COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 28, Number 15. April 22, 2019
In Appeal, MD Anderson Says HIPAA Penalties Don't Apply Because It's a State Agency

By Nina Youngstrom

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.

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 nondisclosure 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:

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.

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.

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 precedent 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.