Report on
Patient Privacy

Volume 18, Number 4 • April 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

To Stem Opioid Crisis, OCR Promises Rule on Sharing, Urges Entities to 'Get the Word Out'

Allowing providers to more easily share information with family members whose loved ones become incapacitated due to opioid use is the impetus for a new proposed rule the HHS Office for Civil Rights (OCR) is drafting.

Referring to family members as "often the last best hope" for those struggling with opioid addiction, Director Roger Severino filled in some blanks about this and another proposed rule regarding notices of privacy practices (NPPs) during a recent keynote address at the HIPAA Summit in Washington, D.C. In March, *RPP* reported that these were in development (*RPP 3/18, p. 5*). Severino also gave an update on some staff changes and other OCR activities.

OCR's efforts respond to the need for parents—"often the last best hope"—of adult children treated for substance use to learn of the child's diagnosis and treatment when he or she "is in such dire circumstances," Severino said. OCR, he said, is seeking to combat the "many myths surrounding the interaction of our health information privacy laws and difficult circumstances, especially related to opioids" and assist providers with sharing information while complying with HIPAA.

"Far too often, we've seen examples where medical providers err so far on the side of caution that the patients do not necessarily get the best treatment" if their family members who want to be involved are shut out, he said.

Opioid abuse is "not just a medical problem, it's a societal problem, it's a family problem. It needs to be addressed on all fronts," said Severino. To date, OCR has been doing its "part to try to make sure that folks are aware of what doctors can say in those situations to make sure that loved ones are brought in" and now believes a proposed rule is required.

continued on p. 9

Prepare for Ransomware Attack With Archived Forms, Offline Records, and Constant Practice

Hackers hit the 911 emergency system of Baltimore, Maryland; the city of Atlanta, Georgia; and Boeing Co. with ransomware demands late last month. Experts warn that health care entities need to rehearse their responses to potential ransomware attacks, and keep offline backups of everything.

"If you want to prepare to deal with a ransomware attack, our organizations need to practice disaster recovery and business continuity," says Joseph Kirkpatrick, managing partner for KirkpatrickPrice in Tampa, Florida. "The more you practice, the better you'll get at it and the faster you'll be able to recover. How do you go from having all your systems down to getting back up again? You're talking about an IT staff that will be taxed. This is why you need to practice the whole thing."

International rings of opportunists are deploying increasingly sophisticated ransomware attacks, and government services, schools and hospitals have been particularly hard hit so far in 2018.

continued

For example, in Atlanta, the hackers released the malware SamSam, which also was blamed for a major ransomware attack on Erie County Medical Center (ECMC). SamSam is estimated to have facilitated the extortion of more than $1 million from 30 organizations this year and is known to be used against targets most likely to pay the ransom. Hospitals are high on the list of targets, Kirkpatrick says.

Atlanta's ransomware attack began on March 22 and shut down applications city residents use to pay bills and access court-related information. Ten days later, the Municipal Court of Atlanta was rescheduling hearings, and city residents couldn't pay traffic tickets and water bills. No health-related apps were reportedly involved. Baltimore's ransomware attack, meanwhile, shut down its 911 dispatch system for 17 hours beginning March 25. Some Boeing computers were hit by the WannaCry malware on March 28.

Other ransomware incidents affecting health care entities have included last year's more widespread WannaCry attacks and Petya/NotPetya attacks. The WannaCry incidents mostly passed over U.S.-based health care entities but hit the U.K.'s National Health Service hard, knocking many NHS offices offline for several days or more (*RPP 6/17, p. 1*). The Petya attacks caused damage that required at least one hospital to replace parts of its computer systems.

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.

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, as well as a searchable database of *RPP* content and archives of past issues at hcca-info.org.

To order an annual subscription to **Report on Patient Privacy** ($482 for HCCA members; $554 for nonmembers), call 888.580.8373 (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.

Although phishing is the primary method of attack for ransomware—53% of all email threats are phishing, and 75% contain a malicious URL, according to the Microsoft Security Intelligence Report—a study released in March by the consulting firm Accenture indicates that attacks also come from insiders.

The study surveyed 912 employees of health care entities (both payers and providers) in the United States and Canada. It found that 18% of those surveyed said they would be willing to sell confidential data to unauthorized parties for as little as $500 to $1,000. The remaining 82% said no amount of money would make them sell.

The problem was most acute among provider organizations, where 21% of those surveyed said they'd sell access. Staff with the most frequent cybertraining was more likely, not less, to sell access, the study found. "Access" could include handing over login credentials, installing tracking software and downloading data to a portable drive, among other actions.

Just about everyone surveyed—99%—said they felt personally responsible for keeping data safe, but that wasn't enough to deter some from trading on their positions: 24% of the health employees said they actually know of someone in their organization who already has sold their credentials or access to an outsider.

Health care entities should move aggressively to make sure they're ready in the event of their own possible ransomware attack. Kirkpatrick says, referencing the Accenture survey, "Attacks are going to happen, because many of your coworkers let them in."

Practice Using Paper Processes

To prepare for a ransomware attack, health care entities need to know how to conduct business without their computer systems. That requires preparation and lots of practice.

For example, backups are key, but only if they work. "Are your backups tested?" Kirkpatrick asks. "Have you practiced restoring your backups? Do you have offline backups?" If your organization has an offline copy, you should practice restoring that copy, he says.

Business continuity also is key, because everything will need to return to paper records until you're back online, says Kirkpatrick, who spoke March 28 at the National HIPAA Summit. He suggests that health care entities ask themselves:

- Are manual procedures available and practiced?
- Has the company done a business impact analysis in order to find the critical processes that would need to continue on a daily, weekly and monthly basis?
- Does the company know how it will pay employees manually?

ECMC, a 1,000-bed hospital and Level 1 trauma center with 300,000-plus outpatient visits and more than 12,000 surgeries a year, was hit with ransomware in early April 2017, Reg Harnish, CEO of GreyCastle Security, told meeting attendees. The hackers demanded 24 bitcoins—about $44,000 at that time—to ransom the records.

ECMC didn't pay the ransom, says Harnish, who was the incident commander for the case, running a response team that included the FBI and the board of ECMC. Instead, ECMC, which had more than 6,000 compromised assets, spent 13 days offline and 45 days recovering.

Strategies Prevented a True Breach

Following an extensive investigation, the hospital system also was able to declare that no medical records were breached during the attack. ECMC "did a lot of things right," Harnish says.

This included:

◆ Deploying an immediate incident detection and response; within four hours of the first help desk query, the organization had a response team deployed.

◆ Creating an emergency management plan prior to the incident.

◆ Maintaining offline backups.

◆ Running an excellent public relations initiative; instead of hiding the problems, ECMC officials fully disclosed them, and "it actually earned them a lot of good will," Harnish says.

Because of planning and quick response, the ransomware incident had "a negligible impact to patient care—there were no rescheduled surgeries or appointments," Harnish says. "They were fine with operating on paper records. In addition, the forensic investigation showed that "while there was exposure [of protected health information], we were able to determine it did not qualify for what OCR and others consider a breach."

ECMC and other ransomware attacks point out the need to prepare for a worst-case scenario: compromised systems that force the use of paper records and loss of online backups. Harnish says that health care entities should:

◆ Know how to activate the response plan, especially for electronic protected health information (PHI).

◆ Initiate an immediate lockdown of online connections.

◆ Decide on a community relations strategy early, and ensure people are well versed in crisis communications.

◆ Identify and employ an attorney who is fluent in health information.

◆ Make sure to document everything.

◆ Understand that the entity's response will be closely scrutinized following the incident.

"Assemble the right team," Harnish says. "We had a command center set up, and that's really important." It's also critical for first responders to know how to shut down all internet access, he says. "Externally, ECMC was disconnected from the internet for 45 days." It might take physically removing a cable to shut down all online access, he notes.

GreyCastle Security never recommends that an entity pay the ransom demanded, Harnish says.

"That being said, there are cases where we will support clients" who decide to pay ransom. This could take more legwork than expected, he says, adding that most people don't realize that it's possible to accumulate only a certain amount of bitcoin per day, so it may not be possible for an entity to pay ransom immediately.

Previous Attacks Offer Strategies

Still, even in the absence of paid ransom, a ransomware attack is costly. ECMC spent $10 million on its response effort, Harnish says. Target Corp.'s breach in 2013 ultimately cost it $1 billion, he says.

Other ransomware attacks also provide lessons learned. For example, Princeton Community Hospital in Princeton, West Virginia, recovered more quickly from its ransomware attack in June 2017 because Linda Cunningham, administrative assistant to the vice president of patient care services, had kept the templates of all the old paper forms and archived them in a binder, Kirkpatrick says. "They copied those forms, and that's how the hospital ran for six weeks," he says. "It's not IT; it's people like Linda."

Ultimately, Princeton, which fell victim to a strain of the Petya malware, replaced all its hard drives and built a new network, hospital officials said.

The Accenture study touched on areas beyond ransomware and other external threats. It indicated that basic concepts of cybersecurity—such as not keeping passwords on monitors—may need to be stressed more to employees in order to protect against ransomware and other cyberthreats. The study found that 21% of employees write down their username and password near the computer. Again, those who worked for providers were significantly more likely to do this: 23% of provider employees kept their username and password near their computer, while 17% of payer employees did so.

Accenture also reported that nearly half of health care employees say they are aware of patient data breaches in their organization. In fact, 1% of payer employees and 4% of provider employees say they know of 10 or more data breaches within their own organization.

Training was widespread among those surveyed, but one in six said they were unaware of training at their own organization, or that their organization didn't

offer training at all. A significant minority—29%—say they only received training once. Nearly one in three health care employees question the effectiveness of cybersecurity policies in their organizations, and 15% to 20% admit to poor compliance with key policies, such as downloading email attachments and software, secure password management and using insecure networks, according to Accenture. Any of these are a risk for ransomware or other cyberthreats.

Younger Workers Pose Risk

Studies show that it's not the older workers who fall for phishing and other hacks, Kirkpatrick says. Instead, it's the younger workers. For example, a study from the Federal Trade Commission found that 18% of adults over 70 are victims of fraud, compared to 40% of adults ages 20 to 29.

"Millennials are killing us," Kirkpatrick says, adding that health care entities need to train their workforces more effectively. "Our workforce demographics are changing rapidly, and it turns out we need to train them on security fundamentals."

Finally, Kirkpatrick recommends pushing back against the notion that people are "the weakest link" in keeping PHI safe. "Our people are our first line of defense," he says.

Read the Accenture cybersecurity survey at https://accntu.re/2F69Nhm. Contact Harnish at 518-274-7233 and Kirkpatrick via KirkpatrickPrice media relations at media@kirkpatrickprice.com. ✧

Enhanced Review of External Access To EHRs Can Help Thwart Breaches

When patients complain to hospitals that their privacy has been compromised, sometimes the trail of bread crumbs leads to independent physician practices, which often are granted access to the hospital's electronic health records (EHRs) for patients they share. An employee or the physicians themselves may have snooped on a hospital patient, or access may continue after an employee leaves the practice, an invitation for breaches. Without a direct way to enforce HIPAA at independent practices, some hospitals are stepping up their management and oversight of users' access to protected health information (PHI) in the hospitals' EHRs.

"Many health systems grant physician offices access to their computer systems. There is a need to ensure the physician and any office staff have a business need to have that access," says Brian Kozik, chief compliance officer at Lawrence General Hospital in Massachusetts. "We rely on the practice management to conduct HIPAA training which, in an office practice, must clearly highlight no sharing of passwords and no leaving computers logged on. All of this is out of our control."

That hasn't always gone off without a hitch. Recently, Lawrence General Hospital received a HIPAA privacy complaint about a test result, and the hospital tracked it to an independent physician practice. It turned out an employee left their computer on, and another used it to access hospital records. In response, the hospital shut down the practice's access to its EHR system, and the physician fired the employee who snuck into the records. The experience illustrated the importance of monitoring and identifying improper access by physician offices.

"Because we offer outside entities access to our electronic health records, the natural result is you have a higher frequency of inappropriate access," says David Behinfar, chief privacy officer for UNC Health Care System. "It's for a common patient, so we want to give physician practices access so they can follow up for treatment purposes, but we have to step up and manage that information appropriately."

Lawrence General Hospital has a new process to minimize the risk posed to hospital EHRs by independent physician practices, which are allowed to log in to a secure remote site and access read-only versions of their patients' medical records. Maria Palumbo, the hospital's privacy officer, and Alexander Laham, its information security manager, are meeting with practice managers to discuss HIPAA obligations, and all practice employees must sign a remote user access request form and confidentiality agreement (see templates, pps. 5, 6). If they don't, their access is terminated. New hires also must agree to the terms.

The form requires the practice managers to notify Lawrence when employees are terminated so they can be deactivated. Employees who are inactive for 60 days also are cut off on the assumption the employee is gone but the practice forgot to tell, Laham says. "If they are not using it, there is a vulnerability," he explains.

At UNC Health Care System in Chapel Hill, independent physician practices have limited access to patient records at the hospital through CareLink, which is part of Epic, Behinfar says. The practices sign an agreement with the hospital to view the records of patients they have in common. After the agreement is in place, the hospital sets up accounts for practice employees. They are required to enter two patient identifiers (e.g., name and Social Security number), which prevents snooping into the medical records of patients who aren't part of the practice, including VIPs, he says.

The practices agree to only access patient records for treatment purposes and to manage their users. For example, they will notify UNC Health Care System when

continued on p. 7

Protecting Hospital PHI When It's Shared With Independent Practices

These templates can help hospitals develop remote user system access request forms and confidentiality agreements for independent physician practices that are allowed to access the hospital's electronic health record systems for patients they share, says Alexander Laham, information security manager at Lawrence General Hospital in Massachusetts. Contact him at alexander.laham@lawrencegeneral.org.

YOUR LOGO HERE

REMOTE USER SYSTEM ACCESS REQUEST FORM

FAX DIRECTLY TO INFORMATION SYSTEMS at (XXX) xxx-xxxx

Personal Information: **ALL FIELDS in this box are required** **PLEASE PRINT CLEARLY**

Last Name: _____ Middle Initial: ___ First Name: _____

Position/Title: _____ Practice or Office Name: _____

Office Address: _____ Phone: _____ Email: _____

Supervisor Name: _____ Supervisor Phone: _____ Ext.: _____

Supervisor Email: _____

User Start Date: _____

Reason for Request:

_____

_____

_____

Access Request: MUST BE FILLED OUT CORRECTLY FOR PROPER ACCESS PLEASE PRINT CLEARLY

☐ New User ☐ Existing User/Job Change

☐ {*Medical Record*} ☐ Other:_____

In the event of termination, please fill out this section and forward form to the following contacts.

Termination:

☐ Scheduled Termination ☐ Immediate Termination

IS Management needs to be notified immediately upon termination as part of the termination process.

Please email:

{Name of Contact} Person@yourorganization.org

{Name of Contact} Person@yourorganization.org

By signing this request form, I acknowledge that I have reviewed and understand the confidentiality statement and all applicable standards.

Remote User Signature: _____ **Date:** _____

Supervisor: By signing this request form, I validate that this Remote User has a valid, business related reason to access *{COMPANY}* systems and I agree to immediately notify *{COMPANY}* Information Services if this Remote User is terminated or no longer requires remote access to *{COMPANY}* systems.

Supervisor Signature: _____ **Date:** _____

Note: Supervisor Signature required for remote access request

Please return to *{COMPANY}* **Information Systems** Rev 1.2018

REMOTE OFFICE USER
CONFIDENTIALITY AGREEMENT

I understand that *{COMPANY}* has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information. Additionally, *{COMPANY}* must assure the confidentiality of its human resources, clinical, payroll, fiscal, computer systems, and management information (collectively, "Confidential Information").

In the course of my duties, as a remote user of *{COMPANY}* systems, I understand that I may come into the possession of Confidential Information while accessing designated computerized information systems.

I further understand that I must sign and comply with this agreement to get authorization for access to any of *{COMPANY}* Confidential Information.

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it. In addition, I understand that my personal access code, user ID(s), and password(s) used to access computer systems are also an integral aspect of this Confidential Information.
2. I will not access or view any Confidential Information, or utilize equipment, other than what is required to do my job.
3. I will not access my own patient account/medical record or that of family or friends. I understand I have a right as a patient to view this information, but must do so through the proper channels via the medical records department or my physician for the medical record, and patient accounting for billing information.
4. I will not discuss Confidential Information where others can overhear the conversation (for example, in hallways, elevators, in the cafeteria, on public transportation, in restaurants, and at social events). It is not acceptable to discuss Confidential Information in public areas even if a patient's name is not used. Such a discussion may raise doubts among patients and visitors about our respect for their privacy.
5. I will not make inquiries about Confidential Information on behalf of other personnel who do not have proper authorization to access such Confidential Information.
6. I will not willingly share my computer password or knowingly use another person's computer password instead of my own for any reason.
7. I will not make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information in *{COMPANY}* computer system. Such unauthorized transmissions include, but are not limited to, removing and/or transferring Confidential Information from *{COMPANY}* computer system to unauthorized locations using any type of portable media.
8. I will log off any computer or terminal prior to leaving it unattended as to prevent unauthorized use of my user account.
9. I will comply with any security and privacy standards outlined in this agreement promulgated by *{COMPANY}* to protect the security and privacy of Confidential Information.
10. I will immediately report to my supervisor and/or *{COMPANY}* Information Services any activity, by any person, including myself, that is a violation of this Agreement. The transgression must be reported to the Information Security Manager for review.
11. I agree that my privacy obligations under this Agreement will continue after the termination of my employment/services.
12. I understand that my account will be disabled after 60 days of inactivity. Re-activation will require validation of identity via my supervisor and the *{COMPANY}* Information Services department.
13. I understand the violation of this Agreement may result in adverse action up to and including termination of my ability to work at or on behalf of *{COMPANY}*, and/or suspension and loss of privileges, in accordance with *{COMPANY}* Policies and Procedures. In addition, under applicable law, I may be subject to criminal or civil penalties.
14. I further understand that all computer access activity is subject to audit and the status of my employment with the remote office will be validated periodically.

By signing this document, I understand and agree to the following:
I have read the above agreement and agree to comply with all its terms.

Signature of remote user: _____

Print Name: _____ Date: _____

Company (*Office):* _____

Please return to *{COMPANY}* Information Systems Rev 1.2018

continued from p. 4

employees leave the practice or change job functions so their access can be shut down, Behinfar says.

Practices also have to notify the hospital of suspected breaches, including compromised user credentials. For example, if an employee's password was on a Post-it note stuck to his computer screen and someone else used it to access hospital records, the practice must inform the hospital. "Then we get to decide whether a breach and notification is appropriate," Behinfar says. "We don't want them making that decision. It's our information."

Practices Have to Take on Liability

Practices also indemnify UNC Health Care for breach notification costs and fines, which are circumscribed somewhat because the practices don't have access to hospital medical records beyond the patients they treat.

At both Lawrence General Hospital and UNC Health Care, compliance with the user agreements is enforced with the threat of shutting down access. "If we had an issue, we would demand the physician do a HIPAA refresher," Kozik says. "Our big stick is, we have the ability to shut down access."

That's not the road they want to travel because electronic access to patient records is better for everybody and because it may strain relationships with physicians, but sometimes it's necessary. Behinfar says privacy and compliance officers need the support of senior leadership when they're thinking of suspending a practice's remote access to EHRs. "With high-volume practices, that can have consequences," he notes.

The hospitals also use monitoring software for potential breaches, and that extends to independent physician practices. "We have a new system coming online, and that is one area we will focus on," Behinfar says. "The software will build a historical profile for every user." That makes it easier to identify deviations, such as users who access far more records than usual. Lawrence General Hospital also does concurrent audits of practices using its monitoring software, which runs 24/7, Laham says.

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.*

Hospital Workers Allege Biometric Scans Violate Privacy Law. On March 19, a putative class action was filed in Cook County Circuit Court against Illinois's NorthShore University HealthSystem (NorthShore) over claims that NorthShore's practice of requiring employees to scan their retinas or hands to gain access to restricted hospital areas violates the state's Biometric Information Privacy Act (BIPA), *Charles Thurman et al. v. NorthShore Univ. HealthSystem*, Case No. 2018CH03544. The named plaintiff, Charles Thurman, worked at NorthShore's Evanston, Illinois, hospital as a full-time director of security and public safety. As part of his qualification as a restricted access worker, he was required to scan his fingerprint and retina so that NorthShore could use them as authorization methods to allow access to restricted areas at the hospital. In the complaint, Thurman alleged that NorthShore's retention of his data put him and a putative class of restricted access workers at risk for identity theft. Workers may be exposed to "serious and irreversible privacy risks" if a biometric information database is hacked or breached due to the fact that biometric information is unique to the individual from whom it is collected. Thurman further alleged that NorthShore never properly informed him or the putative class in writing about the specific purpose for their fingerprint collection; the length of time that the workers' biometric data would be collected, stored and used; and what might happen to their biometric data if NorthShore merged with another company. He also alleged that NorthShore violated BIPA by releasing the biometric information to vendors. This action is the latest in a string of BIPA suits filed in Illinois state court. Nearly 100 such lawsuits have been filed in Illinois trial courts alone since September 2017. Experts say that the litigation trend may be due in part to the fact that plaintiff attorneys view BIPA claims as "low hanging fruit" given the availability of liquidated damages under the statute. Texas and Washington have passed similar laws regulating businesses' collection of biometric data, but unlike Illinois, Texas and Washington's BIPA statutes do not include a private right of action permitting individual plaintiffs to sue for violations—only the state attorneys general can enforce the law's requirements.

Training and oversight has to be continual, inside and outside the hospital, because there's so much information at everyone's fingertips, Palumbo says. When patients come to the hospital to complain that a friend or relative knows about their diagnosis, convinced it's the hospital's fault, Palumbo sometimes traces the breach to an affiliated physician practice—"someone with remote access." Often the physician is shocked; someone from his or her office has snooped, whether out of curiosity or concern or for darker reasons. "What happens across health care with the electronic health records is you find out more things than you want to uncover. It makes the hospital and physician very vulnerable," she says.

Contact Kozik at brian.kozik@lawrencegeneral.org, Laham at alexander.laham@lawrencegeneral.org, Behinfar at david.behinfar@unchealth.unc.edu and Palumbo at maria.palumbo@lawrencegeneral.org.

This article appeared in the Feb. 19, 2018, issue of *RPP*'s sister publication, *Report on Medicare Compliance*. For more information or to order, visit https://tinyurl.com/ybhxsewy. ✧

Privacy Officer Job Like Playing 'Whack-a-Mole' To Manage Risks

Serving as a chief privacy officer in this era of increased scrutiny and threats requires a keen understanding of all the places protected health information (PHI) can lurk—and potentially be exposed—in a large health organization.

That's the word from four chief privacy officers who spoke March 27 at the National HIPAA Summit. Still, they emphasized that it's probably not possible to address every threat, given the realities of staffing and budgets, so privacy officers need to identify their most important priorities. The privacy officers outlined what they consider their top targets.

"It's like playing whack-a-mole," says Shauna Van Dongen, chief privacy officer at Providence St. Joseph Health in Seattle, Washington.

The changing models in health care delivery lead to "an insatiable desire for information," says Van Dongen. "How do we allow access that's permissible, while still putting controls into place?" For example, she says, developers working on apps meant to be used in health care may never have worked in his industry before, and they may be surprised that email addresses used within the app are PHI.

Kimarie Stratos, senior vice president and general counsel/chief privacy officer for Memorial Healthcare System in Hollywood, Florida, notes that MHS is currently under a three-year corrective action plan (CAP) from the HHS Office for Civil Rights (OCR) that requires both an internal monitor and an external monitor. MHS entered into a settlement order that carried a $5.5 million payment following the 2011-2012 theft of patient data that resulted in identity fraud and the inappropriate access by current and former employees of an affiliated medical practice (*RPP 3/17, p. 1)*.

'Zero Tolerance Follows Settlement'

"Every Tuesday morning, our C-suite meets [on issues of privacy and security]," Stratos says. "For the next two years, we're really at an unbelievably heightened risk assessment stage." The OCR settlement was "a wakeup call that anyone can have," she says, noting that the breach was in a non-employed physician affiliate of MHS. Physician engagement on this issue is challenging, though, Stratos said, and it's something her organization continues to struggle with.

Stratos says that MHS is determined to have no health information issues "between now and the end of the CAP period."

To do that takes a strong training program, plus an attitude of zero tolerance from the top down, she said, adding that detailed workforce monitoring algorithms now check for snooping and other violations. "If you are snooping, you will be caught," she says. "I won't say it was well-received, but it has served its purpose."

Still, "you can't monitor everything," says Sheetal Sood, senior executive compliance officer for information governance at New York City Health and Hospitals Corp. She advises that health care entities focus their surveillance efforts on employees in two types of places: facilities that treat celebrities, and facilities that serve tight-knit communities.

Jana Aagaard, senior counsel for privacy/health information technology at Dignity Health in California, says her organization uses tabletop exercises to assess risk: "It gives a real nice sense of confidence, so we would not be just a deer in the headlights."

Aagaard says her department enlisted the marketing department to help with developing messaging around compliance and risk management, and it "seems to be pretty successful. Engage your marketers to help you."

OCR wants frequent risk assessment and mitigation, and "we've heard what OCR has been saying," says Aagaard. "We're paying a lot more attention. We're assessing more frequently, but we're finding it challenging." For example, she says, Dignity Health is not on one electronic health record platform, and each hospital has a different master patient index system and a different billing system.

Sood says that her office has broken the job of risk assessment down into "smaller chunks" based on OCR guidance, and organization privacy officials conduct "spot checks and mini-audits." For example, she says, her department might decide to target the radiology department one week, or might go into another department and check to see if all devices are secured.

"We'll do unannounced audits—we'll go up to the head nurse unannounced and ask 'Who is your privacy officer?'" she says. "We'll look at passwords on sticky notes on monitors; we'll check the shredder bins; we'll check the garbage."

Internet-connected medical devices also are a major focus, Sood says. "If you're managing a tracker device that can talk to the internet, then the internet can talk back. Medical devices are now increasingly connected and interconnected. As an organization, there's no shortage of risk."

Sood recommends sending out pre-contract questionnaires to uncover risks, and warned that organizations need to be willing to look elsewhere for services if the vendor comes up short.

Contact Van Dongen via Providence St. Joseph spokesperson Nisha Morris at 949-381-4782, Stratos at 954-265-6241, Sood via media relations at pressoffice@nychhc.org and Aagaard at jana.aagaard@dignityhealth.org. ✧

OCR Promises Rule on Sharing

continued from p. 1

A political appointee, Severino came on board OCR last spring. He made his first public remarks as director at the 2017 summit (*RPP 4/17, p. 1*). Before delving into the meat of his March 27 address, Severino quipped that time in the administration "is really like dog years, so it's been like seven years since I saw you last."

Severino's slides describe the "heightened concerns" the opioid abuse crisis and other "national health emergencies" have caused providers to experience. Concerns center on their:

◆ "ability to notify patients' family and friends when a patient has overdosed

◆ reluctance to share health information with patients' families in an emergency or crisis situation, particularly patients with serious mental illness and substance use disorder

◆ uncertainty about HIPAA permissions for sharing information when a patient is incapacitated or presents a threat to self and others."

In October, OCR issued a two-page document it called "clarifying guidance" created to "give medical professionals increased confidence in their ability to cooperate with friends and family members to help save lives (*RPP 11/17, p. 1*)."

A medical provider can disclose protected health information, without patient authorization, "to law enforcement, family and friends, if there is an imminent threat to health or safety. This can take the form of the person posing a threat to another. It can also take the form of the person posing a threat to themselves," Severino said.

"When there is an opioid crisis, and when a person—in a doctor's best medical judgement—is a threat to themselves, to their own health, and it is imminent," the provider "may disclose that fact to those who can help lessen that threat. In many cases, it is loved ones that are there who need to know [because they] could help intervene," he continued.

The situation should not be that a patient enters a hospital, is "stabilized," is discharged and then and has no further interactions with the health care staff until he or she overdoses again, said Severino.

OCR, Severino said, is "trying to spread the word that doctors have circumstances" under which they can share information with a patient's family without authorization "when it's in their best medical judgement to get them involved in their care."

Further, "doctors should feel comfortable" sharing information with any individuals that an adult patient has listed as an emergency contact on forms.

In the wake of the opioid crisis, officials believe they must clarify disclosures related to incapacity issues and "good-faith" provisions in the privacy rule. That's the purpose of the new proposed rule, said Severino.

"Currently there's a presumption of good faith when it comes to reporting an imminent threat to health or safety in our regulations. There is not that presumption when it comes to reporting [or disclosing protected health information] on cases of incapacity," Severino said, such as incapacity that results from an overdose.

Addressing the summit audience, Severino said the proposed rule would "create parity, to make sure that everything I just said to you is fully reflected in our regulations."

This would give health care providers "that confidence that they will be given the benefit of the doubt, that if they act in good faith, using their reasonable medical judgement" and make a disclosure to friends or family members, "we're not going to go after them," said Severino.

To view OCR's 2017 opioid guidance and related materials, visit https://tinyurl.com/ycjcmpav.

Turning to the second rule on OCR's to-do list, Severino indicated the agency is questioning the value

of NPPs. But it wasn't clear from his comments whether OCR has decided to simply do away with the requirement for patient acknowledgement of the NPP or if it might require covered entities to inform patients of the uses and disclosures and access rights through some other method.

"We're in a deregulatory environment generally, as an administration, so this is one opportunity to see if we could address the question of burden and also keeping in mind the value of informing folks of their rights to have their health information privacy protected," Severino said.

Patients sign a form indicating they have received the provider's NPP, but "very few people know what in the world it is they're signing," said Severino. "When you go in the doctor's office, you get a big stack of

OCR Offers Tips for Effective Contingency Plans

"Don't wait for a disaster to happen before designing and implementing a contingency plan."

That's the concluding sentence in the March newsletter issued by the HHS Office for Civil Rights (OCR), which provides monthly advice and information to HIPAA covered entities (CEs).

As the newsletter points out, having contingency plans "aren't just a good idea," but the security rule requires both CEs and business associates (BAs) to "establish and implement" them.

Because organizations are often consumed with daily HIPAA compliance tasks, this requirement doesn't always get the attention it needs. But contingency plans are becoming even more important as ransomware attacks grow (see story, p. 1). Affected CEs and BAs can survive such attacks—without paying a ransom—if they have adequate backup systems and can maintain access to patient records, devices and other functions that are tied to electronic networks that have become compromised.

The requirement for contingency plans is found under 45 CFR §164.308(a)(7), which states that plans would be activated in the following circumstances: "fire, vandalism, system failure, and natural disaster" (*RPP 6/16, p. 1*). The rule doesn't make mention of ransomware, as it was drafted years before these attacks were a fact of life in health care (and elsewhere).

The major purposes of the plan are to ensure "(1) the containment of damage or injury to, or loss of, property, personnel, and data; and (2) the continuity of the key operations of the organization," OCR's newsletter states.

As with most tasks under the security rule, the first step is to perform a risk analysis and corresponding risk management plan. "The end result of a risk analysis can provide a list of potential threats, risks, and preventative controls. Prioritization of critical systems and information will help identify where to focus [contingency] planning efforts," according to OCR.

The rule requires the following three components of a contingency plan:

◆ A disaster recovery plan "focused on restoring an organization's protected health data."

◆ An "emergency mode operation plan," also referred to as a plan for "continuity of operations." This is to be focused on "maintaining and protecting critical functions that protect the security of protected health data."

◆ A data backup plan, "focused on regularly copying protected health data to ensure it can be restored in the event of a loss or disruption."

CEs and BAs should develop "the specific guidelines, parameters, and procedures when enacting the contingency plan and for the recovery of systems and data," OCR advises. Considerations include identifying activities that "must be done during the first hour, day, or week," the types of events that will trigger the activation of the plan, as well as who in the organization "has the authority" to do so.

Don't forget to test the plan on a regular scheduled basis "to identify gaps and ensure updates for plan effectiveness and increase organizational awareness," says OCR. It should also be reviewed "when there are technical, operational, environmental, or personnel changes in the organization."

OCR recommends that the plan be integrated "into normal business operations." It also should be communicated to the workforce "in plain language so that it can be understandable to all types of employees."

This newsletter and other monthly issues can be found at the bottom of OCR's page on cybersecurity guidance at https://tinyurl.com/ycptkn6c.

forms, you're going through it, you just want to go see your doctor, especially if it's the very first time with a new practice." In this situation, many people may "sign whatever is put in front of them, not reading closely what it is," he said.

OCR has been told NPPs cause "a lot of confusion." It is not understood whether an NPP is a contract, a requirement for treatment, or actually "a waiver of your privacy rights." To the agency, one of the questions is, "what is the net benefit of having to collect and sign this form [to] the public?"

The proposed rule will look at "the necessity for having medical providers actually get their patients to sign the form, for them to retain the signed form, as opposed to other alternatives, such as just posting it in a very prominent place and leaving it at that, or oral communications," Severino said.

The agency is "interested in hearing from all of you through the regulatory process as to what would be the best way to address the issue," he added.

Guidance on Texting, Other Efforts Underway

In addition to the proposed rules on incapacity and NPPs, OCR is also working on writing a regulation it was required to produce years ago. Under the 2019 HITECH Act, OCR was to issue a rule providing for compensation to individuals whose rights and protections under HIPAA have been violated.

The agency plans to issue a request for information as the first step in writing the regulation, and will be asking for assistance in "making sure people who have been victimized through violations of HIPAA can receive some sort of recompense," Severino said.

He briefly mentioned that OCR expects to issue guidance on texting, social media, and encryption. The agency also is considering updating existing guidance "in the wake of the Parkland shooting," he said referring to the murder of 17 people at a high school in South Florida.

Severino said the issues relate to HIPAA and the Family Educational Rights and Privacy Act, known by its acronym, FERPA. OCR has "issued past guidance, joint guidance, with the Department of Education on the interaction of health care privacy law, education privacy laws, mental health in the school context," Severino said. OCR wants to consider how information could be shared "to actually help inform law enforcement, medical practitioners…so we could avoid these tragedies in the future," he said.

Severino summarized OCR's two settlements issued so far in 2018 that resolve allegations of HIPAA violations—both in February.

The first, announced Feb. 1, is for $3.5 million with Fresenius Medical Care North America (*RPP 2/18, p. 1*). The second, for $100,000, was made with the receiver for a defunct medical records storage firm, FileFax, Inc. (*RPP 3/18, p. 1*).

Although he didn't give any hints as to whether new settlements are in the offing, Severino mentioned that OCR's complaint total isn't going down. Complaints often form the basis of enforcement and settlement actions. From April 14, 2003, when the privacy rule went into effect, the agency has received 173,426 complaints. Of these, OCR has resolved 25,695 "with corrective action or technical assistance."

This year, OCR expects to receive more than 24,000 complaints, he said.

'Star' Staff Now at Headquarters

Severino also announced the appointment, on an acting basis, of two individuals who are replacing high-ranking former OCR officials well-known to the compliance community. OCR is following federal processes to name people to these posts on a permanent basis (the positions are not political and do not require Senate confirmation).

Historically, OCR directors have encouraged compliance officials to reach out to the agency and its staff for assistance, a suggestion Severino also made at the summit while introducing the new staff.

Deven McGraw resigned from her job as OCR's deputy director in September for an electronic health records start-up (*RPP 11/17, p. 1*). Tim Noonan is now acting in this job, hailing from OCR's Southeast Region, where he was the manager.

Severino referred to the Southeast's Atlanta headquarters as one of OCR's "star offices." Noonan resolved "four high-impact cases" that brought OCR "more than $9 million in settlement money," Severino said.

Also from the Southeast Region is Serena Mosley-Day, who Severino named acting senior advisor for HIPAA compliance and enforcement. Mosley-Day is the acting replacement for Iliana Peters, who joined the law firm of Polsinelli PC in February as a shareholder. Mosley-Day was the region's deputy regional manager.

This region consists of Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina and Tennessee. ✧

PRIVACY BRIEFS

◆ **Banner Health says it anticipates "negative findings" from an ongoing federal probe of a 2016 cyberattack that exposed the records of nearly 3.7 million patients, employees and others,** according to AZCentral. The Phoenix-based health provider disclosed in its 2017 annual report that an OCR investigation has included queries about the health provider's security assessments. Banner also faces a class action lawsuit over the data breach. Read the story at https://bit.ly/2GpagQz.

◆ **Insider threats pose the greatest risk to sensitive health information, with 58% of breaches of protected health information coming from insiders, according to Verizon's 2018 Protected Health Information Data Breach Report.** Another one-third of threat actions resulted from error, while 29.5% came from misuse, 16.3% came from physical threats, 14.8% resulted from hacking, and 10.8% resulted from malware. Hard copy documents were the assets most involved in incidents involving error. Verizon analyzed more than 1,300 security incidents across 27 countries. Get the full study at https://vz.to/2FvldiW.

◆ **A researcher at Vanderbilt University's Owen Graduate School of Management has linked more than 2,100 patient deaths to hospital data breaches and lack of cybersecurity,** according to a report in the *Wall Street Journal*. Sung Choi, Ph.D., presented the study in March at a conference hosted by Drexel University's LeBow College of Business. The research compared patient care metrics at hospitals that had experienced a breach and those that had not, and found that death rates increase at hospitals following breaches. Read the report at https://bit.ly/2GiVUgp.

◆ **BJC HealthCare in St. Louis, Missouri, has notified 33,420 patients that a data server configuration error, discovered during an internal security scan, made it possible for stored images of identifying documents to be accessible online** from May 9, 2017, to January 23. The scanned documents on the data server included copies of patient driver's licenses, insurance cards and treatment-related documents that were collected during hospital visits spanning 2003 to 2009. Names, addresses, Social Security numbers, driver's license numbers, insurance information and treatment-related information could be affected. The BJC investigation didn't reveal that any personal data was actually accessed. Learn more about the incident in the company's statement at https://bit.ly/2GzXEmj.

◆ **A northern Colorado dermatology practice is alerting some patients that some of their protected health information was breached on January 12.** Front Range Dermatology Associates says a terminated employee had improperly acquired a list of patients who had been seen at the practice in the previous six months. Another employee gave the terminated employee the list, the practice said. The list contained only information on patients who had been seen by the fired employee. Information included patients' names and insurance information. The practice said the former employee may have taken the list to attempt to confirm payments owed, or to make future contact with patients at a different medical practice. See more details at https://noconow.co/2uBCfXM.

◆ **The Kansas Department for Aging and Disability Services says an employee sent an unauthorized email containing protected health information to a group of current department business associates.** The email that was sent included an attachment with names, addresses, Social Security numbers, in-home services program participation information and Medicaid identification numbers, but no financial information. Around 11,000 people may have been affected. Learn more at https://bit.ly/2pUSM3u.

◆ **Primary Health Care Inc., a practice in Des Moines, Iowa, reports that the email accounts and associated Google drives of four of its employees were accessed without authorization more than a year ago,** in February 2017, leading to a possible breach of protected health information for more than 10,000 patients. A forensic investigation could not determine the scope of the unauthorized access. Information that may have been inappropriately accessed includes a combination of patient names, phone numbers, credit card numbers, diagnosis and treatment information, and other financial and medical data. Read the statement at https://prn.to/2GLKwxe.

◆ **The University of Virginia Health System is warning nearly 2,000 patients that their private health information may have been viewed** by an unauthorized third party on a UVA physician's laptop computer and other devices between May 2015 and December 2016. The doctor's devices were infected with malware that gave the third party access to what the physician was reviewing. The FBI has arrested the hacker. Get more details at https://bit.ly/2Ja0qjl.