor for encrypted data if the decryption key is believed to have been leaked as well. Additionally, organizations are required to notify the attorney general about security

PATIENT PRIVACY COURT CASE

This monthly column is written by Jenny Harrison of Morgan, Lewis & Bockius LLP in San Francisco. 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 Jenny at jenny.harrison@morganlewis.com.*

◆ **Hawaii Supreme Court finds de-identified medical records are protected by the Hawaii Constitution.** On June 13, the Hawaii Supreme Court ruled that the state constitution's privacy policy protects patients' medical records, even when de-identified, from disclosure when the patients are not parties to the litigation and there is no compelling state interest in disclosure. In his concurring opinion, Chief Justice Mark E. Recktenwald agreed with the decision, but noted that HIPAA may preempt the holding to the extent that the decision prevents the disclosure of de-identified medical records. He noted that federal courts have determined that de-identified medical records are not individually identifiable health information. Therefore, such records do not fall under HIPAA's preemption exception for more stringent state laws and future cases may raise federal preemption issues. The medical records at issue were requested in an action between plaintiffs, Pacific Radiation Oncology (PRO) and several doctors, and defendants, Queens Medical Center and Queens Development Corporation (collectively QMC). PRO initially sued QMC in the U.S. District Court for the District of Hawaii, challenging QMC's decision to allow only QMC physicians to provide radiation oncology services at its facilities. PRO alleged this was an unfair trade practice designed to force PRO to forego ownership in the Cancer Center of Hawaii (TCCH). In its counter-claim, QMC alleged that the plaintiff doctors steered patients from QMC to TCCH without disclosing their ownership interests in the facility. During discovery in this action, QMC publicly filed a list of 132 patients that were allegedly diverted to TCCH and requested production of their medical records. The court denied the patients request to block the disclosure, finding that the records were discoverable if the information was de-identified. The Hawaii Supreme Court disagreed, holding that Article I, Section 6 of the Hawaii Constitution protects "confidential patient medical records, even if sufficiently de-identified, in litigation where the patient is not a party [and] no compelling state interest has been shown." However, as the Chief Justice warned, this result regarding de-identified data may be preempted by HIPAA. *Pac. Radiation Oncology, LLC v. Queen's Med. Ctr.*, No. SCCQ-15-0000300, 2016 BL 187654 (Haw. 2016).

incidents. The changes go into effect July 20. Read the law at http://tinyurl.com/gqnapfx.

◆ ***Tennessee:*** Gov. Bill Haslam (R) in March signed SB2005 into law, effectively removing the safe harbor protection for breaches of encrypted information. As of July 1, organizations will be subject to reporting requirements regardless of whether the exposed information was encrypted or unencrypted, and will be obligated to notify consumers within 14 days of discovery unless more time is needed by law enforcement. Read the law at http://tinyurl.com/zm6bqma.

Visit https://patientprivacyrights.org/privacy-laws-by-state for summaries of privacy laws by state and links to the websites of all state legislatures. ✧

First Settlement Reached With a BA

continued from p. 1

According to OCR, the compliance date for BAs was September 23, 2013; they must comply with the security rule and some of the privacy rule. If the theft had occurred prior to that date, OCR could not have pursued CHCS.

Little is known about the theft beyond the few details in the settlement and a statement CHCS provided to *RPP*. Under the breach notification rule, because the data of fewer than 500 patients were involved, the nursing homes were not required to make a public announcement; the theft does not appear, for example, on OCR's so-called "Wall of Shame" (see https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf).

OCR said the "information on the iPhone was extensive, and included Social Security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information."

At the time of the breach, the organizational structure was such that CHCS "provided management services to and was the sole corporate parent of [the] six nursing homes," OCR said.

In an email in response to questions from *RPP*, OCR Deputy Director Deven McGraw said that, in "any case involving multiple parties, OCR, as part of its investigation, determines which entity or entities are responsible for the noncompliance. The allegations of noncompliance in this case are with respect to the business associate, CHCS."

In a statement announcing the settlement, OCR said the dollar amount took into account the fact that "CHCS provides unique and much-needed services in the Philadelphia region to the elderly, developmentally disabled individuals, young adults aging out of foster care, and individuals living with HIV/AIDS."

As required by the enforcement rule, OCR assesses "both mitigating and aggravating factors, which we evaluate in determining the penalty amounts and settlements in all of our cases," McGraw said.

In this instance, "we considered both the role that CHCS plays in its community as well as the level of sensitivity of the data and the nature of the alleged violations when determining the penalty amount and settlement," she said.

Settlement Is Called 'Amicable'

As of November 2014, CHCS no longer owned the homes, an assisted living facility and an "adult medical day care program," having sold them to Center Management Group, owner of more than a dozen nursing homes in New Jersey and New York, CMG and the archdiocese announced at the time.

Ken Gavin, spokesman for the Archdiocese of Philadelphia, declined to answer any of *RPP*'s questions and instead provided the following statement, which indicated that the breach did not seem to result in misuse of patient data.

"Catholic Health Care Services has reached a voluntary and amicable settlement with the U.S. Department of Human Services, Office for Civil Rights, resolving the theft of an employee's company iPhone in 2013. There have been no reports of unauthorized access to patient information on the stolen iPhone, and all individuals that may have been affected were timely notified. Since the theft, CHCS has taken corrective measures and remains committed to complying with HIPAA and diligently safeguarding its clients' protected health information while serving the greater Philadelphia community."

CHCS "had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan," the agency said.

OCR said CHCS is still serving as a business associate to another organization, namely Catholic Clinical Consultants (CCC), a "faith-based, multidisciplinary behavioral health team." It is not clear what functions CHCS provides on behalf of the behavioral health firm. According to CCC's notice of privacy practices, it may disclose PHI "in the course of our businsess (sic) operations. For example, we may use your PHI in evaluating the quality of services provided, or disclose your PHI to a HIPAA-defined business associate such as our accountant or attorney for audit purposes."

CEs, BAs and the HIPAA consulting and compliance community have been waiting for OCR to bring an enforcement action against a business associate, and many

expected such action would involve both the CE and BA jointly.

In fact, then-OCR Director León Rodríguez told *RPP* in 2012 that was the likely approach. "Once we have our rule and we are in the business of enforcing against BAs, I think it is entirely possible, if not in fact likely, that you are going to have cases where we do enforce against both the CE and the BA," he said. "You can readily imagine that there is a scale here — that there are going to be cases where culpability is shared equally between the CE and BA and in other cases where it might be more heavily found on one side or the other" *(RPP 4/12, p. 1)*.

OCR's press release and the resolution agreement are silent as to whether the nursing homes were in compliance or not; the only mention of the homes is in reference to the actual loss.

In response to *RPP*'s query as to what the CE's responsibility was to assure compliance by its BA, McGraw said there is no "single answer to that question." Agency officials "evaluate these cases based [on] their facts," and OCR's investigation "determined that the business associate, CHCS, was not in compliance."

According to Mac McMillian, president of the HIPAA consulting firm CynergisTek, OCR, in general, cannot pursue sanctions against a CE when a BA is involved in a breach or possible violation except in two instances — when there is no business associate agreement (BAA) or when the CE knows of noncompliance or should have known and takes no action to correct this situation, including severing the relationship.

In fact, it was the absence of a BAA, as well as other failures, that cost North Memorial Medical Center of

New CAP Shows Policies Needed by Business Associates

In this case (see above), the phone belonged to a worker for Catholic Health Care Services (CHCS), part of the Archdiocese of Philadelphia, and the data came from patients at nursing homes it owned. OCR considered CHCS at fault, settling its investigation with a $650,000 financial payment and a two-year corrective action plan (CAP).

While CAPs are specifically designed for individual entities to bring them into compliance, they also hold great use as a blueprint for others to follow as they embody what OCR thinks are best practices.

The June 30 CAP, in particular, can serve as a handy checklist for any CE to ensure that its BAs have the required policies and procedures.

The CAP calls for CHCS to conduct an annual, "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of e-PHI held by CHCS" and to "document the security measures CHCS implemented or is implementing to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level."

In addition, the CAP gave CHCS five months to write policies and procedures that address:

- Encryption of ePHI
- Password management
- Security incident response
- Mobile device controls
- Information system review
- Security reminders
- Log-in monitoring
- Data backup plan
- Disaster recovery plan
- Emergency mode operation plan
- Testing and revising of contingency plans
- Applications and data criticality analysis
- Automatic log off
- Audit controls
- Integrity controls

Although CHCS has since sold the nursing homes and is no longer their BA (or corporate parent), OCR said CHCS is still serving as a BA to another organization, namely Catholic Clinical Consultants (CCC), which describes itself as a "faith-based, multidisciplinary behavioral health team."

Further, OCR required CHCS to provide the agency with copies of all of the BAAs that it has with CEs and "copies of its management services agreements" with CEs.

Training is also part of the CAP, with employees required to receive training on any new policies "within 30 days of HHS approval of such policies and to new members of the workforce within 14 days of their beginning of service."

In addition, "CHCS shall review the training at least annually, and, where appropriate, update the training to reflect changes in Federal law or HHS guidance, any issues discovered during audits or reviews, and any other relevant developments," the CAP states.

Minnesota $1.55 million in a settlement earlier this year *(RPP 4/16, p. 4)*. An organization acting as a BA — but lacking a BAA — experienced the theft of an encrypted laptop in July 2011 that contained PHI for 9,500 North Memorial patients. Without a BAA, North Memorial "impermissibly disclosed the PHI of at least 289,904 individuals," according to OCR.

Occurring prior to the compliance date for BAs, OCR pursued action only against North Memorial, and not Accretive Health, a quality assessment agency.

Still, the lesson in the settlement is much the same regardless of who is at fault, says McMillan. In fact, when he heard that an encrypted device was at the center of the settlement, he assumed a laptop was the issue.

"I am a little surprised that they picked this one" to be the first BA enforcement action, McMillan says. "Apparently this was the first one they thought they could get to closure on." A search of OCR's online database of breaches indicates there were approximately 120 breaches from Sept. 23, 2013, to July 5 of this year that involved BAs.

But even though it's a first for a BA, "it's the same old story," McMillan says — mobile devices should be encrypted, period. "It may be the first one involving a phone but they are all mobile devices," he says. "My iPhone is encrypted. The lesson could be there are people out there who don't think about phones and they need to." Consider creating "sectors on the phone that are encrypted and protected" if the whole phone is not.

It may not have been "reasonable" for the nursing homes to know that the CHCS employee was using an unsecured phone, he adds. If a BA had said "we don't put your data on our phones, then the CE would have no reason to suspect their data was at risk." OCR "can absolutely hold the BA responsible for the breach," but perhaps not the CE. "This is one of the problems with the [security] rule," he emphasizes.

McMillian contends that "in most any other industries" the nursing homes, as the "owners" of the data, would still be held to account. "The data belongs to the CE, he says. "The BA is merely providing some kind of service and has access to the data, but the data doesn't belong to the BA."

He argues that in banking, energy and other industries, the CE "would still be responsible for the data. But in health care, all you have to do is sign a BAA."

The idea of holding BAs directly liable, which came about under the HITECH Act, was seen as a way to close this loophole. But because there's no real joint accountability, big gaps in security remain.

"It's a bad rule. There is nothing that says the CE has to ensure that the BA has done a risk assessment, or other requirements in the BAA," McMillan says. Because CHCS was the corporate parent of the homes, nursing officials could have been in an awkward and weakened position if they had to call CHCS on the carpet.

McMillian and others have been pushing for a wholesale rewrite of the security rule and other data protection regulations, a battle they lost when Congress passed a "watered-down" law last year. A mandatory "framework" turned into a "voluntary" one in some drafts of the Cybersecurity Information Sharing Act.

Contact McGraw at Deven.McGraw@hhs.gov, Gavin at kgavin@archphila.org and McMillan at mac.mcmillan@cynergistek.com. ✧

PRIVACY BRIEFS

◆ **IBM Security and Ponemon Institute LLC on July 1 unveiled a data breach calculator to help organizations determine the potential cost of a security incident.** The calculator is a quick questionnaire that analyzes the size and privacy practices of a company, asking about past data breaches and current incident response plans. Visit www.ibmcostofdatabreach.com to try the calculator.

◆ **Massachusetts General Hospital (MGH) on June 29 said that data for nearly 4,300 patients were accessed through a third-party vendor,** the *Boston Herald* reported. In a statement on its website, MGH said that, in February, it discovered that an unauthorized person had accessed some dental patients' electronic files through a contractor, Patterson Dental Supply Inc. Compromised data included names, dates of birth, appointment information, provider names, medical record numbers and Social Security numbers. Visit http://tinyurl.com/jxd2wls.

◆ **States are enacting laws to protect dependents' personal health information from policyholders,** Kaiser Health News reported. The changes come as more children are taking advantage of the ACA's opportunity to remain on their parents' policies until the age of 26. While HIPAA allows individuals to request that insurers refrain from sending explanations of benefits to policyholders, insurers are not required to do so. California, Colorado, Maryland, Oregon and Washington are among those who have enacted reforms. Visit http://tinyurl.com/hfck6ol.

PRIVACY BRIEFS (continued)

◆ **Hospital workers routinely circumvent password restrictions,** according to a report from a team of researchers at the University of Pennsylvania, Dartmouth College and the University of Southern California. The study found that hospital staff regularly wrote down passwords, building "sticky stalagmites" of Post-It notes on medical devices and in prep rooms. The researchers said they found that entire hospitals often share one password to a medical device, and that emergency supply rooms often have the entry code written on the door. Read more at http://tinyurl.com/jn8tt7x.

◆ **A hacker has reportedly posted 655,000 PHI records from three hospitals and 9.3 million records from a major insurer up for sale,** multiple outlets reported on June 27. Security blogger Dissent Doe wrote on databreaches.net that at least some of the records appear to be old, having followed up with individuals in a sample the hacker provided for verification. Reporters at Motherboard were able to verify the information of some other individuals from the purported hospital records. The hacker, who goes by the name thedarkoverlord, said he has already sold some of the information and is declining to name the organizations unless they refuse to pay a ransom. Visit http://tinyurl.com/h3ahwhj.

◆ **Seven employees at Ohio-based ProMedica Bixby and Herrick Hospitals were disciplined or terminated following the revelation that they had improperly accessed approximately 3,500 patient records.** In a June 24 statement, the health system said it does not appear that the employees meant to use the information inappropriately, and told *The Blade* that it determined none of the records were printed out. The announcement comes on the heels of another former employee's conviction on HIPAA charges for improperly accessing nearly 600 records (see story, p. 1). Visit http://tinyurl.com/hw546g3.

◆ **Office of the National Coordinator for Health IT Chief Privacy Officer Lucia Savage indicated HHS might copy the Dept. of Defense's ethical hacking program to help shore up the health care industry's cyber defenses,** the *Federal Times* reported on June 23. The DoD program offers rewards to hackers who locate weaknesses in the agency's defenses. Savage's comments came at a Collaboration of Health IT Policy and Standards Committee meeting, where she said the practice was a topic of discussion at an FDA meeting on medical device cybersecurity. Visit http://tinyurl.com/jlb4tkb.

◆ **Ransomware attacks worldwide between April 2015 and March 2016 increased by nearly 18% over the previous 12-month period,** according to a June 22 report from data security vendor Kaspersky Lab. In spite of the recent string of high-profile ransomware attacks, home users still are overwhelmingly the main target of ransom-seeking hackers, accounting for a whopping 93% of cyberattacks. In the U.S., only 2% of users experiencing a cyberattack were hit with ransomware. Visit http://tinyurl.com/jb2a9yv.

◆ **In a lawsuit filed on June 10, a former Aspen Valley Hospital employee alleged the facility fired him upon learning of his HIV-positive status,** according to *The Aspen Times*. The man accused the hospital's human resources manager of outing him to a colleague over drinks at a conference, after learning about his condition as she was perusing employee insurance records in an effort to cut health costs. In a series of complaints he filed with OCR, the former employee alleged that his treatment at work deteriorated and that he was eventually terminated. Visit http://tinyurl.com/hr8t8su.

◆ **The HHS Office of Inspector General (OIG) will evaluate how hospitals are complying with HIPAA in their use of electronic health records (EHRs),** according to the agency's mid-year update to its 2016 Work Plan. "We will determine the extent to which hospitals comply with contingency planning requirements of [HIPAA]," OIG wrote. "We will also compare hospitals' contingency plans with Government-recommended practices." Read the Work Plan at http://tinyurl.com/j3zwnaa.

◆ **HHS issued guidance to health care organizations on preventing and responding to ransomware attacks.** In the June 2 document, the agency recommends taking a number of preventive steps, including initiating offline back-ups, testing the ability to maintain operations in the event of an attack, whitelisting applications and performing penetration testing, or attempting to hack one's own systems. HHS also encouraged organizations to contact the FBI immediately if they are hit with a ransomware virus. Visit http://tinyurl.com/jens6dc.

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.)