Report on
PATIENT PRIVACY

Volume 17, Number 11 • November 2017

Practical News and Strategies for Complying With HIPAA

Contents

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

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

Senior Writer
Jane Anderson

Copy Editor
Nancy Gordon
nancy.gordon@hcca-info.org

HIPAA Doesn't Mean 'No': McGraw Shares OCR Insights as She Joins Records Start-Up

A long-time patient advocate and sought-after speaker on the HIPAA compliance conference circuit, Devin McGraw brought her passion and expertise to the HHS Office for Civil Rights (OCR) in 2015. At the time, she called her new position as deputy director for health information privacy "the job of a lifetime."

An acknowledged critic and sometimes fan of OCR, McGraw had already run the well-regarded Health Privacy Project and spent a year with a law firm by the time she joined the federal workforce (*RPP 7/15, p. 8*). McGraw's reputation as a stalwart was so cemented that her Twitter handle is simply @healthprivacy. Her move to OCR raised eyebrows, but she saw it as a unique opportunity to bring a "focus on outreach, education and guidance" and to be "influential" in creating policies regarding the data privacy and security matters about which she cares deeply.

But almost as quickly as she came, McGraw was gone from OCR. In September, a tech start-up in Silicon Valley that's building an electronic health record for consumers lured her from OCR to become its chief regulatory officer. The company is so new that McGraw can't yet disclose its name, she tells *RPP*. In a wide-ranging interview, McGraw shares her reasons for leaving, highlights of her tenure—including what made her "tear my hair out"—and thoughts about the work of the officemates she's leaving behind at OCR.

continued on p. 8

OCR: After an Opioid Overdose, Sharing Patient Information Can 'Help Save Lives'

Doctors and other medical professionals 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.

"We know that support from family members and friends is key to helping people struggling with opioid addiction, but their loved ones can't help if they aren't informed of the problem," Roger Severino, director of the HHS Office for Civil Rights (OCR) says in a statement.

Severino made his remarks as OCR issued what he called "clarifying guidance" on Oct. 27 to "give medical professionals increased confidence in their ability to cooperate with friends and family members to help save lives."

The two-page guidance came days after a presidential declaration that the misuse of opioids in the United States is a "public health emergency."

As OCR explains, "Current HIPAA regulations allow healthcare providers to share information with a patient's loved ones in certain emergency or dangerous situations."

But providers who misunderstand HIPAA "can create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose," OCR says. "It is critical for healthcare providers to

continued

Ransomware Attacks Grow; Most Incidents Are Reportable Breaches

As a new version of the WannaCry malware threatens health care organizations, attorneys who specialize in health care privacy and security issues warn that the vast majority of successful ransomware attacks should be considered reportable breaches.

In addition, attorneys caution that health care entities should consider the possibility of ransomware attacks when contracting with a business associate and should make certain their business associate is well protected, as well.

While not all ransomware gains access to an organization's private data, the risk is substantial.

"If it can be demonstrated that the protected health information (PHI) subject to the ransomware attack was already appropriately encrypted, this would be a helpful fact" in determining if the attackers gained access, says Lucie Huger, an attorney with Greensfelder, Hemker & Gale, P.C., in St. Louis. "I would also want to know what type of ransomware variant was involved and if it had an exfiltration feature. I'd also look to see whether the PHI was successfully restored through back-ups."

To assist in this type of analysis, Huger says she would engage a forensic IT firm to review the incident and prepare a report detailing their findings. "I believe that if it is appropriately documented by a person or firm with technical expertise that PHI was not compromised, then I do not believe an entity would need to report it as a breach." However, many health care entities will not be able to demonstrate this, she says.

WannaCry Just Tip of Iceberg

Ransomware attacks seemingly are rampant. The global cyberattack known as WannaCry, which peaked in May, affected at least two large, multi-state hospital systems in the U.S. and hit the U.K.'s National Health Service hard, knocking many offices offline for several days or more (*RPP 6/17, p. 1*). But smaller-scale attacks can be just as devastating to the organization involved. Here is a sampling of those that have been reported in the last several months:

◆ FirstHealth of the Carolinas, a not-for-profit health care network based in Pinehurst, N.C., reported that a new strain of the WannaCry malware forced the health care system to take its computer network offline in October. FirstHealth said it has more than 4,000 devices and more than 100 physical locations connected to its network, but "as a result of the quick response by the Information System security team, the virus did not reach any patient information, operational information or databases. Patient information has not been compromised." The health system was deploying a patch.

◆ Namaste Health Care in Ashland, Mo., reported a ransomware attack that encrypted the data stored on the organization's file server on Aug. 14. "Namaste took steps to protect patient information and its computer systems, but ultimately had to pay a ransom to the cyber attacker in order to restore and regain access to the affected data," the organization said in a statement. "Namaste has been unable to conclusively determine whether the cyber attacker may have viewed information contained on that file server," but "out of caution and to be in compliance with state and federal regulations, the office is treating this security incident as a potential breach of personal and medical data."

◆ Arkansas Oral & Facial Surgery Center, which has three locations in northwest Arkansas, says it discovered a ransomware attack on July 26, within 24 hours of when the malware had been installed on its systems. The attack rendered imaging files and documents inaccessible, and also encrypted all electronic patient data pertaining to visits within about three weeks prior to the incident. "Because we are unable to determine with reasonable certainty whether or not the perpetrator(s) placing the ransomware on our systems accessed patient information, and due to the impact on the availability of images and other files, we are providing you with notification of this incident," the organization said in its breach notification.

Ransomware is a clear threat to poorly protected organizations. In an October report, cybersecurity firm Carbon Black, Inc., found there has been a 2,502% increase in the sale of ransomware on the dark web. "This increase is largely due to a simple economic principle—supply and demand," the report concluded. "Cybercriminals are increasingly seeing opportunities to enter the market and looking to make a quick buck via one of the many ransomware offerings available via illicit economies. In addition, a basic appeal of ransomware is simple: it's turnkey. Unlike many other forms of cyberattacks, ransomware can be quickly and brainlessly deployed with a high probability of profit."

Carbon Black found there are currently more than 6,300 dark web marketplaces selling ransomware, with 45,000 product listings. The prices for do-it-yourself kits range from 50 cents to $3,000, and the median price is $10.50.

OCR is clear in its belief that ransomware attacks can—and generally do—constitute breaches. The HHS fact sheet on ransomware states:

> When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because

the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA privacy rules.

Unless the covered entity or business associate can demonstrate that there is a '...low probability that the PHI has been compromised,' based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred. The entity must then comply with the applicable breach notification provisions, including notification to affected individuals without unreasonable delay, to the Secretary of HHS, and to the media (for breaches affecting over 500 individuals) in accordance with HIPAA breach notification requirements. See 45 C.F.R. 164.400-414.

Attorney Patricia Shea, a partner at K&L Gates LLP in Harrisburg, Pa., points out that HIPAA's regulations place the burden on the organization experiencing the attack to prove there is a low probability that the information was "compromised," based on four factors:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent the risk to the PHI has been mitigated.

"More likely than not, an evaluation of these four factors—at least in the health care space—will result in a finding of compromise and therefore a breach," Shea tells *RPP*. "If there is a forensic analysis of the computer/system that can establish that the information was not copied or exported, perhaps you could make a good faith argument that the information was not compromised. But it really puts the organization in the position of having to prove a negative, i.e., prove that no information was compromised. Given the independent value of protected health information—or financial information—the risk of compromise may simply be too great."

The exception to this could be encrypted PHI, Shea says. "Remember also that HIPAA's breach notification obligations apply to 'unsecured PHI,' which is PHI that 'is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of the Department of Health and Human Services] in guidance,'" she says.

"With respect to electronic PHI, this definition means that the PHI is encrypted while in transit and while at rest," Shea says. "If the organization encrypted its PHI in accordance with the secretary's guidance and as long as the organization has no reason to believe that the encryption key was compromised during the attack, an organization could certainly argue that the attack did not compromise the PHI and no breach occurred. The burden rests with the organization to prove this."

In either case, she adds, "solid forensic analysis of the system under attack will be crucial to the organization."

Cover Ransomware in BA Agreements

Some covered entities may tend to overlook their business associates when considering the possibility of ransomware—but they definitely shouldn't. "Ransomware should certainly be covered in business associate agreements," Huger says.

According to Huger, covered entities should:

- Determine what their business associates have included in their risk analysis to address ransomware, including "proactive steps they are taking and disaster recovery."
- Require prompt reporting of a suspected or an actual ransomware attack. "I believe a CE would want to know within 24 hours because early reporting generally provides...more success in mitigating the harm of a breach."
- Ascertain that the business associate has appropriate insurance in the event of a ransomware attack.

"I do expect ransomware to be an important issue for covered entities and business associates to be mindful of going forward. It is essential to recognize this situation in a risk assessment and take steps to mitigate the risk," Huger says.

Shea says she's currently assisting a client in a business associate role with a response to a successful ransomware attack. She declined to share details, but she says that health care entities must consider the possibility of ransomware attacks against a business associate when contracting.

"Organizations that subcontract with others need to be vigilant regarding those subcontractors' abilities to prevent and respond to a ransomware attack," she says. "If the subcontractors are not taking the same steps to mitigate the risk of a ransomware attack, the contracting organization has a weakness and allowing them access to the organization's system may not be a good option."

When contracting with these subcontractors, Shea says, "organizations should be conducting some careful due diligence on the subcontractors' practices, policies and procedures related to systems as well as their ability to indemnify the organization for any losses incurred as a result of the subcontractors' failure to have appropriate safeguards in place."

She adds: "Good indemnification clauses are certainly recommended, but they are only as good as the financial stability of the subcontractors providing them. Organizations need to be sure that the subcontractor has the financial ability to provide that indemnification."

Preventing Attacks Involves Training, Patches

To prevent attacks, Shea says both covered entities and business associates should take steps to guard against malware, including:

- Continuous training of employees on how to recognize phishing emails and on how to respond if they click on one by mistake;
- Considering a policy prohibiting employees from receiving personal emails at work; and
- Keeping all systems patched and up to date.

"In addition to technology and operational safeguards, organizations should be making constant systems backups so that if they are successfully targeted, they can recover the system," Shea says. "Remember that with HIPAA, the access or removal of data certainly constitutes a breach, but the loss of data is equally problematic and would, at a minimum, constitute a security incident—and likely a breach. Organizations need to prepare for the possibility and have their response plans ready."

Finally, Shea says, organizations should consider purchasing cyber insurance. "While this would not prevent a ransomware attack, these attacks do likely constitute a breach—at least in the view of regulators—and responding to a breach can be very expensive. Organizations would likely find the purchase of such insurance as a solid risk mitigation strategy."

Huger says that even the most diligent organization may not be able to prevent ransomware attacks, because the methods used are always changing. "We all counsel clients to 'think before they click,' however, with methods like 'malvertising,' a compromise can occur without ever clicking a link. I think it's more realistic to say that an organization can work to lower the odds and lessen the impact of an attack."

This can be accomplished, Huger says, through education and by installing software that detects malware. "An organization can lessen the impact of the attack by having an effective business continuity plan with comprehensive daily back-ups of data, so that if an organization is locked out of its data, it can be restored."

Read the Carbon Black report at http://bit.ly/2gGDbQM. Contact Huger at lfh@greensfelder.com and Shea at Patricia.Shea@klgates.com. ✧

To Protect PHI, Improve Credential Protection, Shun Password Sharing

Health care organizations should make major changes to how they grant access to systems that contain protected health information, including limiting the use of shared passwords and adding more secure authorization procedures, says a former Anthem, Inc., executive and expert in cybersecurity.

Steve Moore, who signed on in August as vice president and chief security strategist at security consulting firm Exabeam after spending seven years at Anthem, most recently as staff vice president of cyber security analytics, says 80% to 81% of hacking-based breaches leveraged passwords, and that health care organizations can be at greater risk simply because of the nature of their business: care-giving.

"A lot of people are sharing accounts because it's the smartest way someone found to solve the care problem," Moore tells *RPP*. When a clinic or a hospital has money to invest, they'll tend to invest it in systems or technology that improve care, not that improve security, he says. "With some of these smaller clinics or even major hospitals, quality of care is paramount. Sometimes they just aren't up to speed on information technology."

Study Shows Password Sharing Rampant

A lack of focus on security in health care organizations is clear from the results of a recent study on the sharing of access credentials among medical staff for electronic medical records.

The study, published in *Healthcare Informatics Research*, found that nearly three-quarters of medical staff surveyed had obtained the password of another medical staff member. Of those who estimated how many times this happened, the average was 4.75 times. All of the residents who took part in the study had obtained the password of another medical staff member, while only 57.5% of the nurses reported having done so.

"Medical staff share access credentials all the time," study author Ayal Hassidim tells *RPP*. "It's not because we are bad—it's because we are required to do stuff that can't be done with our credentials or because we give our credentials to less senior staff to help us do our work, due to an extremely high workload."

The study included only Israeli medical staff members, but the study authors also have done preliminary research on a group of American medical staff members and "found very similar results," Hassidim says. "I think that this problem is worldwide and we will find similar results in any medical system," he says. "It seems to me that the problem is not too many passwords—the issue here is too much work. When the on-call resident needs