Report on
Medicare Compliance

Volume 28, Number 15 • April 22, 2019

Weekly News and Compliance Strategies on Federal Regulations, Enforcement Actions and Audits

Contents

In Appeal, MD Anderson Says HIPAA Penalties Don't Apply Because It's a State Agency

If MD Anderson Cancer Center gets its way, a federal court will declare that the Texas hospital doesn't ever have to pay civil monetary penalties (CMP) for violating HIPAA privacy or security regulations. In its April 9 appeal of a $4.3 million penalty stemming from breaches caused by unencrypted thumb drives and a laptop, MD Anderson argued that CMPs don't apply to "states and state agencies" like MD Anderson because they were not included in the 1996 HIPAA statute, and the HHS Office for Civil Rights (OCR) overstepped by adding them to the HIPAA regulations. MD Anderson also argued that the penalty—which was upheld last year by an administrative law judge (ALJ) – exceeds statutory caps on HIPAA violations.

The appeal's prospects for success are iffy because HHS acknowledged in its enforcement regulations that it was adding states and state agencies to the original statute, but "a victory would be significant," says attorney Thora Johnson, with Venable in Baltimore, Maryland. If MD Anderson wins, it would put public hospital districts and other state agencies potentially in the position of saying "OCR doesn't have any enforcement authority over us. We are complying because 'it is the right thing to do,'" she says. "We will see in time how strong an argument it is. MD Anderson is certainly pointing out a potential weakness." Either way, states and state agencies may have obligations under other state and federal laws to keep health information private and secure, Johnson notes.

continued on p. 6

Hospitals Find Ways to Reduce Seven-Day Readmissions, But 30-Day Denials Provoke Ire

When a patient with sickle cell disease was readmitted to the hospital 15 times in the last 12 months of her life, the Medicaid managed care plan denied the claims. It was one of the more frustrating experiences that Self Regional Healthcare in Greenwood, South Carolina, had with readmissions, which is an ongoing challenge because hospitals don't always control the variables that affect readmissions, including physician shortages and patient compliance. Although the Medicaid managed care plan has a more reasonable readmission policy than other payers in terms of timing—they don't pay when a patient is readmitted within 15 days of an admission vs. 30 days—it seemed absurd the hospital was "dinged" for readmissions in this circumstance, says Phillip Baker, M.D., medical director of case management at Self Regional Healthcare.

"She was in terrible pain and had liver damage because she had been transfused so many times," Baker says. "We tried to appeal and they said within 15 days 'we are not going to pay for this.'"

continued

HCCA

Managing Editor
Nina Youngstrom
nina.youngstrom@hcca-info.org

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

Denials for readmissions are a thorn in the side of hospitals, which are trying various strategies to reduce them. Denying payment for readmissions within seven days is one thing—that's a good demarcation line for discharge planning and follow-up to prevent readmissions—but hospitals are exasperated when payers won't cover them up to 30 days later, sometimes for unrelated conditions depending on the payer.

"The only potential hospitals have for impacting readmission is seven days," Baker says. "You can have huge impact on readmissions in the first week. It's a valuable thing to track. Did we miss something on discharge? Is the primary care physician seeing the patient? Are we getting indigent patients on a medication program?" But a month is another story. Hospitals are skeptical about the influence they exert on readmissions beyond the week after discharge, when they try to make sure patients are seen by a primary care physician or specialist and fill their prescriptions and understand how to take them. "Do you know why they chose 30 days? There's no rhyme or reason. Why not two weeks or 6 weeks? There's nothing magic about a 30-day timeline," Baker says. "This policy is driving us all up the wall."

A 2016 study in JAMA Internal Medicine found only about a quarter of readmissions "are potentially preventable when assessed using multiple perspectives" (Preventability and Causes of Readmissions in a National Cohort of General Medicine Patients).

Self Regional has reduced readmissions significantly over the past decade, partly by using a transitional care clinic and having pharmacy technicians explain medications to patients at discharge and nurses phone patients at home. "We want everyone to say we're a high-quality hospital."

With commercial and MA plans, readmission denials translate into no payment. That's different from original (fee-for-service) Medicare, which has two policies: (1) When a patient is discharged from the hospital and readmitted on the same day for symptoms related to the evaluation and management of the condition treated earlier, the two stays must be combined on a single claim; and (2) Under the Hospital Readmission Reduction Program, CMS penalizes hospitals with excess readmissions for six conditions/procedures by reducing their total MS-DRG reimbursement up to 3% based on data from prior years.

United Denies Preventable Admissions

In the MA and commercial world, readmission payment policies can get complicated. For example, UnitedHealthcare's updated April 1 hospital readmission policy for commercial plans says readmissions will be reviewed only if they're related and preventable. Hospitals like the related part—why should they be on the hook for a heart failure patient who is admitted for a hip fracture three weeks later?—but the preventable part is trickier.

"When you think of a 'preventable readmission,' it's typically been a case in which a patient was discharged too early, while he or she still required a hospital level of care," says Martie Ross, a principal at PYA in Overland Park, Kansas. But she thinks United's policy goes beyond this. It says readmission reviews may be conducted to determine if a related readmission could have been prevented with "optimal" quality of care during the inpatient stay, "optimal" discharge planning, "optimal" post-discharge follow-up and "improved coordination between inpatient and outpatient health care teams." The kicker: In its readmission reviews, United will consider whether the hospital adequately addressed the social determinants of health, Ross says. If readmissions are declared clinically related, reviewers move onto whether they were "potentially preventable," and one of the factors is "whether documentation supports that all salient

Report on Medicare Compliance (ISSN: 1094-3307) is published 45 times a year by the Health Care Compliance Association, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. 888.580.8373, hcca-info.org.

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

To order an annual subscription to **Report on Medicare Compliance** ($665 for HCCA members; $765 for nonmembers), call 888.580.8373 (major credit cards accepted) or order online at hcca-info.org.

Subscribers to this newsletter can receive 20 non-live Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB)®. Contact CCB at 888.580.8373.

financial and social needs of the patient have been addressed." That presents new challenges for hospitals, Ross says. "Is it now hospitals' responsibility to address food insecurity, arrange for transportation, or complete a home assessment to address potential fall risks before they send patients home?" Any of these factors may result in a readmission: the patient suffers from inadequate nutrition, misses a follow-up appointment, or trips and falls in the home. There's an expectation with payers that "hospitals will be more directly involved in patients' transitions of care," she says.

Baker also takes issue with the idea of basing claims for readmissions on "optimal" post-discharge care for patients. "What do they consider optimal? Making sure the air conditioning is on? That drugs are delivered to their house? Sending a nurse to their house to make sure they're taking their drugs? Sending physicians to their house? Nobody does these things," he says. "It takes us weeks sometimes to get patients an appointment with a primary care physician because of a shortage," even though the physicians benefit because "the reimbursement they can get for office visits for hospital follow-up within seven days is significantly more. Why wouldn't they want to do that? Because they are booked for a month."

Cheaper Nebulizers Help COPD Patients

Baker says all hospitals have readmissions, and some are unavoidable. For example, if chronic obstructive pulmonary disease (COPD) patients resume smoking when they leave the hospital, they will be back, Baker says. The same goes for congestive heart failure patients who eat high-salt diets. Medication compliance is also a problem, but that's sometimes compounded by finances or difficulty complying with confusing medication regimens, especially if they live alone.

To help reduce readmissions, Self Regional has a committee that meets daily to review all patients who have been admitted within 30 days of the initial admission. It has found that COPD patients top the list. The committee came up with a clever idea to help the patients. "A lot of inhalers they use are ridiculously expensive—hundreds of dollars a month. We found we can use much cheaper nebulizers that can accomplish the same goal," Baker says. "For a lot of our patients who can't afford expensive meds, it is an alternative—a few dollars vs. hundreds." And the hospital sends heart failure patients home with a scale to weigh themselves every day, and they're told to call their physicians if they gain more than two pounds a day.

The hospital also established a transitional care clinic for patients who don't have a primary care physician or can't get an appointment with theirs to ensure they have follow-up care after a hospital stay. If patients don't have insurance, the hospital eats the cost, Baker says. Another strategy: keeping patients in the hospital an extra day to reduce the odds they will return anytime soon.

Ronald Hirsch, M.D., vice president of regulations and education at R1 RCM, says many payers, taking their cue from CMS, deny payment for readmissions whether or not they're related to the initial admission. The "related" aspect tends to fall down as two admissions get farther apart, he explains. A study reported in the June 5, 2018, edition of the Annals of Internal Medicine found a "drastic difference" in readmissions that occur in seven versus 30 days, he says ("Preventability of Early Versus Late Hospital Readmissions in a National Cohort of General Medicine Patients").

Because flat-out claim denials for readmissions is an MA and commercial payer thing, "hospitals need to know what their contracts say," Hirsch says. If payers are applying a readmission policy to hospitals that don't have it in their contracts, that's inappropriate and should be challenged. "If the contract says the standard readmission policy will be in place, you are stuck. If they're silent on that issue, does that mean they can apply it or not? Does it have to be present to be penalized or is it there by default?"

Contact Baker at Roy.Baker@selfregional.org, Ross at mross@pyapc.com and Hirsch at RHirsch@R1RCM.com. ✧

Medical-Device Security Has More Hurdles; 'Zero Trust' Is Option

When HHS identified the top five cybersecurity risks faced by the health care industry in a December 2018 report, connected medical devices were right up there. Like other risks in the report, including phishing and ransomware, connected medical devices have the potential to expose all patient, billing and demographic information on hospital networks to hackers and other cybercriminals. Unlike the other risk areas, connected medical devices put hospitals in an exasperating position because often security measures are out of their hands, a consultant says. Medical device manufacturers have control over them and may resist prompt security updates, partly because they worry their devices will be adversely affected. That's increasing hospitals' vulnerability to cyberattacks, although they may be able to improve the security of

their devices, including MRI and CT machines, by using measures that don't "touch" the machines.

"You have to go through the device manufacturer" for security updates, says Barry Mathis, consulting principal with PYA in Knoxville and a former hospital chief technology officer. "That's not something you have domain over. The device manufacturer has to be involved." It's frustrating for hospitals, which may be told by manufacturers they need Food and Drug Administration (FDA) approval for changes to improve cybersecurity, which he says isn't true (see box, p. 5).

"The FDA doesn't test devices for cybersecurity before they go into circulation," he notes. "The FDA approves them based on manufacturer testing. Some people say manufacturers can't update the device, but yes, they can—they don't want to. It's not the FDA saying the medical device manufacturer can't update the software." It's challenging for manufacturers as well because they have to ensure the anti-malware software and other security measures don't interfere with the medical device's function and reliability, Mathis explains.

Devices Are a Conduit to Networks

Medical devices are vulnerable to hacking and other direct forms of cyberattacks, and they make hospitals vulnerable generally because they're increasingly connected to hospital networks, sending results to electronic health records (EHRs) for clinical, billing and other purposes. That includes X-ray machines, fetal monitors, blood-pressure cuffs, ultrasounds and even stethoscopes, to name a few. As a result, anyone with access to the medical device could access patient information. "It may be one patient or every patient seen that day or all patients over a period of time," Mathis says. The medical device also becomes a conduit to the other areas of the hospital network that are more vulnerable, he explains. "That single card at the bottom can bring down the house of cards" (see box, p. 6)

To protect medical devices from hackers and other cybersecurity threats, they require anti-malware software, patches, updates and other cybercriminal deflectors. "There are specific things medical device manufacturers have to do to guarantee to the FDA and the Department of Homeland Security that software can't be hacked, touched or manipulated," Mathis says. That's where two myths come in. First, people tend to think only the FDA is responsible for oversight of medical-device security, but "it's also the Department of Homeland Security" (DHS). Second, hospitals may think cybersecurity software updates (e.g., anti-virus, patches) apply universally, but that's not the case. When they update software, hospitals are unable to apply it to most medical devices, Mathis says. "You can't go up to the device on your network and say, 'We will load Norton on all our machines.' If you do it, you will be violating your contract with the medical device company and breaking the support agreement," he says. "You have to go through the device manufacturers."

Suppose Java has an update, and it releases a note saying the current version is vulnerable to attack. Hospitals run an update, but they're not allowed to touch the medical devices. "They have to call the manufacturer, which says to wait until it releases the next version of the medical device," Mathis says. "Hospitals are forced to run an old, vulnerable version on their network." That jeopardizes the network, but there are physicians who insist on using the device anyway. By not updating Java, hospitals have increased the risk to their entire network and to the data on the device, he says.

Some medical device companies will tell hospitals their hands are tied because the medical device has only been approved by FDA with the original cybersecurity software, Mathis contends. But as the FDA itself states, it "does not typically need to review changes made to medical devices solely to strengthen cybersecurity." He notes that medical-device manufacturers are getting better about this; "they're on board with making sure cybersecurity is a priority, but they still insist you can't go out there and do anything and they have to be involved and it can slow down this process." Also, a lot of software updates are now built into medical devices, so the problems he's describing apply more to "legacy" devices. But security updates are still in the hands of device makers, not hospitals.

An Option: Making Devices Invisible

It's possible to sidestep these challenges by protecting the devices without touching them at all, Mathis says. "One of the ways I manage that vulnerability is with zero trust," he says. The concept of zero trust has been around since 2010, and it's becoming the norm for protecting devices, Mathis says. As the name implies, zero trust technology prevents everyone from connecting to a device in the network unless a person has specifically been given permission through authentication. "The device is seeing fewer people. I have already determined based on who someone is who can access the room," Mathis explains.

For fighting cybercrime, he thinks the most promising version of zero trust is the concept of first-packet recognition. It makes access to the data inside the medical device invisible to everyone except the users who have been identified as trusted. First-packet authentication doesn't require a device to acknowledge another device through the standard "handshake," Mathis explains. His analogy for first-packet recognition is a street with hun-

dreds of houses where one house is completely invisible to everyone except the people who are allowed to see the door. "Imagine that in a hospital network," Mathis says. As far as hackers can tell, there are no medical devices because they've been cloaked. "I make it hidden from the rest of the world. You can use this technology to protect EHRs and even create a micro segmentation framework to protect many devices and systems." Mathis is only aware of one company, BlackRidge Technologies, that has patents for first-packet recognition, but other companies provide zero-trust technology.

Contact Mathis at bmathis@pyapc.com. View the December HHS cybersecurity report at http://bit.ly/2GlSGtH. ✧

MEDICAL DEVICE CYBERSECURITY: DISPELLING THE MYTHS

This fact sheet was posted on the web site of the Food and Drug Administration (FDA). Visit http://bit.ly/2vifyFD.

FDA FACT SHEET
THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY
Dispelling Myths and Understanding Facts

As medical devices become more digitally interconnected and interoperable, they can improve the care patients receive and create efficiencies in the health care system. Medical devices, like computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device. By carefully considering possible cybersecurity risks while designing medical devices, and having a plan to manage emerging cybersecurity risks, manufacturers can reduce cybersecurity risks posed to devices and patients.

The FDA has published premarket and postmarket guidances that offer recommendations for comprehensive management of medical device cybersecurity risks, continuous improvement throughout the total product life-cycle, and incentivize changing marketed and distributed medical devices to reduce risk. Even with these guidances, the FDA continues to address myths about medical device cybersecurity.

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.
Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.	The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.
The FDA is responsible for the validation of software changes made to address cybersecurity vulnerabilities.	The medical device manufacturer is responsible for the validation of all software design changes, including computer software changes to address cybersecurity vulnerabilities.
The FDA tests medical devices for cybersecurity.	The FDA does not conduct premarket testing for medical products. Testing is the responsibility of the medical product manufacturer.
Companies that manufacture off-the-shelf (OTS) software used in medical devices are responsible for validating its secure use in medical devices.	The medical device manufacturer chooses to use OTS software, thus bearing responsibility for the security as well as the safe and effective performance of the medical device.

The FDA encourages medical device manufacturers to address cybersecurity risks to keep patients safe and better protect the public health. This includes monitoring, identifying, and addressing cybersecurity vulnerabilities in medical devices once they are on the market. Working collaboratively with industry and other federal government agencies, the FDA continues its efforts to ensure the safety and effectiveness of medical devices, at all stages in their lifecycle, in the face of potential cyber threats. Learn more about medical device cybersecurity on www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.

Medical device cybersecurity is part of the FDA's broader digital health technology platform. To learn more about the FDA's efforts to advance digital health technology visit http://www.fda.gov/MedicalDevices/DigitalHealth/default.htm, or email digitalhealth@fda.hhs.gov.

Threat: Attacks Against Connected Medical Devices That May Affect Patient Safety		
Vulnerabilities	**Impact**	**Practices to Consider**
Patches not implemented promptly; includes regular and routine commercial system patches to maintain medical devices Equipment not current, or legacy equipment that is outdated and lacks current functionality Most medical devices, unlike IT equipment, cannot be monitored by an organization's intrusion detection system (IDS); safety of patients and protection of data integrity are dependent on identifying and understanding the threats and threat scenarios. However, it is the challenge of identifying and addressing vulnerabilities in medical devices that augments the risk of threats compared with managed IT products For medical devices, the cybersecurity profile information is not readily available at health care organizations, making cybersecurity optimization more challenging. This may translate into missed opportunities to identify and address vulnerabilities, increasing the likelihood for threats to result in adverse effects Heterogeneity of medical devices means that the vulnerability identification and remediation process is complex and resource intensive; increases the likelihood that devices will not be assessed or patched, leading to missed opportunities	Broad hospital operational impact due to unavailable medical devices and systems Medical devices do not function as required for patient treatment and recovery Patient safety compromised due to breach	Establish and maintain communication with medical device manufacturer's product security teams (9.L.A) Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested (9.M.B) Assess current security controls on networked medical devices (9.M.B, 9.M.E) Assess inventory traits such as IT components that may include the Media Access Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks (9.M.D) Implement pre-procurement security requirements for vendors (9.L.C) Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities (1.L.A) Engage information security as a stakeholder in clinical procurements (9.L.C) Use a template for contract language with medical device manufacturers and others (9.L.C)Implement access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, MFA, and minimum necessary or least privilege (9.M.C) Implement security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities (9.L.B) Develop and implement network security applications and practices for device networks (9.M.E)

Source: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Visit http://bit.ly/2GlSGtH

MD Anderson: HIPAA CMPs Don't Apply

continued from p. 1

The case also illustrates how easily the need for encryption can fall through the cracks at large health systems, says attorney Joseph Dickinson, with Smith Anderson in Raleigh, North Carolina. "They have so many assets—laptops, phones, thumb drives and pagers—that need to be encrypted that the human resources needed to make that happen can be prohibitive," he says. "They probably don't even have an accurate list of all devices with protected health information." Health systems make themselves more vulnerable by developing policies and procedures without ensuring they're implemented and followed, Dickinson says. That was at the heart of the allegations against MD Anderson, which reiterated in the appeal that no patients were harmed by the breaches.

OCR: MD Anderson Didn't Implement Controls

OCR fined MD Anderson Cancer Center in connection with three breaches that led to the disclosure of 33,500 people's electronic protected health information (ePHI) when the mobile devices went missing. MD Anderson appealed, arguing the fines were unreasonable, that it wasn't required to encrypt the ePHI, and that the information isn't subject to HIPAA non-disclosure requirements because it's research related, but ALJ Steven Kessel upheld the fine, siding with OCR ("ALJ OKs $4.3M HIPAA Fine on MD Anderson Over Encryption; Layered Security Is Advised," *RMC* 27, no. 23).

OCR had informed MD Anderson of the penalty in a 2017 Notice of Proposed Determination (NPR), which said it "failed to implement access controls—encryption and decryption, or an equivalent alternative measure, as required by 45 C.F.R. § 164.312(a)(2)(iv)" and "impermissibly disclosed the PHI of at least 34,883 individuals, in violation of 45 C.F.R. § 164.502(a)."

At the root were three incidents reported by MD Anderson:

1. An unencrypted laptop with the ePHI of 29,021 people was stolen from the home of physician/faculty member Dr. Randall Millikan in 2012. "Dr. Millikan purchased this laptop with funds provided by MD Anderson and used it as a telework computer. Dr. Millikan acknowledged that his stolen laptop was never encrypted or password-protected," OCR said. The laptop wasn't secured in any other way, and family members could have accessed the ePHI.

2. A summer intern in the Department of Stem Cell Transplantation and Cellular Therapy said in 2012 that she misplaced a USB thumb drive. She had uploaded the ePHI of 2,264 people on the unencrypted thumb drive and thinks she misplaced it on her way home from work.
3. A visiting researcher from Brazil, Dr. Marisa Gomes, uploaded MD Anderson ePHI on a personal, unencrypted USB thumb drive and kept it in a tray in her desk. It contained the ePHI for 3,598 individuals. "She reported that she had last seen the thumb drive on the afternoon of November 27, 2013, when she left work for Thanksgiving break, and was unable to find it when she returned the morning of December 2, 2013," OCR said. When she couldn't find the thumb drive, Gomes notified her department administrator (infectious diseases).

Before the three breaches, MD Anderson allegedly knew the ePHI should have been protected by encryption, according to the NPR.

For example, according to MD Anderson's corporate compliance risk analysis for fiscal year 2011, there wasn't an enterprise-wide solution for encrypting laptops and mobile devices, and members of the workforce were downloading ePHI onto them and taking mobile devices outside MD Anderson. Even after the three breaches, MD Anderson didn't fully encrypt electronic devices with ePHI until Jan. 25, 2013, when 98% of its computers were encrypted.

HHS calculated a CMP at $2,000 a day and at a culpability level of "reasonable cause." In its appeal to the ALJ, MD Anderson argued that encryption of devices is optional—an "addressable" standard under the HIPAA security regulation—and that it had plans underway to adopt it. The ALJ didn't agree. Although HIPAA doesn't mandate the use of a specific mechanism to protect ePHI, "Respondent failed to comply with regulatory requirements because it failed to adopt an effective mechanism to protect its ePHI."

On the penalty amounts, the ALJ found them "reasonable." MD Anderson was "noncompliant on each day of the period at issue" and knew of the risks of not encrypting ePHI on mobile devices. Even so, the penalties are a fraction of what's permitted by the HIPAA regulation. MD Anderson also argued that HIPAA doesn't apply to the lost or stolen ePHI because it's research information, and there's an exemption for all data used in research. "This argument rests on what is at best a fanciful interpretation of governing regulations, and I find it to be without merit," Kessel asserted.

The ALJ granted OCR summary judgment and MD Anderson appealed to the HHS Departmental Appeals Board (DAB), which upheld the ALJ's decision. But the ALJ and DAB refused to consider three of MD Anderson's arguments, saying they fall outside their authority. The three arguments are at the heart of the new appeal to the U.S. District Court for the Southern District of Texas.

First, MD Anderson argues it isn't subject to CMPs because it's part of the University of Texas system and therefore a state agency. The 1996 statute—the Health Insurance Portability and Accountability Act—only allows CMPs against a "person," which the law defined as "an individual, a trust or estate, a partnership, or a corporation." But in the HIPAA regulations, HHS went farther, MD Anderson said. "Despite the statutorily prescribed limits of 42 U.S.C. § 1320d-5 and 42 U.S.C. § 1301(a)(3), the Secretary, without Congressional authority, expanded the definition and scope of the term 'person' in regulation 45 C.F.R. § 160.103 (for purposes of issuing a CMP under HIPAA) to include the States and state agencies," according to the appeal. HHS went too far when it broadened the definition of person in the regulation and imposed a CMP on MD Anderson, which asked the court to set it free.

Johnson says it's an interesting argument, but she's unsure MD Anderson will prevail. "MD Anderson has not addressed the fact that the Department of Health and Human Services foresaw this potential challenge in the preamble to its proposed enforcement regulations. It cited to Supreme Court prec-

CMS Transmittals and *Federal Register* Regulations April 12-18

Live links to the following documents are included on *RMC's* subscriber-only webpage at compliancecosmos.org.

Transmittals

Pub. 100-04, Medicare Claims Processing Manual

- Pub. 100-04, Chapter 29 – Appeals of Claims Decisions - Revisions, Trans. 4278 (April 12, 2019)
- New Waived Tests, Trans. 4277 (April 12, 2019)

Pub. 100-20, One-Time Notification

- Implementation to Exchange the list of Electronic Medical Documentation Requests (eMDR) for Registered Providers via the Electronic Submission of Medical Documentation (esMD) System, Trans. 2281 (April 16, 2019)

Federal Register

Final Regulation

- Medicare and Medicaid Programs; Policy and Technical Changes to the Medicare Advantage, Medicare Prescription Drug Benefit, Programs of All-Inclusive Care for the Elderly (PACE), Medicaid Fee-For-Service, and Medicaid Managed Care Programs for Years 2020 and 2021, 84 Fed. Reg. 15680 (April 16, 2019)

edent as the basis for its authority to define 'persons' subject to the CMPs in its regulations broadly enough to include states and state agencies. This may come up in the government's response." Meanwhile, MD Anderson has publicly embraced HIPAA; its notice of privacy practices is on its web site, and "state agencies have held themselves out as covered by HIPAA," she says.

In the appeal, MD Anderson also argued that OCR's penalty was higher than allowed under the statute and asked the court to stop its enforcement. The law has four CMP tiers based on culpability: (1) "did not know" violations; (2) "reasonable cause" violations; (3) "willful neglect and corrected" violations; and (4) "willful neglect not corrected" violations. Because the statute allows a maximum annual penalty of $100,000 per violation, the fine is "an amount almost 10 times more than the statutory caps," which violates the Excessive Fines Clause of the Eighth Amendment, MD Anderson contends.

"I don't think that's a winning argument," Johnson says. OCR has plenty of leeway in how it counts the number of violations.

The appeal also contended that encryption is an "optional" standard. But Dickinson says optional and addressable aren't the same thing, a fact that's sometimes lost on covered entities. "It's true that HIPAA doesn't require encryption—it's addressable," he says. But covered entities have to assess whether addressable specifications in the security regulation are reasonable and appropriate, implement the specification, come up with a "reasonable and appropriate" alternate security measure or do neither if they document why. "In theory you can do a thorough risk assessment and [determine] no alternative solution is reasonable and appropriate, even though today you probably can't because the cost of encryption has come down. It would be tough to meet that burden," Dickinson contends. In this case, that shouldn't apply to MD Anderson because allegedly it decided encryption was appropriate, adopted a policy and developed an encryption plan, but never carried it out, he says.

Encrypting all mobile devices is "aspirational," especially when employees disregard their privacy and security training, Dickinson says. For example, they may lose their Iron Key thumb drive—an encrypted thumb drive that's very secure—and, under pressure to get work done at home or on vacation, employees may pick up an unencrypted version at Best Buy and download patient data. "The simple reality is, the volume of data and number of devices and end points we need to control makes it tough to do. It's a challenge for large health care organizations because health care is the number-one target for cyber hacktivists and hackers," Dickinson says.

In a statement, MD Anderson said "patient privacy is of extreme importance at The University of Texas MD Anderson Cancer Center, and substantial measures are in place to ensure the protection of patient information… Regardless of the final decision, MD Anderson hopes this process brings transparency, accountability and consistency to the Office for Civil Rights' enforcement process. The institution remains committed to safely protecting patient information."

Contact Dickinson at jdickinson@smithlaw.com and Johnson at tajohnson@venable.com. Read the appeal at http://bit.ly/2XuCUnv. ✧

NEWS BRIEFS

◆ **The HHS Office of Inspector General has updated its work plan, which is its road map of audits and evaluations.** Visit https://go.usa.gov/xmTDM

◆ **Sixty people, including 31 doctors, seven pharmacists and eight nurse practitioners, were arrested in the Appalachian Regional Prescription Opioid Surge Takedown, the Department of Justice, HHS Office of Inspector General and other state and federal law enforcement agencies said April 17.** The people were arrested for allegedly participating in the illegal prescription and distribution of opioids and other narcotics and in health fraud schemes. The case involves more than 350,000 prescriptions and 32 million pills in West Virginia, Ohio, Kentucky, Alabama, and Tennessee; 24,000 patients received prescriptions from the medical professionals who were charged, DOJ said. For example, 15 people were charged in the western district of Tennessee, including eight physicians and other medical professionals. One of them is a nurse practitioner who called himself the "Rock Doc" and allegedly prescribed "powerful and dangerous combinations of opioids and benzodiazepines, sometimes in exchange for sexual favors," DOJ said. Five people were charged in the eastern district of Kentucky, including a dentist who allegedly wrote opioid prescriptions without a legitimate medical purpose, extracted teeth unnecessarily, scheduled unnecessary follow-up appointments and billed improperly for services, DOJ said. Visit http://bit.ly/2VdZkvI