Report on
PATIENT PRIVACY

Volume 17, Number 2 • February 2017

Practical News and Strategies for Complying With HIPAA

Contents

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Editor
Theresa Defino
Theresa.defino@hcca-info.org

Senior Writer
Jane Anderson

Case With $3.2M Penalty Gives Rare Look At OCR Investigation Into Noncompliance

Anyone wondering if the HHS Office for Civil Rights' (OCR) aggressive 2016 enforcement streak would continue this year has an early hint: In just the first 30 days of 2017, the agency announced it had collected nearly $6 million in penalties from three errant HIPAA covered entities (CE).

Two of them also broke the mold. The Jan. 9 settlement with a health system in Illinois for $475,000 marked the first time a CE was dinged for late notification of a breach (see story, below).

And on Feb. 1, OCR announced it had imposed a $3.2 million penalty on Children's Medical Center of Dallas for security rule failures and a series of breaches that the medical center insists harmed no one. *Worth a special note:* Allowing OCR to impose the penalty, rather than paying a penalty through a voluntary settlement agreement, may actually save Children's in the long run because it does not have to comply with the usual, multi-year corrective action plan (CAP), which has accompanied all of OCR's settlements except one.

This case also provides something of a gift to the HIPAA compliance community, in that OCR describes a series of missteps it says Children's made over the years, providing rare specifics that belong on the "don't do this" list for CEs and their business associates (BAs).

continued on p. 9

Sole Failure of Timely Notification After Breach Costs Covered Entity $475,000

The first enforcement action of 2017 by the HHS Office for Civil Rights (OCR) has something new and something old. Announced on Jan. 9, the $475,000 settlement, which includes a two-year corrective action plan (CAP), marks the first time OCR has sanctioned a HIPAA covered entity (CE) or business associate (BA) for making a breach notification later than the proscribed 60 days from the point of discovery.

The something old is the fact that the protected health information (PHI) that was breached was contained on paper, and was not inappropriately disclosed due to hacking, ransomware, faulty firewalls or the failure of any electronic security safeguards.

OCR didn't find fault with the content of Presence Health's notices or take issue with any other aspect of its compliance with the breach notification rule, nor did the agency make more HIPAA-related findings regarding the nonprofit, 11-hospital system based in Chicago. OCR made no statements indicating that, for example, Presence lacked a risk analysis.

Becky Williams, chair of the Health Information Technology/HIPAA Practice Group at Davis Wright Tremaine LLP, says this may be the first such settlement, but that late notifications are a common occurrence. And they are often understandable, she adds.

continued

"A detailed forensics investigation can take a significant amount of time. Also, an organization generally will want to remediate the breach — or stop the bleeding — before providing the notification, and that can take time as well," Williams says. "Meeting the timing deadlines can result in notification without understanding the full scope of the breach." (For more of Williams' strategies on how to stay within the 60 days, see story, p. 3).

The sole issue involved in this settlement was that Presence was approximately 45 days late in notifying 836 patients, the media and OCR of the loss in 2013 of surgery scheduling sheets. According to OCR, the sheets were discovered missing from Presence St. Joseph Medical Center in Joliet, Ill., on Oct. 22, 2013, but notifications didn't begin until late January.

When contacted by *RPP*, Presence Health issued a general statement and would not answer specific questions. But, according to OCR, "due to miscommunications between its workforce members, there was a delay in its provision of breach notifications."

Under the breach notification rule, CEs are required to "notify, without unreasonable delay and within 60 days of discovering the breach," any affected individuals, as OCR explained in announcing the settlement. In addition, when the breach affects 500 or more people, notification to OCR and "prominent media outlets" is also required within the same 60 days.

Presence first notified OCR at 101 days from discovery, followed by patients at 102 days. The media was last, at 106 days post-discovery. According to a news report at the time, the hospital "apologized" for the incident and was attempting to find the sheets. It also offered patients a year of credit monitoring.

OCR Found Other Late Notifications

But this wasn't the first time Presence was late, OCR said. The agency found "several" instances of late notification to individuals involved in breaches affecting fewer than 500 people, as disclosed by Presence in 2015 and 2016 annual reports. It provided no details as to how late these notifications were.

The agency did not explain how it arrived at the $475,000 payment, except to state that "OCR balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether." The fact that three small breaches that were considered "untimely" could lead to such a high settlement — and a CAP — should give all CEs and BAs pause. (For a look at how OCR arrived at a recent $3.2 million settlement, see story, p. 11).

The settlement was one of the last to be announced by then-OCR Director Jocelyn Samuels, a political appointee who stepped down Jan. 20. "Covered entities need to have a clear policy and procedures in place to respond to the Breach Notification Rule's timeliness requirements," she said in a statement. "Individuals need prompt notice of a breach of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach."

The CAP itself deals with the notification process primarily and mirrors the problems that OCR said it found. Presence is required to revise its policies and submit them to OCR for approval within 60 days of the signing of the agreement. Following OCR's sign-off, training must occur.

Key Features of Breach Policies

The level of detail OCR has specified it wants to see in breach policies could prove helpful to other CEs and BAs. Presence agreed to revise its policies and procedures "to more explicitly delineate its workforce members' roles and responsibilities with respect to" the following:

- "Receiving and addressing internal reports made by workforce members of potential breaches of unsecured PHI";
- "Receiving and addressing external reports made by individuals and business associates of potential breaches of unsecured PHI";

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Health Care Compliance Association, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. 888.580.8373, www.hcca-info.org.

Editor, Theresa Defino; Senior Writer, Jane Anderson

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.hcca-info.org 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.hcca-info.org.

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

◆ "Completing risk assessments of potential breaches of unsecured PHI to determine the probability that the PHI has been compromised";

◆ "Preparing notifications to Individuals whose unsecured PHI has been compromised as a result of a breach";

◆ "For breaches of unsecured PHI affecting more than 500 residents of a state or jurisdiction, preparing notifications to prominent media outlets serving the applicable state or jurisdiction";

◆ "Preparing notifications to HHS regarding breaches of unsecured PHI; and"

◆ "Ensuring that all required breach notifications are submitted to the affected individuals, the media, and HHS without unreasonable delay and within the timeframes prescribed by the Breach Notification Rule."

And to make sure the policies and procedures stick, Presence is also required to "revise its existing policies and procedures related to applying appropriate sanctions against workforce members who fail to comply with its policies and procedures." (To review the CAP, visit http://tinyurl.com/jd3bje8.)

In a statement to *RPP*, Presence officials say they are up to the task. "Because patient privacy is a top priority at Presence Health, we are working diligently with the OCR on all steps required under the corrective action plan," which includes "training in HIPAA policies and procedures," they said. "We are confident that reports on our progress to quickly implement revised policies and procedures will be positive." ✧

Don't Be Late! Costly Settlement Raises Stakes for Breach Notices

Last month, the HHS Office for Civil Rights announced the first settlement with a HIPAA covered entity (CE) that missed the 60-day timeframe to notify individuals when their protected health information (PHI) is disclosed. Failure to comply with this aspect of the breach notification rule cost Presence Health Network of Chicago $475,000 (see story, above).

When the PHI of more than 500 individuals is involved, notification is also required to OCR and the media within 60 days. If fewer than 500 are involved, the media do not have to be notified, and notice to OCR may occur through annual reports.

For the past several years, the annual HIPAA Summit conference in Washington, D.C., has featured a presentation on breach notification. Each time, the speaker has been Becky Williams, chair of the Health Information Technology/HIPAA Practice Group at Davis Wright Tremaine LLP. So it seemed apropos to seek out Williams for strategies on ensuring that notifications are made on a timely basis.

RPP: What are the strategies to use that will help CEs and BAs make the 60-day deadline?

Williams: The key strategy is preparation. It is critical that covered entities and business associates have established processes for responding to potential breaches. The incident response team should be identified. Policies and procedures should be developed. Organizations should educate the workforce to immediately report concerns and to know who within the organization should receive these reports.

It is better to begin an investigation that turns out to not be an issue than to delay in reporting a potential breach. Table-top exercises are helpful to identify potential gaps in your incident response plan. The clock starts ticking from the moment of discovery — or actually from when you should have discovered the event. You want to avoid the "deer in the headlights" syndrome where people do not know what to do and precious time is lost.

RPP: What are some of the frequent mistakes made in the notification?

Williams: I have seen people wait in the hopes of finding the missing PHI, which delays the process and wastes precious time. You should assume that a breach will happen to you and know what to do in that event. Also, don't forget about state law. States may have different timing and content requirements.

RPP: Please address this aspect of the 60 days. You don't report inappropriate uses; you are required to report only breaches of unsecured PHI. So shouldn't the 60 days start when you've determined there is a reportable breach, not when there's a suspected breach resulting from an unauthorized use or disclosure?

Williams: To clarify, a reportable breach is the impermissible access, acquisition, use, or disclosure of unsecured PHI, so even an [unauthorized] use could result in notification, depending on the circumstances.

The clock starts ticking when the event is discovered, not when the correct compliance officer is notified and not at the conclusion of an investigation and formal determination. That's a reason why trying to

'Isolated Incident' Results in $2.2 Million Settlement With OCR

A USB drive with data for some 2,000 patients stolen more than five years ago has led to the sixth largest fine ever paid to the HHS Office for Civil Rights (OCR), following an investigation that revealed widespread noncompliance with the HIPAA security rule.

OCR announced this settlement, its second of 2017, on Jan. 18. (For two other recent enforcement actions, see stories, p. 1). OCR said MAPFRE Life Insurance Company of Puerto Rico agreed to a $2.2 million penalty, while hinting the amount could have been higher. OCR "balanced potential violations of the HIPAA Rules with evidence provided by MAPFRE with regard to its present financial standing," the agency said.

For its part, MAPFRE told *RPP* the theft — the USB device was attached to a computer and "left without safeguards overnight" in the IT department — "was an isolated incident and there has been no evidence that the data on the device was ever accessed or used by an unauthorized third party."

But, according to OCR, the firm had systemic security rule failures of the type often described in settlement agreements. MAPFRE, which did not admit to any wrongdoing, is also required to follow a three-year corrective action plan (CAP).

On September 29, 2011, MAPFRE filed a breach report with OCR indicating that a USB data storage device (described as a "pen drive") containing ePHI was stolen from its IT department. According to the report, "the USB data storage device included complete names, dates of birth and Social Security numbers," the agency said.

MAPFRE knew what was on the drive by "reconstituting the data on the computer" to which the USB data storage device was connected, OCR said.

OCR concluded that MAPFRE failed "to conduct its risk analysis and implement risk management plans, contrary to its prior representations, and [failed] to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014." Without being specific, OCR claimed that "MAPFRE also failed to implement or delayed implementing other corrective measures it informed OCR it would undertake."

Alexis Sánchez Geigel, MAPFRE's executive vice president and COO, also told *RPP* that his firm "has always been committed to safeguarding its insureds'

meet the deadline can be so difficult. It may take weeks to figure out what actually happened, not leaving much time to provide notification. I work with some clients who go down both tracks at the same time — verifying addresses and preparing the contents of the notification, while at the same time continuing the investigation and hoping for the best.

Technically, the clock also starts ticking when the organization should have known of the event. So hiding your head in the sand and ignoring a situation does not extend the timing. Also, OCR wants to encourage appropriate diligence in protecting PHI.

RPP: Can you list a few key points CEs and BAs need to make in their training and policies so that workers will be incentivized to report a possible breach?

Williams: There will be no retaliation for good faith reporting. This should be backed by a policy. Act as if the information is about you or your family. The sooner the possible breach is reported, the faster the organization can address the problem, including shutting down the breach. Some organizations reward workforce members who report concerns, even [with] something as simple as candy. Complying with the law should be everyone's goal. [Reporting a breach] is the right thing to do. The problem just gets bigger with a delay.

RPP: Do you think it is sometimes better to skip the assessment and notify to avoid being late?

Williams: A "LoProCo" risk assessment, to determine whether there is a low probability of compromise, is not necessary if the entity is going to provide the notification. So, skipping that assessment saves time. But, it could result in consumers being unnecessarily notified of an event. There is no good answer, but OCR seems to be sending a message on the importance of meeting the timing requirements.

RPP: OCR has stated that it will issue guidance on breach notification, but that still has not been forthcoming. Were it to be issued, what are the gray areas that guidance needs to address?

Williams: We once had a definition of "compromise" but it was tied to the risk of harm threshold [in the pre-2013 rule]. When OCR dumped the risk of harm threshold, the definition of "compromise" went out the window. So we need to decide whether a particular event constitutes a compromise of the information but we have no definition of "compromise."

Contact Williams at beckywilliams@dwt.com.

protected health information and, during the past years, it conducted an exhaustive review of company policies and procedures, and implemented additional controls to ensure the security of the protected health information."

MAPFRE, he said, "looks forward to continuing our efforts to protect our insureds' health data in compliance with the applicable laws and regulations and to continue working with the OCR towards an efficient completion of the CAP."

The CAP lays out a series of tasks MAPFRE must complete within certain timeframes, beginning with "an accurate, thorough, enterprise-wide risk analysis of ePHI security risks and vulnerabilities that incorporates all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by MAPFRE Life and its Workforce (which term means employees, independent contractors and consultants that have access to ePHI and that are not Business Associates or covered entities and any other individual as defined by 45 CFR §160.103) that contain, store, transmit or receive MAPFRE Life ePHI."

This is due to OCR within 220 days, nearly twice the amount of time the agency usually provides in other CAPs. MAPFRE is also required to develop a plan to mitigate the risks identified in the analysis, update its policies and procedures as necessary and retrain its workforce. (For more details, see http://tinyurl.com/hxc7ud8.)

Settlement Has Important Reminders

Whether OCR would find such widespread issues at other CEs today is an open question, but many remain noncompliant, says Joseph Lazzarotti, principal in the Morristown, N.J., office of Jackson Lewis P.C.

"Over the years, we have helped many providers and other covered entities with HIPAA compliance, including in connection with breaches and ransomware attacks. In the course of that work, we have found a fair amount of covered entities that have had compliance gaps, including some with significant gaps," he says. "On a positive note, in many cases, the gaps relate to the failure to document in writing otherwise compliant practices that are otherwise in place. My sense is that, since 2011, covered entities have improved compliance."

The message that OCR seems to be sending is that "noncompliance will cost covered entities a significant amount," Lazzarotti says.

As with others, the case also shows how long an investigation might drag on, a situation that CEs and BAs should prepare for. As Lazzarotti says, "there tends to be back and forth with the agency on compliance with certain standards and implementation specifications. In some cases, OCR is digging more deeply into the decisions being made by covered entities and the safeguards they are representing are sufficient to satisfy particular standards. For example, in some recent cases, OCR investigators have made requests, such as copies of business associate agreements with certain vendors; reasoning on why the covered entity did not keep an inventory of mobile devices when it uses those devices in the practice; and copies of device management programs and a description about whether or not implementation was successful."

This settlement is also another reminder that CEs and BAs "should be thinking more critically about whether their policies and procedures are reasonable and defensible," he says.

Contact Lazzarotti at lazzaroj@jacksonlewis.com. ✧

Employee Training Is Important to Thwarting Phishing Email Attacks

Training employees to report suspected phishing emails can reduce the standard time for detection of a breach from 146 days to just 1.2 hours, reducing the potential fallout from a data breach or ransomware resulting from the attack, says a new report from IT security consulting PhishMe, Inc.

The conclusion has significant implications for health care covered entities, which PhishMe rated as among the most vulnerable to particular types of phishing attacks.

Phishing simulation exercises are an effective way to educate workers about the different types of phishing attacks, the report says, noting that susceptibility to phishing email drops almost 20% after just one simulation.

Using phishing simulations developed by security consultants can help improve awareness among employees of HIPAA covered entities (CEs) of these types of attacks, and will enable health care workers to identify and report scams earlier. Early reporting can reduce a CE's exposure and limit the damage, but it isn't the only piece of the puzzle.

"Education and raising awareness can have a very strong impact on decreasing the number of successful phish attacks," says Fred Cox, CEO and managing director of security consulting firm FDC Associates, LLC. "However, this is only one technique that management should deploy in a layered security model," Cox tells *RPP*.

Hospitals generally are on top of this issue, Cox says: "In my experience most hospitals — 80% — do have an active anti-phishing program in force and do send out false emails to raise the awareness of their employees, because it has been found that education and reporting

does reduce the risk of a realized data breach or other adverse event."

However, Chris Apgar, CEO and president of Apgar & Associates, LLC and former HIPAA compliance officer for Providence Health Plans, thinks the percentage of all CEs that have taken the necessary steps to protect themselves against phishing attacks is far lower — more in the range of 30%, with insurers possibly "slightly better off" than providers.

"Larger organizations are more likely to spend some money on this," Apgar tells *RPP*. "But one of the problems with health care is the industry is behind in terms of security." Vendors, meanwhile, "are likely to pay more attention," Apgar says. "If they can't demonstrate HIPAA compliance, [CEs] will take their business elsewhere."

Phishing attacks are "one of the more common ways people are accessing data — stealing data," says Apgar. Up-front training can help, he says. Still, it won't prevent 100% of problems: "You can train the heck out of [your employees], but you're still going to have incidents."

He adds: "Phishing is so prevalent because the hacker technology to do something like that has been out there for a while," and has improved over time as hackers learn what works. In fact, phishing schemes have evolved to the point where the email bait can seem incredibly believable, even to someone who's well-trained, since they often include personal information targeted directly at the person to whom the email is addressed, Apgar says. "This makes it effective."

For example, a hospital's CFO might receive an email that looks like it's a legitimate request from the hospital's CEO, asking for specific financial information or data, Apgar says. Unless there's an obvious clue that the email is a spoof, the CFO might be inclined to reply with the data without checking on the request's authenticity.

Emails can contain a variety of different types of appeals to induce targets to click on links or attachments, PhishMe says, including phrases that motivate based on fear, curiosity, urgency or entertainment. Therefore, employees need to be trained to be aware of their natural reactions and use those reactions to signal the need to examine the email more closely for technical or process errors, the report says.

The PhishMe report analyzed data from its own simulations with companies to determine the vulnerability level for firms in different industries. It found health care entities were particularly vulnerable.

For example, when simulating an attack with a phishing email containing a "File from Scanner," an average of 31% of employees from the health care industry clicked on the attachment. That rate, PhishMe says, was second only to employees in the transportation industry, who clicked on the phishing attachment 49% of the time. Technology company workers clicked on it 10% of the

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.*

◆ **Third Circuit revives a data breach class action.** Horizon Healthcare Services Inc. provides medical insurance products and services to individuals and employers in New Jersey. In November 2013, two Horizon laptops containing the personal information of approximately 840,000 customers were stolen from a Horizon office building. In December 2013, four Horizon policyholders, the plaintiffs in the case, sued Horizon on behalf of themselves and all other affected individuals, alleging that Horizon failed to properly protect its customers' personal information. A New Jersey federal judge dismissed the lawsuit in March 2015 on the grounds that the plaintiffs failed to demonstrate they suffered sufficient harm. Specifically, while their personal information had been stolen, they were not able to allege that the stolen information had been used to their detriment. (In re. Horizon Healthcare Services Inc. Data Breach Litigation, 2-13-cv-07418 (D.N.J., Mar. 31, 2015)). Plaintiffs appealed the dismissal and the Third Circuit overturned the dismissal on January 20, 2017. (In re. Horizon Healthcare Services Inc. Data Breach Litigation, 15-2309 (3rd Cir., Jan. 20, 2017)). The Third Circuit held that the plaintiffs did not have to show that their personal data was actually misused, but rather they had alleged sufficient cognizable injury for Article III standing purposes by alleging improper disclosure of personal data in violation of the Fair Credit Reporting Act. Plaintiffs' alleged disclosure of personal information created a "de facto injury." The matter has been remanded back to the federal district court for further proceedings.

time, and those from nonprofits were fooled 5% of the time, the report says.

"This further stresses the need to fully baseline your organization and processes so that your biggest phishing threats can be identified and mitigated through focused repetition of high response scenarios and additional awareness activities," the report says.

According to Cox, the two main exposures that can result from a phishing attack on a health care entity include:

(1) A data breach, where the attacker uses the access gained by phishing to steal data, and

(2) A disruption of service in the form of a denial of service attack, which also can be used as a ransomware attack.

Ways to Reduce the Risks of Phishing

There are several steps health care organizations can take to safeguard against phishing, according to the PhishMe report.

First, they should analyze prior successful and unsuccessful phishing scenarios to identify those that seem particularly successful in their organization. Then, they should develop training — including phishing simulation — for employees, and stress the importance of reporting. High-risk users and departments should undergo additional training.

Phishing simulation exercises look like the real thing, says Cox. "The company can create false sample phish emails and send them to employees who are 'busted' when they click on the link or respond to the phish," Cox says. "This is a way to raise the awareness of being on the lookout for these types of emails. This is relatively easy to set up and keep working overtime."

Finally, PhishMe recommends that companies track suspected "real" phishing attempts to determine the success of the educational efforts, and make adjustments as necessary. PhishMe, which markets a reporting tool, says susceptibility to attacks declines over time as reporting of suspicious emails rises.

A 2016 report on phishing for health care firms from cyber security software company Symantec notes that technological solutions can't always detect phishing attacks. "By sending out well-crafted and relevant phishing test emails to employees regularly, you can detect problems and provide coaching," says the report. "By conditioning employees to look for certain cues in all emails that enter their inbox, they'll be able to more quickly and easily identify attacks and report them to security teams to close the feedback loop and thwart others from becoming victims."

However, a strong phishing reporting program won't prevent all attacks, and that's why Cox recommends additional steps, including using a data leak prevention utility.

"By deploying a data leak prevention utility you can add an effective layer should an employee fail to recognize a phish email and click the link that starts a download of data," Cox says, adding that behavior analytics can help to "detect atypical behavior or user actions that are a breach or denial of service in progress and stop that session."

Apgar says his organization is working with health care organizations to set up phishing exercises. These exercises take employees through various phishing scenarios and the privacy issues associated with them to show the organizations what can happen to the organization and to individuals in the event of a successful phishing attack.

Companies seeking to set up active reporting programs to combat phishing schemes don't necessarily need a reporting tool. Cox says they could create an email address or other means to receive notices from employees that they have observed — or strongly suspect — a phishing email. This would get that suspect email to the company's IT security staff members, who "can get the word out to the community that such a scheme is in play and to be on the lookout for it, and not to become a victim."

Greater Resources = Greater Compliance

Larger CEs may be in a better position to implement a robust anti-phishing program, because they have more substantial resources, while smaller CEs "don't have the budget dollars to invest," says Apgar. "If I'm working with a small practice or clinic, the person dealing with HIPAA is also doing the payroll and everything else."

continued

Phishing Schemes Are the Most Common Attacks

While more than half of business security professionals believe their companies are well-defended against ransomware attacks, some 53% have been the victim of such attacks in the last year, a survey finds. Information Security Media Group reported that phishing schemes are the most common attacks. Most security professionals say they've never paid ransom, but 54% said ransom — while a bad idea — can represent the fastest way to resolve the attack. Read the survey at https://tinyurl.com/jnlze8g.

For a clinic with two physicians, an anti-phishing program that costs $1,000, "or sometimes even $100," isn't affordable, he adds, "everyone is vulnerable to phishing." Larger CEs are more subject to significant data breaches, he says, but small clinics or other CEs can be subject to a phishing attack that leads to ransomware, according to Apgar.

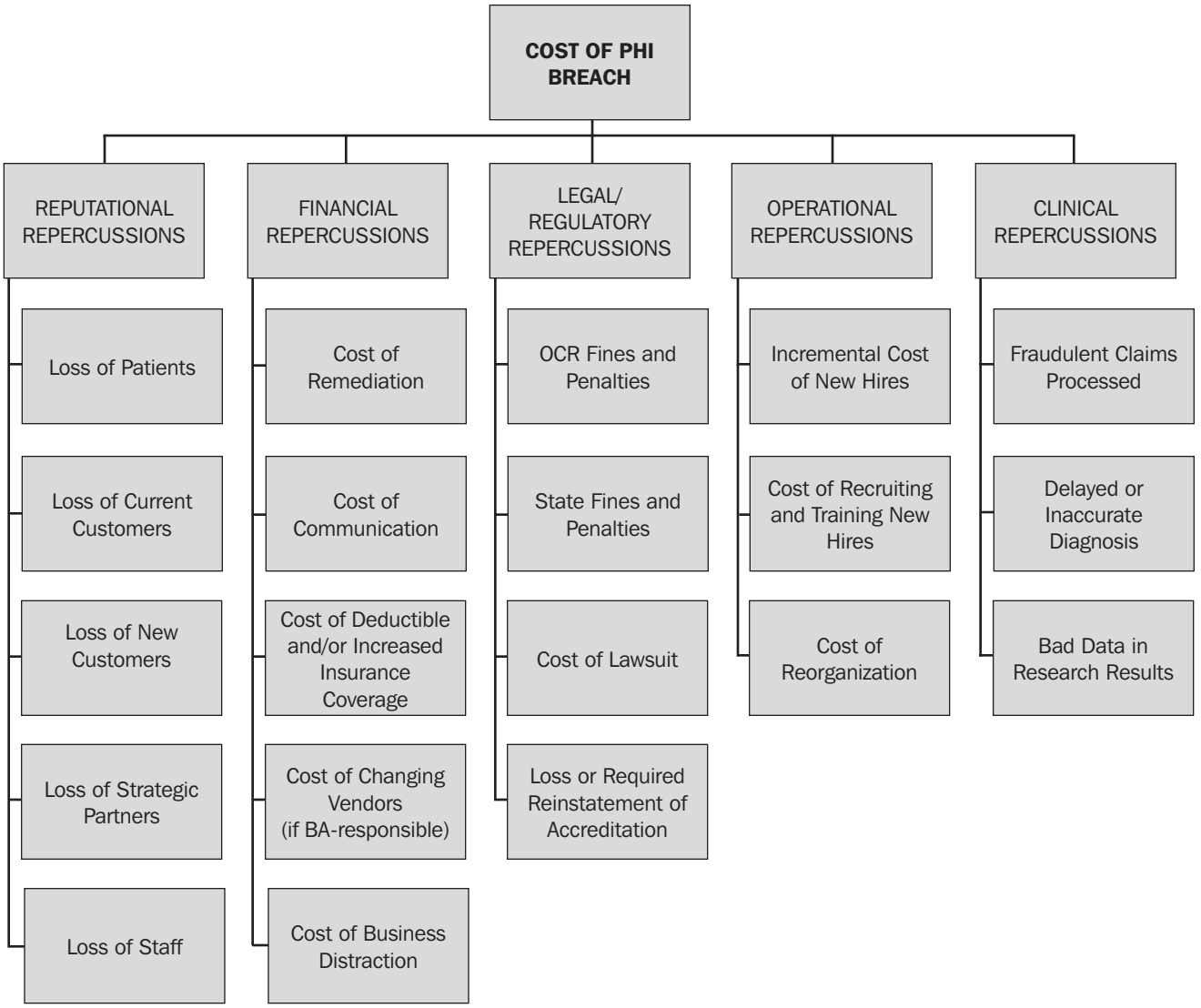
Cox adds that vendors may be more aware of phishing risks than their clients: "CEs are pressuring their vendors to clean up their act and not to be a victim of a data breach via a phish attack."

Even if the CE has a robust anti-phishing program in place, companies should follow U.S. Department of Justice recommendations when employees receive phishing emails, Cox says.

These recommendations include reporting phishing email to reportphishing@antiphishing.org, the address of the Anti-Phishing Working Group, which includes ISPs,

The Cost of a PHI Breach

The following chart appeared in *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security,* which was published by the American National Standards Institute (ANSI) in partnership with The Santa Fe Group/ Shared Assessments Program Healthcare Working Group and the Internet Security Alliance (ISA).To access the full 67-page report, visit http://webstore.ansi.org/phi.



SOURCE: American National Standards Institute. Reprinted with the permission of ANSI.

security vendors, financial institutions and law enforcement agencies. The working group uses the reports to fight phishing.

In addition, he says, company IT personnel should file a report with the Federal Trade Commission at www.ftc.gov/complaint, and also forward the email to the "abuse" email address at the company that is being spoofed — for example, spoof@ebay.com.

Nonetheless, anti-phishing programs — especially programs that allow early detection, which can limit the damage — are only one layer of necessary security, Cox warns. "The use of layers is prudent, as we need to start thinking about how our security models will react when a control fails, not if it fails, and have a layer that backs up the failure," Cox says. "Reporting and educational programs are but one layer of risk mitigation. Deploying Data Leak Prevention software to detect when a data breach is occurring is a highly recommended second layer to the educational/awareness efforts. Education alone will not stop a breach — correctly deployed DLP solutions will."

Contact PhishMe at (703) 652-0717, Cox at fcox@fdcassociates.com and Apgar at capgar@apgarandassoc.com. View the Symantec report at https://tinyurl.com/jebqyvh. ✧

'Letter' Provides Strong Guidance

continued from p. 1

In making its findings of noncompliance, OCR sent Children's a "determination letter" that charts the developments from when it first began investigating Children's. Such communications are usually seen only by the CE at issue. The letter reveals, for example, precisely when, and how, it arrived at the $3.2 million payment, and even includes a handy chart (see story, p. 11). Among the remarkable details included is that OCR apparently had offered to resolve the situation through "informal means," which would have meant some corrective actions but no penalty.

Children's declined to respond to specific questions from *RPP*. Instead, spokesman Scott Summerall emailed *RPP* the following statement, which speaks of weariness of the entire process.

"For the past six years, the Office for Civil Rights has been investigating the loss of three electronic devices. Two of the devices contained patient information," Summerall said. "We have fully cooperated with the investigation, and we have no reason to believe that any patient or their families were affected by the loss of these devices. We have decided to pay the imposed fine because the efforts to formally contest the claims would be a long and costly distraction from our mission to make life better for children. We remain committed to protecting the privacy of our patients."

When asked whether Children's was required to, or is following, a CAP, he replied, simply, "We are not."

Since it began taking enforcement action for HIPAA violations in 2008, OCR has settled 43 of 47 cases with voluntary agreements (with financial penalties) by the CE or BA. Children's is just one of three where it used its authority to *impose* a fine.

In Children's case, OCR identified the following breaches that contributed to the $3.2 million penalty. For the first three, no data were provided on numbers of affected individuals, and the breaches occurred prior to publication of the breach rule. Children's revealed these losses to OCR during its investigation, the agency said.

- ***February 2008:*** theft of a laptop.
- ***October 2008:*** theft of a laptop.
- ***July 2009:*** theft of a Blackberry.
- ***November 19, 2009:*** loss of an unencrypted, non-password protected BlackBerry device at the Dallas/Fort Worth International Airport; 3,800 individuals affected; reported on Jan. 18, 2010.
- ***December 2010:*** loss of an iPod by an "unidentified medical resident" that was "synched to the resident's Children's email account;"at least 22 individuals affected; reported on Aug. 22, 2011.
- ***April 2013:*** theft of unencrypted laptop "from an operating room storage area;" 2,462 individuals affected; reported on July 5, 2013.

In looking at what Children's had done wrong, OCR came up with quite a list, from lack of appropriate physical safeguards to failure to encrypt to not having a mobile device policy.

Regarding the 2013 laptop loss, "Children's internal investigation concluded [it] was probably stolen by a member of the janitorial staff," according to OCR. The medical center, OCR contended, provided "janitorial staff with unrestricted access to the area where the laptop was stored" and "did not provide encryption to protect the ePHI of this laptop from access by such unauthorized persons."

"Although Children's implemented some physical safeguards to the operating room storage area (e.g., badge access was required, and a security camera was present at one of the entrances), it also provided access to the area to staff who were not authorized to access ePHI," OCR said.

OCR also maintained that "Children's issued unencrypted BlackBerry devices to nurses beginning in 2007 and allowed its workforce members to continue using unencrypted laptops and other mobile devices until at least April 9, 2013."

continued

Encryption is an "addressable" standard under the security rule, not a required one. But when it is not used, a CE or a BA is expected to explain why and describe what it is doing instead. "Children's failed to appropriately document its decision to not implement encryption on mobile devices and/or any applicable rationale behind a decision to use alternative security measures to encryption," OCR said.

Children's also experienced an issue that may be common to large systems. "Prior to November 2012, Children's information technology (IT) assets were inventoried and managed separately from the inventory of devices used within its Biomedical Department," OCR said. As such, the medical center "was unable to identify all devices to which the device and media control policy should apply prior to completing a full-scope inventory to identify all information systems containing ePHI in November 9, 2012. Children's IT asset policies did not apply to devices that accessed or stored ePHI that were managed by the Biomedical Department."

Further, "[p]rior to at least November 9, 2012, Children's did not implement sufficient policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within the facility," OCR wrote in the determination letter.

Ignoring Recommendations Proves Perilous

OCR seems to be blaming Children's for the penalty, stating that, in May of last year, it "informed Children's that OCR's investigation indicated that Children's failed to comply with the Privacy and Security Rules and that this matter had not been resolved by informal means despite OCR's attempts to do so."

"Informal means" are when the CE or BA makes corrective actions required by OCR and does not pay a penalty. Given the pervasive areas of noncompliance OCR said it found, it is surprising the agency was willing to consider an informal resolution, but perhaps more surprising that Children's didn't bite. OCR said it tried the informal process from November 2015 to August 2016.

It's impossible to know why OCR pivoted from that point to assessing a penalty of $1,000 a day, totaling more than $3 million. It might have been bad luck on Children's part or bad timing — maybe a bit of both. The breach that first got OCR's attention was reported to the agency in January 2010 and was only the 26th breach report affecting 500 or more individuals to be filed. As of *RPP*'s deadline, there are now 1,820 reported breaches of this size, and OCR is required to investigate, and resolve, all of them. Perhaps the process with Children's went on so long that OCR officials felt they simply had to exact a high financial toll for their troubles.

In announcing the penalty, OCR Acting Director Robinsue Frohboese said the agency "prefers to settle cases and assist entities in implementing corrective action plans."

But one thing is clear: OCR was able to use analyses and other data that Children's itself provided during the investigation against it. In OCR's view, the medical center did not heed recommendations it was given to safeguard its PHI.

CEs Must Act on Risks They Identify

This continues a theme that OCR sounded last year. In separate settlements with both the University of Mississippi Medical Center and Oregon Health & Science University, OCR faulted the organizations for identifying risks and then doing nothing, or not enough, to address them. Each paid $2.7 million and agreed to corrective action plans *(RPP 8/16, p. 10)*.

The Children's determination letter also revealed details of those analyses that few organizations would ever make public. Interestingly, OCR also disclosed that Children's was the target of a 2012 audit by the HHS Office of Inspector General (OIG). This audit does not appear to have been released publicly.

OCR said Children's was privy to the following:

◆ "During the course of OCR's investigation, Children's submitted a Security Gap Analysis and Assessment conducted for Children's December 2006-February 2007 by Strategic Management Systems, Inc. The SMS Gap Analysis identified the absence of risk management as a major finding and recommended that Children's implement encryption to avoid loss of PHI on stolen or lost laptops."

◆ "In August 2008, PricewaterhouseCoopers (PwC) conducted a separate analysis of threats and vulnerabilities to certain ePHI for Children's and determined that encryption was necessary and appropriate. The PwC Analysis also determined that a mechanism was not in place to protect data on a laptop, workstation, mobile device, or USB thumb drive if the device was lost or stolen and identified the loss of data at rest through unsecured mobile devices as being 'high' risk. PwC identified data encryption as a 'high priority' item and recommended that Children's implement data encryption in the fourth quarter of 2008."

◆ "As a result of its receipt of the 2007 SMS Gap Analysis and 2008 PwC Analysis, Children's had actual knowledge of the risks to unencrypted ePHI at rest by at least March 2007, at least one year prior to the reported security incidents. Appropriate commercial encryption products were available to achieve encryption of laptops, workstations, mobile devices, and USB thumb drives in use by Children's staff by, at least, the time of the PwC

Analysis in 2008; however, Children's had not implemented encryption on all devices as of April 9, 2013."

◆ "Despite the findings of SMS and PwC and Children's actual knowledge about the risk of maintaining unencrypted ePHI on its devices, Children's issued unencrypted BlackBerry devices to nurses beginning in 2007 and allowed its workforce members to continue using unencrypted laptops and other mobile devices until at least April 9, 2013."

◆ "Children's did not implement security measures that were an equivalent alternative to the security protection available from encryption solutions as recommended by the 2007 SMS Gap Analysis and the 2008 PwC Analysis."

◆ In September 2012, OIG "issued the findings from its audit of Children's that focused on information technology controls for devices such as smartphones and USB drives. Among other things, the report, entitled 'Universal Serial Bus Control Weaknesses Found at Children's Medical Center,' found that Children's had insufficient controls to prevent data from being written onto unauthorized and unencrypted USB devices.

In OCR's view, the message to CEs and BAs is simple: "Ensuring adequate security precautions to protect health information, including identifying any security risks and immediately correcting them, is essential," said OCR's Frohboese. ✧

OCR Kept Hitting the Add Button Until It Hit $3.2 Million

Earlier this month, the HHS Office for Civil Rights (OCR) imposed a $3.2 million civil money penalty (CMP) against Children's Hospital of Dallas for a series of breaches and security rule failures. Children's did not admit to wrongdoing and did not agree to a settlement with OCR. It accepted the penalty amount "to avoid a long and costly appeal process" (see story, above).

Children's submitted "information and arguments" that it deserved a "waiver" on the penalty, which, when granted, can significantly reduce the actual CMP that could be assessed.

OCR has the latitude to negotiate fines. For example, an investigation by *RPP* of a 2013 settlement between OCR and Parkview Health System, Inc., of Indiana, revealed that the agency at one time considered a finding of four violations and a payment of $1.05 million, with penalties based on willful neglect.

The final agreement, however, was based on one violation and carried a payment of $800,000 *(RPP 12/14, p. 1)*. The system dropped paper files on the driveway of a retired physician with whom it was unable to close a deal *(RPP 7/14, p. 1)*.

The 2009 HITECH Act gave OCR four categories of CMPs to choose from, which apply: when the organization didn't know and couldn't have known there was a violation; when the violation had a "reasonable cause and was not due to willful neglect"; when the violation was due to willful neglect but was corrected; and when the violation was due to willful neglect and was not corrected.

In Children's case, OCR chose the "reasonable cause" category, which allows for a fine of $1,000 to $50,000 per violation, with a maximum of $1.5 million per year for "identical violations during a calendar year."

The agency said it imposed the minimum of $1,000 per violation per day/per violation "in consideration of Children's assertion that the CMP should be mitigated because the alleged encryption noncompliance did not result in any known physical, financial or reputational harm to any individuals nor did it hinder any individual's ability to obtain health care."

The agency also considers "aggravating" and "mitigating" factors when calculating CMPs. In this case, it saw only aggravation. It cited how long it took Children's to encrypt its devices as well as its "prior history of noncompliance."

The penalty added up quickly and would have been higher if not for the annual maximum cap.

OCR tallied the infractions as follows:

◆ ***$923,000 for failing to implement access controls*** (encryption and decryption, or an equivalent alternative measure), required under 45 C.F.R. §164.312(a)(2)(iv). This spanned from September 2010 to April 2013.

◆ ***$772,000 for lack of device and media controls,*** required under 45 C.F.R. §164.310(d)(1). These violations continued from September 2010 to November 2012.

◆ ***$1.522 million for "one-time" impermissible disclosures,*** prohibited under 45 C.F.R. §164.502(a). This arose from two incidents. OCR counted the December 2010 loss of the iPod as 22 separate violations because PHI for that number of individuals was involved, for $22,000. Then it calculated $2.46 million for the April 2013 theft of a laptop containing PHI of 2,462 people, again with $1,000 assessed for each, or a total of 2,462 violations. However, because of the annual cap, this was shaved down to $1.5 million.

PRIVACY BRIEFS

◆ **The Office for Civil Rights has issued new guidance clarifying that the HIPAA privacy pule permits disclosures to loved ones** regardless of whether they are legally recognized as relatives. The OCR FAQ was developed in large part to address confusion following the 2016 Orlando nightclub shooting about sharing protected health information with patients' loved ones, OCR said. The FAQ makes clear that the potential recipients of information are not limited by the sex or gender identity of the person. OCR also issued updated guidance stating that the terms "marriage," "spouse," and "family member" include same-sex marriages and dependents from same-sex marriages. View the new FAQ and additional information at https://tinyurl.com/gpr9tkp.

◆ **A laptop stolen from a physician's car may have contained information from 3,600 Children's Hospital Los Angeles patients,** and the hospital has begun notifying those who may be affected. The laptop allegedly stolen from a locked car on Oct. 18 may have contained names, addresses, medical record numbers and clinical information of patients. It's possible an encryption program wiped the device, the hospital says. For more information, visit https://tinyurl.com/zkefvxl.

◆ **In 2016, health care data breaches occurred at an average rate of more than one per day,** according to the Breach Barometer Report. HHS received reports of 450 breach incidents, and more than 27 million patient records were affected. Four out of five entities affected were health care providers. Insiders were responsible for 43% of those breaches, and hacking/ransomware accounted for about 27%. Learn more at https://tinyurl.com/gkuhlpm.

◆ **Emory Healthcare's Brain Health Center may have fallen victim to a ransomware attack involving limited information on some 90,000 patients,** a security researcher says. The attack apparently involved a third-party database that was infiltrated by bitcoin ransomware, according to MacKeeper Security Research Center, which reported the incident. The information allegedly stolen included names, addresses, email addresses and cell phone numbers, but not Social Security numbers or financial information. Learn more at https://tinyurl.com/j7dde8t.

◆ **Privacy and security concerns aren't leading more patients to withhold information from their providers,** a study finds. The study compared patient behavior in 2011 and 2014 to see if publicized breaches of medical records had made patients less inclined to share information with their physicians. It found no real differences between the two years. The authors suggest that physicians can ameliorate privacy concerns by highlighting quality of care benefits offered by electronic medical records. View the study at https://tinyurl.com/gmknrpz.

◆ **President Trump plans to appoint an advisory team to develop an anti-hacking plan within his first 90 days in office,** according to a statement. Although the plan appears to be a response to the issue of cybersecurity and its role in the Nov. 8 election, the plan will "aggressively combat and stop cyberattacks." Visit https://tinyurl.com/z77kff5.

◆ **Researchers at Binghamton University, State University of New York, are studying whether it's feasible to protect patients' electronic health records using the patients' own heartbeats.** ECG signals are commonly collected physiological parameters, the researchers say, and the unique signals could be repurposed as passwords. However, ECGs can change due to illness and age, so the researchers are studying how to incorporate these variables into their encryption techniques. Read more at https://tinyurl.com/j5cxjjd.

◆ **The 15,000 victims of a data breach at New Hampshire Hospital are experiencing long wait times when calling a hot line,** said the state's Department of Health and Human Services. Also, some of the letters were addressed to deceased individuals, which raised additional concerns, the state agency said. A former psychiatric patient has told investigators he copied the files, and state officials are considering charges against him. For more information, see https://tinyurl.com/jmewnct.

◆ **Health care data breaches cost a total of around $6.2 billion annually, and breaches across all industries cost $4 million each, on average,** according to a white paper from security firm Protenus, Inc. The seven potential costs of a health care data breach include forensics, notification, lawsuits, lost business, lost brand value, HIPAA fines and post-breach costs, the white paper said. Read more at https://tinyurl.com/jugnlrf.