Report on
# Patient Privacy

Volume 18, Number 1 • January 2018

Practical News and Strategies for Complying With HIPAA

Contents



HCCA

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

**Senior Writer**
Jane Anderson

**Copy Editor**
Bill Anholzer
bill.anholzer@hcca-info.org

## $2.3 Million Payment Following 'Criminal Intrusion' Closes Banner Year for Settlements

The HHS Office for Civil Rights (OCR) ended 2017 with a bang. A mighty big bang. But the whole year was pretty astounding.

With just four days left in the year, OCR announced its 10th and final settlement of 2017 for alleged HIPAA violations: $2.3 million with 21st Century Oncology (21CO), which bills itself as "the largest, physician-led provider of integrated cancer care services."

While the amount itself wasn't record-breaking, the settlement brought OCR a cumulative $19.4 million for the year, making 2017 OCR's second highest for financial penalties collected (see story, p. 4). Top billing came in 2016, when OCR announced 13 enforcement actions totaling $24.5 million (*RPP 12/16, p. 1*).

Announced Dec. 28, the 21CO settlement also calls for a comprehensive, three-year corrective action plan (CAP) with numerous requirements, including the appointment of an external "assessor" (see story, p. 8). Also of note: OCR pursued the agreement while 21CO was in the middle of bankruptcy, a breach insurer was identified as the source for the $2.3 million payment, and it ends a seven-month drought of no settlements.

*continued on p. 11*

## Outlook 2018: Use Training, Patching to Counter More Sophisticated Cyberthreats

Expect more phishing, more ransomware and more cyberattacks using the internet-of-things in 2018, as hackers use increasingly sophisticated tools and techniques to steal and sell valuable medical records or to deny health care entities access to their own systems for ransom money.

Humans remain the weakest link in the security chain, security experts tell *RPP* in a series of interviews, and organizations' HIPAA security personnel should focus on training to ward off threats in 2018. They also need to focus on their business associates to make certain they are also complying. Neglected patches for known security vulnerabilities and poor security in internet-of-things devices also represent growing threats, experts say.

David Harlow, principal in the health care law and consulting firm The Harlow Group LLC, anticipates similar attacks to what was seen in 2017. "Most hackers rely on a combination of technical vulnerabilities that are exacerbated by human factors," Harlow tells *RPP*. "For example, the largest breach of the past year, the Equifax hack, was made possible by the failure of staff to apply a patch released by a software vendor to address a known vulnerability."

Phishing and ransomware attacks will continue to exploit humans, who are "the weakest link in our cybersecurity infrastructure," Harlow says. "The coming year is likely to bring new and different versions of the same-old, same-old—the hackers

*continued*

are becoming more and more sophisticated, spoofing URLs, for example, in a manner that is entirely indistinguishable from the real thing by anyone but the most sophisticated users."

Roger Shindell, president and CEO of Carosh Compliance Solutions, tells *RPP* that 2018 will see an increase in ransomware. The health care industry will continue to see more of a threat than other industries due to the value of medical information on the black market, he says.

### Hackers Will Exploit Same Vulnerabilities

Hackers have been successful employing ransomware and exploiting unpatched systems, and so they'll continue to do so in 2018, says Patricia Shea, partner at K&L Gates LLP. "After all, why mess with success?" she tells *RPP*. "I expect more sophisticated phishing, ransomware, and opportunities to do bad things because of the exploding array of devices and connectivity and data. There are just so many entry points."

Bad actors will ramp up their profiling of potential victims based on internet activity and other online information available to them, Shea says, and will be able to create scenarios that are plausible and non-suspicious. In addition, the "bring your own device" problem will continue, she says. "Health care entities need to take a long, hard look at their policies and procedures for permitting these devices to be used and whether the risk is simply too great," she says. "If they permit it, they must require safeguards such as encryption to be installed. The potential for misuse—intentional and negligent—is very real with the use of these devices."

Tareva Palmer, chief information security officer at WVU Medicine, says the types of threats health care entities experience in 2018 will be the same as those seen in 2017. "External bad actors are always a concern, attempting to gain access for monetary gain from stolen medical and financial information. This includes identity theft and medical fraud as well as ongoing malware threats. Threat vectors such as phishing attempts and network scans aimed to detect exploitable vulnerabilities continue to be on our radar," she says.

Rebecca Herold, president of SIMBUS360 and CEO of The Privacy Professor, says she expects the most significant threats in 2018 to include:

- increases in ransomware and associated ransom costs;
- increases in denial of service attacks, particularly through internet-of-things devices;
- increases in insiders selling patient data, since insiders realize that data is valuable;
- more breaches from lack of training and awareness, especially since organizations are providing less training, not more; and
- more and larger breaches from business associates who "simply still do not think they need to comply with HIPAA."

Shindell also cites security lapses at business associates as an under-addressed security problem, although he says the problem is getting some awareness and is attracting attention from OCR: "Expect this to become a growing trend in 2018."

### Digital Devices Pose Growing Threat

Consumer-grade wearables and other devices could represent an up-and-coming security issue in 2018 as medical organizations attempt to tap into the data they contain and add that data to their own medical records, Harlow says. The Food and Drug Administration has expressed its intention to leave "a broad swath" of digital health application functionality unregulated, "which means that much of that functionality is coming soon to a smartphone near you," he says. "As a result, there is likely to be more and more personal and health data collected on our phones and shared with health care organizations and with app developers." Melding these systems could lead to new chances for security breaches, he says.

**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, hcca-info.org.



Editor: Theresa Defino

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 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 hcca-info.org.

**Subscribers to this newsletter can receive 12 non-live Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB)®. Contact CCB at 888.580.8373.**

Medical professionals will eagerly adopt patient care devices that can be used in patients' home environment, but those devices must be secure, Palmer says. "We will continue to see increases in the volume of internet-of-things devices." She cites the $2.5 million settlement OCR obtained against CardioNet, now called BioTelemetry, Inc., a publicly traded, cardiac medical device and remote monitoring company that lost two unencrypted laptops in 2011 (*RPP 5/17, p. 1*).

"OCR determined that CardioNet did not understand HIPAA and obtained a $2.5 million settlement," she says. "OCR found that CardioNet failed to conduct an accurate and thorough risk analysis to assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of the ePHI [electronic protected health information] and failed to plan for and implement security measures sufficient to reduce those risks and vulnerabilities." Other organizations employing internet-of-things devices are at risk for breaches, she says.

To combat these growing threats, security experts urge health care organizations to improve their training regimens, to patch known vulnerabilities, and to make certain they have the resources needed to deploy adequate safeguards.

Shea says the top priority for 2018 should be promptly installing patches, although she says she's encountered pushback on this issue. "I recently had a former security officer for a hospital respond to my advice in this regard as, basically, 'That's easy for you to say—you are not the one to tell end-users that you are taking potentially life-saving systems down to install the patch.' I question that view for a number of reasons, including whether it accurately represents the technical reality of installing patches. If it does, there may be bigger issues."

Training also represents a key tool in combatting breaches, but it needs to be more than minimal annual training, and it should employ some sneaky tactics, Shea says. "In some cases, a little paranoia may be good," she says. "Health care entities should consider testing the waters of their personnel to see if they really get it. For example, send a fake phishing email and see who opens it. The results will be surprising and provide health care entities with teachable moments for their personnel."

## PATIENT PRIVACY COURT CASE

*This monthly column is written by Ellie F. Chapman 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 Ellie at ellie.chapman@morganlewis.com.*

◆ **Illinois Firm Must Face Privacy Claims over Deposition Disclosure.** On December 11, 2017, an Illinois appeals court partially reversed and remanded *Doe v. Williams McCarthy, LLP, 2017 IL App (2d) 160860*, a privacy lawsuit against Illinois-based firm Williams McCarthy, LLP. In the suit, "Jane Doe" alleged that Williams McCarthy attorney Treva Sarver improperly revealed Doe's mental health status during a deposition in previous litigation involving claims that Sarver exerted undue influence to exclude Doe from a trust. Doe challenged this disclosure as a violation of the Illinois Mental Health and Development Disabilities Act (Act), among other claims. On April 19, 2016, a Lee County Circuit Court judge ruled in favor of Williams McCarthy, holding that Doe's complaints of a privacy violation were barred by the absolute-litigation privilege, which immunizes certain statements and conduct by attorneys in the course of litigation in the name of vigorously acting on behalf of their clients. However, on December 11, 2017, the three-judge appellate panel disagreed, holding that the violation of the Illinois state statute trumped the absolute-litigation privilege. In so holding, the court relied on the Act's plain language, which stated that the Act applied "in any civil, criminal, administrative, or legislative proceeding." According to the panel, such language indicated that the legislature intended to control "all releases of the material [the Act] makes confidential in all types of proceedings." The panel, however, did not reverse all of the lower court's conclusions in Doe's favor and declined to weigh in on the extent to which Doe's privacy was violated: "In this case, almost all of the people upon whom plaintiff bases her claim bore a relationship to the litigation, whether it be courtroom personnel, participants in a deposition, or potential witnesses. To the extent that plaintiff seeks to rely on unidentified members of the general public who might have viewed the court proceedings or court file (and who might not have had some relationship to the litigation), her allegations are far too speculative to merit consideration."

Shindell says poor workforce security training and poor training on HIPAA policies and procedures are the biggest HIPAA security threats in 2018 for covered entities and business associates alike. "Too many entities give staff generic 'HIPAA 101' training, when the regulations additionally require that training must include specific ways that each organization guards their protected health information. People are on the front line of the cyber-war—people need to be properly trained to fight it."

Good security requires constant surveillance of the environment, plus buy-in from the C-suite in the entity and adequate budgets, Shea adds. WVU's Palmer agrees: "Health care entities should have a strong risk and vulnerability management program. HIPAA security and privacy risks should be ranked alongside all other risks for the organization. Our organization does this at the health system level."

Herold agrees that more training—and more frequent training—is important for improved security (*RPP 12/17, p. 6*). Training should feature frequent awareness reminders and other types of communications and events, she says. Herold also says organizations need to implement stronger business associate security and privacy oversight programs, and work to secure wireless and internet-of-things devices within facilities (see related story, p. 6).

Harlow also advocates better workforce education, but he urges organizations to look at innovative technologies such as artificial intelligence in cybersecurity tools and blockchain.

### Update Security Risk Assessments

In addition to constant, ongoing training, Shindell recommends that health care entities update their security risk assessments: "This should occur annually, in addition to whenever you experience a breach. Subsequently, remediation plans should also be updated to reflect priorities given new threat landscapes. All devices that transmit or store electronic protected health information should be included." He also urges HIPAA security staff to change default passwords. "Take inventory of all devices that access, store or transmit electronic protected health information in your security risk assessment, and be sure they have robust passwords."

At WVU Medicine, Palmer says the security team's top three priorities include:

◆ Hardware security. "Security and privacy is a major focus in our purchasing processes," she says.

◆ Education. "Information technology team members have been educated to search for potential issues, and we must continue this practice, just as we educate our customers (employers and providers) about the reasons certain security controls are needed. We will continue to share with our customers why balancing ease of access with security is crucial," Palmer says.

◆ Auditing and risk assessments. "Continuous ongoing internal auditing by our privacy team helps ensure that employees and providers have the access that they need, and verifies that the access is appropriate. We will also continue to perform ongoing security risk assessments to ensure that the network, health technology management devices, servers, workstations, operating systems, databases and applications are secure," she adds.

Overall, Palmer says, "processes should be hardwired to ensure security and privacy [are] part of project plans and implemented along with new applications. Audits of currently deployed applications help keep applications secure." To manage the human side of the equation, ongoing HIPAA training reminds all workers "that HIPAA privacy and security is everyone's responsibility." In one example of a "gentle reminder," she says the privacy and security team distributed pens in October 2017 during Cyber Security Month with the message: "Information Security: It's Everyone's Responsibility."

Contact Harlow at david@harlowgroup.net or at healthblawg.com, Shindell at rshindell@carosh.com, Shea at patricia.shea@klgates.com, Palmer via WVUHS spokesperson Leigh Limerick at limerickl@wvumedicine.org, and Herold at rebeccaherold@rebeccaherold.com. ✧

## Late Notification, Unauthorized Press Disclosures Among 2017 Settlements

In March, the Office for Civil Rights (OCR), which polices enforcement with the HIPAA privacy, security and breach notification rules, received a new director, Roger Severino (*RPP 4/17, p. 1*). This was expected, as OCR directors are political appointees who typically change with the administration.

While it takes time to reveal whether a new leader will influence the pace, size or number of enforcement actions, Severino now presides over an agency that closed out 2017 with a near-record $19.4 million collected from covered entities (CEs) and business associates (BAs) to resolve allegations of HIPAA violations.

The last agreement came in the final days of the year (see story, p. 1). Settlements were packed into the first five months of the year, with a drought from June to November.

The year's enforcement actions held noteworthy developments, including four firsts: the first for late notification of a breach, the first to be issued to a medical device firm, the first involving an organization in the middle of bankruptcy and the first for an errant fax.

Typically CEs and BAs settle with OCR over allegations of HIPAA infractions and pledge to adhere to a corrective action plan (CAP) as part of the settlement terms. That was the case with all but one of 2017's 10 cases. Last year OCR took the rare step of imposing a penalty. Other 2017 cases were more routine, triggered, for example, by the theft of unencrypted laptops.

The following are details about the 2017 settlements, listed by date of OCR announcement:

◆ **Jan. 9, Presence Health of Chicago**, $475,000 and a two-year CAP for failing to make timely notification of a breach, which is required within 60 days of discovery. 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 (*RPP 2/17, p. 1*). This marked the first time OCR cited an organization for this issue.

◆ **Jan. 18, MAPFRE Life Insurance Company of Puerto Rico**, $2.2 million and a three-year CAP for failing to "conduct its risk analysis and implement risk management plans, contrary to its prior representations" and "to deploy encryption or an equivalent alternative measure on its laptops and removable storage media until September 1, 2014." The triggering incident was the theft of a USB drive that contained the protected health information (PHI) for some 2,000 patients (*RPP 2/17, p. 4.*)

◆ **Feb. 1, Children's Medical Center of Dallas**, $3.2 million penalty imposed by OCR with no CAP. The fine followed six separate breaches from 2008-2013 that involved the loss of an iPod and several laptops and Blackberries. Children's admitted no wrongdoing related

## OCR Addresses Mental Health, Forms Working Group

In the hustle and bustle of the end of the year, covered entities and business associates could be forgiven if they missed all of the activities that the Office for Civil Rights (OCR) engaged in during December. The agency issued its 10th settlement agreement, bringing in $2.3 million to end the year with more than $19 million collected from alleged HIPAA violators (see story, p. 1).

But OCR also announced the launch of companion web pages for providers and patients that focus on mental and behavioral health, including substance abuse. The pages "reorganize existing guidance" to be more "user-friendly and provide a one-stop resource for our new guidance and materials," OCR said on Dec. 18. Included is a 13-page FAQ that contains updated responses to questions, such as what is incapacity and what rights do minors have.

OCR previously issued guidance on the sharing of protected health information (PHI) when a person is in treatment for opioid abuse. Released in November, that guidance reminded providers that they can tell the friends and loved ones that a person who overdosed may be abusing opioids or other drugs or substances without fear of violating the HIPAA privacy rule (*RPP 11/17, p. 1*).

That November guidance is now joined by fact sheets, an infographic and "decision charts," OCR said.

In addition, the agency said it had updated its 2002 guidance on HIPAA and research.

"OCR continues its work to ensure that patients and their family members can get the information they need to prevent and address emergency situations, such as an opioid overdose or mental health crisis. At the same time, these tools and initiatives also fulfill requirements of the 21st Century Cures Act to ensure that the healthcare sector, researchers, patients, and their families understand how [HIPAA] protects privacy and helps improve health and healthcare nationwide," the agency said.

OCR also reported that it recently had:

◆ Launched a working group "to study and report on the uses and disclosures under HIPAA" of PHI used in research. Members "include representatives from relevant federal agencies as well as researchers, patients, healthcare providers, and experts in healthcare privacy, security, and technology." They are expected to "release a report addressing whether uses and disclosures of PHI for research purposes should be modified to facilitate research while protecting individuals' privacy rights," OCR said.

◆ Formed a new "collaboration with partner agencies within HHS to identify and develop model programs and materials for training healthcare providers, patients, and their families regarding permitted uses and disclosures" of PHI related to patients "seeking or undergoing mental health or substance use disorder treatment." The purpose is to "develop a plan to share the programs and materials with professionals and consumers."

For details see https://tinyurl.com/ycbyw78w.

to the breaches, which totaled less than 10,000 affected individuals (the number affected is not provided for all incidents). OCR also said Children's had failed to encrypt its mobile devices, despite being warned by multiple consultants (*RPP 2/17, p. 1*).

◆ **Feb. 16, South Florida Hospital District**, also known as Memorial Healthcare System (MHS), $5.5 million and a three-year CAP. The settlement followed the 2011-2012 theft of patient data that resulted in identity fraud and the inappropriate use by 12 employees of an MHS affiliate physician's office. The workers were said to be using a login assigned to an employee who was no longer with the practice. The two incidents led to the exposure of the PHI of 115,000 people (*RPP 3/17, p. 1*). The amount is tied for the largest ever paid for alleged HIPAA violations. In 2016, Advocate Health Care also paid $5.5 million following the theft of desktop computers holding records for 4 million individuals (*RPP 9/16, p. 1*).

◆ **April 12, Metro Community Provider Network of Colorado**, $400,000 and a three-year CAP. The federally qualified health center was the victim of an email phishing scam in 2011 that exposed the PHI of 3,200 individuals. OCR contended that the health center had completed its security risk assessment later than required and that it was incomplete. As with other settlements, there was no admission of wrongdoing (*RPP 5/17, p. 6*).

◆ **April 20, Center for Children's Digestive Health (CCDH) of Chicago**, $31,000 and a two-year CAP for failing to have a business associate agreement (BAA) with FileFax, a firm it hired to store and dispose of old patient records. The OCR settlement followed an enforcement action by the state of Illinois. Records from a different practice were found in a dumpster and were later traced back to FileFax, which settled with Illinois officials for $30,000 and was required to identify its other clients. OCR concluded that, although FileFax was a business associate of CCDH, there was no BAA. Without this, CCDH had "impermissibly disclosed" the PHI of nearly 11,000 patients (*RPP 5/17, p. 5*).

◆ **April 24, CardioNet, now named BioTelemetry, Inc., of Penn.**, $2.5 million and a two-year CAP following the theft of two unencrypted laptops containing PHI for approximately 4,000 patients. OCR found that CardioNet had "insufficient risk analysis and risk management processes in place at the time of the theft," a lack of encryption as well as policies for the use of mobile devices. This marked OCR's first case involving a medical device company (*RPP 5/17, p. 1*).

◆ **May 10, Memorial Hermann Health System of Houston**, $2.4 million and a two-year CAP for disclosing PHI about a patient to the media after she was arrested at one of its clinics for allegedly providing false identification. OCR said the system did not err in calling the police regarding her IDs but lacked the patient's authorization to reveal the details that it later disclosed to the media in an attempt to explain its actions. The case sparked national media attention and protests (*RPP 6/17, p. 1*).

◆ **May 23, St. Luke's-Roosevelt Hospital Center of New York**, $387,000 and a three-year CAP. OCR found two instances when a worker from a program that "provides comprehensive health services to persons living with HIV or AIDS and other chronic diseases" inappropriately faxed medical records to a patient's employer and to the office where a different patient was a volunteer. OCR called the mistakes "egregious" but did not cite St. Luke's for any other alleged lapses (*RPP 6/17, p. 6*).

◆ **Dec. 28, 21st Century Oncology of Florida**, $2.3 million with a two-year CAP. An FBI informant reportedly purchased patient files that were "illegally obtained by an unauthorized third party," affecting some 2,213,597 individuals (see story, p. 1). ✧

## Consider Separate Networks for Unsecured Medical, Other Devices

Networked medical devices such as portable monitors and non-medical devices like printers represent significant threats to the security of protected health information. Organizations often fail to carefully track and update this equipment to guard against hacks.

In fact, equipment is often so old that it cannot be patched, experts say. And hospitals and other medical organizations may not even know how many devices they have or where those devices are. To manage security, health care entities need to inventory this equipment and segregate some items on limited networks.

"I have seen estimates that the average hospital has six pieces of biomedical equipment for each licensed bed, more than the number of workstations—laptops and desktops," says Clyde Hewitt, vice president of security strategy for CynergisTek, Inc.

"It is typical for hospitals to keep medical equipment in service for 15 years or more," Hewitt tells *RPP*. "These older devices rely on obsolete operating systems, some with vulnerabilities that cannot be patched. The level of security risk will vary depending on how these systems are integrated into their environment." He adds that it's not possible to determine the level of cybersecurity risk without an assessment of each individual device and how it's used in its environment.

It's possible to secure these devices so that they're unlikely to lead to a HIPAA breach. However, doing so first requires awareness of the problem.

"The challenge is that, when HIPAA came out, senior staff was focused on servers and laptops," Hewitt says.

"Since then, biomedical equipment has been storing so much patient data. It's generally not managed by the IT department," which means the security-savvy IT staff generally isn't involved.

"For most people, when a laptop gets to be four years old, it's ready for the trash heap," Hewitt says. The same rule doesn't apply to biomedical equipment. Older equipment is likely running Windows 95 or XP, two versions that aren't supported any longer, he says.

At least two reportable data breaches have involved biomedical devices:

◆ A medical device that looked like a laptop computer was stolen on April 12 from SSM Health Orthopedics in St. Louis. The device contained some physiological data and names, dates of birth, medical record numbers and symptoms from 836 patients who participated in a study between 2002 and 2017.

◆ A portable ultrasound diagnostic machine was stolen from Baylor Heart and Vascular Center in Texas in late 2010. The machine had been placed in service in 2006 and had been used in about 8,000 patient procedures, but Baylor said the device probably only contained data on a very small fraction of those 8,000 patients since the data was regularly purged and overwritten. Patient health information on the device included names, dates of birth, blood pressures, heights, weights, and ultrasound images of patients' hearts.

However, the actual threat is far larger and encompasses more than just obvious medical technology in a covered entity's environment, says Roger Shindell, president and CEO of Carosh Compliance Solutions. "For example, a dentist's dental practice in Toronto learned that their practice activities were being live-streamed in Russia on a site called insecam.org. What happened was that the practice had installed a wireless security camera system after a break-in but left the default password intact, enabling the Russians to access the live feed and stream everything that occurred in the office—which included patient and staff activities, but also clear access to private information on computer screens. These types of vulnerabilities will be increasingly exploited," Shindell tells *RPP*.

Many medical devices are designed to be mobile. They're used to collect data that's then downloaded when they're plugged in. When these devices are plugged into the network at the nurse's station, they represent a security vulnerability, Hewitt says.

Meanwhile, some devices are equipped with internal wireless capabilities that may or may not be encrypted, he says. "Hospitals will purchase printers, but they don't do software upgrades on them, and they don't do security on them," Hewitt says.

The problem of older devices isn't unique to health care—other sectors, such as financial services, also use devices that aren't as secure as newer models, says Brian NeSmith, CEO at data security firm Arctic Wolf Networks. However, health care is the most affected industry, even though awareness is low, NeSmith tells *RPP*.

"In general, I'd say the majority of people who have had problems weren't even aware of this as an issue," he says. "It's simple ignorance—not recognizing that hackers could us[e] this as a way to get into your network." NeSmith estimates that some 20% to 30% of health care organizations are aware of the problem. Larger organizations are more aware of the problem, but the scope of their problem is bigger, since they have many more devices, he says.

Meanwhile, a "fairly low percentage of people" are using this as a way to attack the network, NeSmith says, but he adds, "We've seen it, especially where there's a device with a weak password." And he warns it could become more common: "As we find better ways to defend other parts of the network, hackers are looking for easier ways in."

Most of these biomedical devices—whether they're imaging machines or specialized monitoring equipment—run a version of Windows or Linux, NeSmith says. It won't be a standard version of the software, which means health care organizations will be dependent on that particular developer to update and patch the software, he says.

Therefore, the best defense against hacking is a barrier in front of the device, rather than strong defenses within the device itself, he says, and most often, this will involve a separate network.

Organizations first need to identify the devices that place them at risk, Hewitt says, adding, "a lot of organizations don't have good asset inventory."

"Hospitals are required to maintain an accurate inventory of medical devices—a condition to meet their Joint Commission accreditation," he says.

### Separate Networks Can Mitigate Risk

However, hospitals face many challenges in keeping a good inventory, including "disconnects between what is purchased and what is acquired through other means, such as equipment loans, incomplete inventories during mergers and acquisitions, and equipment acquired through shadow procurement sources (defined as unauthorized channels)," Hewitt says. "The lack of individual accountability for individual devices makes it harder to know when individual devices are lost or stolen."

Identifying all these devices will be easier said than done, NeSmith notes. "A lot of them are not discoverable, depending on how the network is put together. What you will have is a bunch of IP addresses in your organization, and you're not sure what they're applied to. You'll have

to do fingerprinting of devices, and if you're starting from zero, there could be hundreds or thousands of devices."

Organizations could fingerprint 80% of those devices relatively easily, but identifying and listing the rest could prove challenging, he says. Also, different groups in the organization often acquire their own equipment, adding to identification issues, he says.

Next, organizations need to take specific device-by-device action to reduce their risk. That might mean installing patches, isolating devices from the internet and from other internal networked devices, and implementing physical and administrative controls.

However, NeSmith warns that organizations shouldn't wait to discover every single poorly protected biomedical device before moving to segregate and patch problematic devices. Instead, security personnel should discover as many as possible, block entry on those devices, and then do the harder work of identifying more.

"They can isolate [them] based on the risk," says Hewitt, noting that many devices connect to hospital networks. "It's a huge effort," Hewitt says. "It is one of several controls that can help mitigate technical risks. However, it does nothing to mitigate physical risks."

NeSmith also recommends a separate network—or potentially, several networks—with robust firewalls. "That way, you can control what is able to talk to those devices," he says. "Sequestering a network limits where a person can get if they get inside." It's important to limit and control which devices can join these networks, he adds.

In addition, health care entities need to put in place a patch management system, along with some sort of maintenance schedule, Hewitt says.

Finally, they need to beware of theft. "Another huge issue is the theft of these devices," Hewitt says. Most organizations train their employees to carefully track laptops and thumb drives that contain patient data, but they don't keep as careful an inventory of biomedical devices, which may be borrowed informally between departments and transported from floor to floor at a hospital, he says.

Hewitt says responsibility for biomedical security ultimately belongs to the organization's CEO and requires a multidisciplinary team to solve.

Contact Hewitt at clyde.hewitt@cynergistek.com, Shindell at rshindell@carosh.com and NeSmith via spokesperson Cara LaMaina at lamaina@merrittgrp.com. ✧

## New CAP Calls for Compliance Rep, External Assessor

The most recent settlement between a HIPAA covered entity (CE) and the HHS Office for Civil Rights (OCR) calls for an extensive, three-year corrective action plan (CAP) (see story p. 1).

In several ways, the CAP deviates from the norm. Among the unusual requirements in the CAP that accompanied 21st Century Oncology's (21CO) $2.3 million settlement are the hiring of an external "assessor" who must make surprise visits to the practice's locations, submission of 21CO's business associate agreements (BAAs), and reporting to OCR all violations of HIPAA policies and procedures.

The CAP makes repeated references to electronic protected health information (ePHI), though as a CE, 21CO and its workforce are required to safeguard protected health information (PHI) regardless of where it is used or disclosed, including on paper. A review of the CAP may be a useful exercise for CEs and business associates (BAs) as it lays out OCR's current thoughts on compliance and oversight, spelling out strategies these organizations can adopt to ensure their own efforts are up to snuff.

The following are highlights of the CAP.

◆ 21CO is required to appoint a compliance representative (CR) who "shall be responsible for assuring 21CO's compliance with this Agreement and the CAP and for arranging for the provision of such assistance as 21CO may require to comply with the Agreement and the CAP, including, but not limited to, arranging for and/or providing policies, procedures, training and internal monitoring services, and including after resolution of 21CO's bankruptcy." The CR must be "knowledgeable about the HIPAA Rules and about the policies and practices of 21CO with respect to" ePHI.

◆ In addition to the CR, 21CO is required to name an external assessor, as noted earlier. This is the first action in the CAP that has a deadline—the individual must be selected within 60 days of the effective date of the CAP. OCR must approve the choice of a "qualified, objective, independent third-party assessor" whose duties include monitoring compliance with the CAP and writing reviews and reports. OCR is requiring that a proposed assessor "certify in writing at the time of his, her or its designation, and must provide reasonable written documentation to the effect that he, she or it has the requisite expertise and experience regarding the implementation of the HIPAA Rules and has the necessary resources and is otherwise able to perform the assessments and reviews described herein in a professionally independent fashion, taking into account any other business relationships

*continued on p. 9*

*continued from p. 8*

or other engagements that the individual or entity may have." HHS also reserves the right to interview the assessor, who cannot be removed without OCR approval.

◆ Within 120 days, 21CO must conduct a risk analysis and develop a corresponding risk management plan. The analysis must be "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability" of ePHI. Then 21CO is to "document the security measures 21CO implemented or is implementing to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level." The analysis and plan are due to OCR within 120 days of the effective date of the CAP.

◆ Once the analysis and plan are approved by OCR, 21CO has 90 days to "revise its policies and procedures" to address a number of activities. Policies must require "regular review of audit logs, access reports, and security incident tracking reports" and to specify "protocols for access to 21CO's ePHI by affiliated physicians, their practices, and their employees."

◆ HHS will review the new policies and procedures and may require changes, which 21CO must make within 30 days.

◆ After final OCR approval, 21CO has 30 days to "finalize and officially adopt the policies and procedures" and distribute them to appropriate workforce members. New workforce members must receive the policies within 15 days of starting at 21CO.

◆ Policies must be "routinely" reviewed and revised as needed "to reflect changes in operations at 21CO, federal law, HHS guidance, and/or any material compliance issues discovered by 21CO that warrant a change in the policies and procedures."

◆ Within the first 120 days during which the risk analysis and compliance plan are being developed, 21CO is to send OCR information on its BAs. Specifically, OCR wants names, "a description of services provided, a description of the business associate's handling of 21CO's PHI" and the "date services began." OCR is also requiring copies of BAAs.

◆ After being hired, the assessor has 60 days to submit to OCR and 21CO "a written plan, describing with adequate detail, the Assessor's plan for fulfilling the duties" spelled out in the CAP. The plan is to be reviewed "at least annually," with any changes sent to OCR for approval.

◆ To "make specific determinations about 21CO's compliance with the requirements of this CAP," the assessor will "perform unannounced site visits to the various 21CO facilities and departments," hold "quarterly progress meetings with 21CO's key management, including the CR, Privacy Officer, Security Officer and any other appropriate personnel; interview workforce members, employees of affiliated physician practices, and business associates as needed; and follow up on reports of noncompliance with the CAP."

◆ The assessor is required to submit reports to OCR and 21CO at the one-, two-, and three-year anniversaries of his or her hiring, which are due to OCR within 60 days of those occasions. The CR at 21CO has 60 days to respond to the assessor's reports, "including, when appropriate, a plan of correction." Should the assessor find a "significant violation," 21CO is to respond within 30 days.

◆ OCR also provides specifics as to the content of the annual reports, which must include an "attestation signed by the CR attesting that the revision or implementation of policies and procedures required under this CAP: (a) have been adopted; (b) are being implemented; and (c) have been distributed to all 21CO workforce members, workforce members of affiliated physician practices, business associates, and vendors." In addition, the report must spell out all reportable events that occurred and "any corrective or preventative action(s)" that 21CO took as a result.

◆ Internal monitoring plays an important role in the CAP. Within 60 days of the effective date, 21CO must submit to OCR for approval its "internal monitoring plan."

◆ Guidelines for internal reporting are also part of the CAP. 21CO must require members of the "workforce who have access to ePHI to report to the CR at the earliest possible time any violation of 21CO's policies and procedures related to the HIPAA Rules of which they become aware," although presumably they must report inappropriate uses and disclosure of all PHI. The reporting policy is to be submitted to OCR for approval within 60 days of the agency's sign-off of the internal monitoring plan.

◆ The CAP requires 21CO to "promptly investigate the allegations raised and shall document each investigation in writing. If 21CO determines that a member of its workforce has failed to comply with 21CO's policies and procedures related to the HIPAA Rules, the CR shall notify both the Assessor and HHS in writing of the finding within thirty days of such determination."

◆ Finally, the CAP notes that OCR retains its enforcement authority. "The use of an assessor does not affect or limit, in any way, HHS's authority to investigate complaints against 21CO or conduct additional compliance reviews of 21CO under any applicable statute or regulation that HHS administers."

For more details, see https://tinyurl.com/y7nufhet.

## Calling Texting 'Essential,' CMS Clarifies Uses, Required Safeguards

Hospital compliance officers have been whipsawed recently over whether the HHS Centers for Medicare & Medicaid Services (CMS) forbids the texting of protected health information (PHI), even when it is secure.

But a new memorandum "clarifying" the issue now states when texting is allowed, giving some assurance to hospitals and other HIPAA covered entities (CE) whose providers rely on this speedy and ubiquitous communication method.

On Dec. 18, *Report on Medicare Compliance*, a sister publication to *RPP*, broke the news that officials within a division of CMS had sent emails to at least two hospitals saying that "texting is not permitted"—an edict they said was applicable even when secure text messaging programs are used.

The "hospital team" from CMS's Survey & Certification Group cited concerns about privacy, security and the integrity of medical records as the reason for the ban, which effectively reversed CMS's position that secure texting was allowed with one exception.

"After meeting with vendors regarding these products, it was determined they cannot always ensure the privacy and confidentiality of PHI…being transmitted. This resulted in the no texting determination," CMS said in the Nov. 30 email obtained by *RMC*.

CMS seemed to make clear that texting was a no-no.

"At this time, CMS does not permit the use of texting. The receiving or sending phones may not always be secure and encrypted, the privacy of the patient and his/her personally identifiable information (PII) cannot be guaranteed, and the sender or receiver cannot always be identified potentially exposing PHI/PII. In addition, the information contained in the text messages would be required to be entered into the patient's medical record and available for retrieval," emails to the hospitals viewed by *RMC* said.

This position looked like an extension of CMS's stance on the texting of physician orders, which it does not permit. In the hospitals' emails, CMS repeated that policy, so there was no apparent change for these types of texts.

In comments to *RMC*, experts bemoaned the seeming ban on all other forms of texting, with one terming it "almost like a return to the Dark Ages."

But a little more than a week later, CMS appeared to reverse itself, or at least, harmonize the agency's position with what it had been all along.

On Dec. 28, CMS posted an announcement from the director of the Survey & Certification Group under a section on its website titled "Policy & Memos to States and Regions," which contains "memoranda, guidance, clarifications and instructions to State Survey Agencies and CMS Regional Offices."

The title of the memorandum is "Texting of Patient Information among Healthcare Providers."

In sum, it states:

◆ "Texting patient information among members of the health care team is permissible if accomplished through a secure platform.

◆ Texting of patient orders is prohibited regardless of the platform utilized.

◆ Computerized Provider Order Entry (CPOE) is the preferred method of order entry by a provider."

"CMS recognizes that the use of texting as a means of communication with other members of the healthcare team has become an essential and valuable means of communication among the team members. In order to be compliant with the CoPs [conditions of participation] or CfCs [conditions for coverage], all providers must utilize and maintain systems/platforms that are secure, encrypted, and minimize the risks to patient privacy and confidentiality as per HIPAA regulations and the CoPs or CfCs," the Dec. 28 memo states. "It is expected that providers/organizations will implement procedures/processes that routinely assess the security and integrity of the texting systems/platforms that are being utilized, in order to avoid negative outcomes that could compromise the care of patients."

### Records Requirements Apply

This new memorandum provides an opportunity for hospitals and other CEs to assure that their texting meets CMS's requirements, which address storage requirements as well as security.

As noted, the prohibition against physician ordering by text remains in force.

But if texting is employed for other uses, hospitals must have a way to capture the texts so they can be part of the patient's medical record, both inpatient and outpatient. Regarding medical records, these "must be accurately written, promptly completed, properly filed and retained, and accessible. The hospital must use a system of author identification and record maintenance that ensures the integrity of the authentication and protects the security of all record entries," CMS states, citing its "form and retention of record" standard.

Records "must be retained in their original or legally reproduced form for a period of at least" five years. Additionally, the hospital "must have a procedure for ensuring the confidentiality of patient records," the Dec. 28 memorandum continues. "Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain

access to or alter patient records. Original medical records must be released by the hospital only in accordance with Federal or State laws, court orders, or subpoenas."

Finally, CMS's "content of record" standard is also applicable, which requires that records document, as appropriate, "evidence" of "all practitioners' orders, nursing notes, reports of treatment, medication records, radiology, and laboratory reports, and vital signs and other information necessary to monitor the patient's condition."

### Kudos for Speedy Response

So what happened? This could be a case of one hand not knowing what the other was doing.

Once the *RMC* story was published, CMS got more questions about its position on texting, including one from Ronald Hirsch, M.D., vice president of regulations and education at R1 Physician Advisory Services.

In response to his query, Hirsch received an email stating that agency officials were "working with internal CMS components to provide a unified, consistent response to the numerous issues regarding the use of texting platforms," and promising to contact him "once the process and response is complete."

A few days later he was emailed the new memorandum. Even though the issue was confusing, Hirsch praises CMS for the speed with which it resolved the conflict.

"I have never seen CMS respond so quickly to an issue," he tells *RPP*. "They clearly realized that one of their survey staff was improperly interpreting the CoP and CfC by informing hospitals that all texting was prohibited."

To view the new memorandum, visit https://tinyurl.com/yc5wopne. For more information about *RMC*, including how to subscribe, see https://tinyurl.com/ybhxsewy. Contact Hirsch rhirsch@r1rcm.com. ✧

## 'Criminal Intrusion' Prompts Settlement

*continued from p. 1*

In the settlement, OCR describes 21CO as a "provider of cancer care services and radiation oncology. With their headquarters located in Fort Myers, Florida, 21CO operates and manages 179 treatment centers, including 143 centers located in 17 states and 36 centers located in seven countries in Latin America."

The 21CO breach that triggered OCR's investigation is the second largest to result in a settlement. According to OCR, 21CO reported that the records of 2.2 million patients "may have been affected" in 2015 as the result of what 21CO termed a "criminal intrusion" of a server.

In 2016, Advocate Health Care paid OCR $5.5 million following the theft of desktops containing the protected health information of 4 million people (*RPP 9/16, p. 1*).

21CO appears to have learned of the breach in something of a novel way. While it has become common that exposed data ends up on the internet—flagged by a patient or other individual—in this case the FBI, on two occasions in 2015, told 21CO it had been victimized. OCR's press release about the settlement says an FBI informant (i.e., "unauthorized third party") bought patient records. No other details are disclosed, such as where the information was offered for sale or the purchase price. This situation is every HIPAA compliance officer's worst nightmare.

On both Nov. 13 and Dec. 13, the FBI "notified 21CO that patient information was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant. As part of its internal investigation, 21CO hired a third party forensic auditing firm in November 2015. 21CO determined that the attacker may have accessed 21CO's network SQL database as early as October 3, 2015, through Remote Desktop Protocol from an Exchange Server within 21CO's network. 21CO determined that it is possible that 2,213,597 individuals may have been affected by the impermissible access to their names, social security numbers, physicians' names, diagnoses, treatment and insurance information," the settlement states.

21CO itself did not report the breach to OCR until March 4, 2016, with a delay due to its investigation.

OCR says 21CO:

- "failed to implement certain security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 C.F.R. § 164.306(A)."
- "failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."
- "disclosed protected health information to a third party vendors (sic), acting as its business associates, without obtaining satisfactory assurances in the form of a written business associate agreement (BAA)."

The settlement makes no other mention of a missing BAA, but this finding has appeared in previous settlements with other covered entities. Notably, the lack of a BAA was the sole alleged problem cited in OCR's April 20, 2017, $31,000 settlement with the Center for Children's Digestive Health of Chicago.

A company spokeswoman who referred to the breach as a "criminal intrusion" told *RPP* that ensuring the privacy and security of its data is a priority and that the organization will take the actions required under the CAP.

"Protecting our patients' information and data is a key priority for 21st Century Oncology," the spokeswoman told *RPP* in a Dec. 29 email. "Since the criminal intrusion into one of our databases, we have invested in upgrading and improving our privacy safeguards and security

systems. We will continue to work on maintaining best in class security measures to ensure all of our databases are fully protected going forward."

The spokeswoman told *RPP* that 21CO had already paid OCR the $2.3 million, an amount which she said was "negotiated" with OCR. She added that 21CO "did have insurance to cover this." Court documents indicate the OCR payment came from a policy purchased from the Beazley Group, Inc.

### More Challenges Lie Ahead

The OCR settlement is almost the least of 21CO's recent woes. On Dec. 12, the Department of Justice (DOJ) announced it had settled with 21CO for $26 million stemming from admitted and alleged violations of laws. 21CO disclosed to the government that its physician groups had falsified data related to the performance of electronic health record systems.

This settlement also resolved allegations made by a whistleblower that it had violated anti-kickback laws. For more information, see https://tinyurl.com/y7lewthf. The December settlement with DOJ is the latest of several False Claim Act cases involving 21CO and physicians who had been affiliated with it that have now cost upwards of $80 million to resolve.

Additionally, 21CO filed for bankruptcy in May of last year, which meant the judge in that case had to approve the OCR settlement (and those with DOJ), the company spokeswoman told *RPP.*

The bankruptcy will not affect 21CO's ability to fulfill the requirements under the CAP, according to a company spokeswoman.

"While the company is currently in Chapter 11 reorganization, it remains fully operational and intends to comply with the corrective action plan negotiated with the OCR," she said.

According to the spokeswoman, 21CO is nearly finished with its reorganization. "The company expects to complete its financial restructuring and emerge from Chapter 11 as early as next month," she said.

However, 21CO still has at least one more challenge ahead. After the breach was disclosed, 21CO was sued by numerous individuals. "The breach litigation is ongoing," the spokeswoman said. ✧

## *PRIVACY BRIEFS*

◆ **An employee of Washington Hospital in Washington, Pa., who underwent surgery and allegedly was photographed during, has filed suit against the hospital, a doctor and several coworkers, saying photos of her genitals were shared.** Operating room unit secretary Sheila Harosky was undergoing hernia repair in September 2016 when a scrub nurse used a cell phone to photograph her exposed genitals and then shared the photos, the suit said. The hospital disputed the version of events, saying Harosky "initiated and participated in the circumstances giving rise to her lawsuit by bringing fake intestines into the operating room and requesting that they be placed on her abdomen at the time of the surgical procedure as a practical joke on her friends, co-workers and surgeon." Harosky is seeking more than $75,000 in damages. Learn more details at http://bit.ly/2qmblkt.

◆ **A person dropping off trash at a recycling center in Allentown, Pa., discovered medical records with clearly visible identifying information and sensitive protected health information among the recyclable papers.** Nearly all the visible records were printed on letterhead from Women's Health Consultants, a now-closed practice, according to *The Morning Call* newspaper. A city employee, alerted to the problem, buried the sensitive documents deeper in the trash until the container could be transported to the recycling company. View the story at http://bit.ly/2AtAiMc.

◆ **The Oklahoma Department of Human Services (HHS) is issuing a second breach notification to 47,000 clients because the first notification didn't meet HIPAA regulations.** An unauthorized user accessed a computer with protected health information at Carl Albert State College in Poteau, Okla., in April 2016, and clients whose personal information may have been compromised were notified in August 2016. However, the federal HHS wasn't properly notified at that time. Once HHS was notified, it told the state it needed to send a second notice to those involved. Read more at http://bit.ly/2ApJRtP.

◆ **A dental practice in Reno, Nev., fell victim to a ransomware attack in October.** Wager Evans Dental was targeted on Oct. 30 and didn't regain access to its records until Nov. 4. The practice says that two computers were affected by the ransomware, affecting access to the patient database and imaging files. The database contains names, addresses, dates of birth, Social Security numbers, along with diagnoses and treatment plans. Learn more at http://bit.ly/2lW4Fnt.