Report on Medicare Compliance Volume 27, Number 23. June 25, 2018
ALJ OKs $4.3M HIPAA Fine on MD Anderson Over Encryption; Layered Security Is Advised

By Nina Youngstrom

The $4.3 million penalty slapped on MD Anderson Cancer Center for allegedly violating the HIPAA regulations will stand, at least for now. Administrative Law Judge (ALJ) Steven Kessel sided with the HHS Office for Civil Rights (OCR), which fined the Houston health system last year in connection with three breaches that led to the disclosure of 33,500 people's electronic protected health information (ePHI) when an unencrypted laptop and two thumb drives 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 the ALJ wasn't buying.

"The penalties in this case are reasonable given the gravity of Respondent's noncompliance and the number of individuals potentially affected," Kessel said in the decision (No. CR51110). "What is most striking about this case is that Respondent knew for more than five years that its patients' ePHI was vulnerable to loss and theft and yet, it consistently failed to implement the very measures that it had identified as being necessary to protect that information."

The tug of war isn't over, however. MD Anderson said it will appeal. "We hope this process brings transparency, accountability and consistency to the Office for Civil Rights' enforcement process," according to a statement.

A lot of HIPAA penalties hit organizations that fall short on HIPAA security risk assessments, but this time it's also about the alleged failure to follow through, says attorney Richelle Marting, with the Forbes Law Group in Overland Park, Kansas. "It's not just the thought that counts. You have to do something with your security risk assessment or you will face penalties."

Don't put all your eggs in the encryption basket, however, says Alexander Laham, information security manager at Lawrence General Hospital in Massachusetts. While encryption is a no-brainer—"to properly secure your data in conformance with HIPAA security requirements, you need encryption"—it's enhanced by "layered security," he says .

How 'Layered Security' Provides Deeper Protection from HIPAA Violations

The concept of layered security can be compared to an onion, says Alexander Laham, information security manager at Lawrence General Hospital in Massachusetts. Here are examples of varying layers of security measures implemented to defend against some threats. "As you work your way out from the inside, you are met with progressive layers of protection—the inside of that onion being whatever critical asset you are trying to protect; for hospitals that is primarily PHI/ePHI," Laham says. "Typically, the layers involve the data (assets), people, physical space, endpoints (devices), software (applications), and network(firewalls). Defense methods depend on the specific threat and reasonable defense options available to the organization." He notes the examples are not fully developed; they are a snapshot of the types of measures that could be taken to defend assets. Contact Laham at Alexander.Laham@LawrenceGeneral.org.

Risk	A thumb-drive containing ePHI could be lost or stolen, exposing confidential records.	A laptop containing ePHI could be lost or stolen, exposing confidential records.	Malicious phishing emails could compromise endpoints, exposing confidential records.
Layer 1	Organizational policy and recurrent user awareness training to reinforce the proper handling of ePHI and thumb-drives.	Organizational policy and recurrent user awareness training to reinforce the proper handling of ePHI and portable computing.	Organizational policy and recurrent user awareness training to reinforce identification and management of phishing emails.
Layer 2	To support the policy and user training, the organization evaluates and purchases encrypted thumb-drives for provision to employees when needed.	To support the policy and user training, all laptops are whole disk encrypted as part of the standard provisioning process.	To identify and block malicious software from running, endpoint protection software with advanced anti-virus is deployed to workstations.
Layer 3	To ensure that only encrypted thumb-drives are used, computer policy is applied to endpoints disabling USB ports, with a whitelist allowing only approved encrypted drives.	To validate encryption status of laptops, laptop tracking software is installed on all laptops to allow for geolocation and remote erasure.	To limit the volume of phishing emails reaching employees, email protection system policies are updated to blacklist known or potential malicious phishing email sources.
Layer 4	To reduce the chance of users circumventing hospital policy, utilize firewall and endpoint protection policies to blacklist unapproved cloud-based file sharing services and provide staff with a secure alternative methodology for file transfer.		To limit external threats, next-gen firewalls are deployed to provide antivirus, anti-malware, URL filtering, intrusion detection and intrusion prevention on the perimeter network.
Layer 5	If capable, employ Data Loss Prevention software to restrict the flow of data and documentation based on data type.		Endpoint and network devices are evaluated and patched regularly to reduce susceptibility to malicious exploits.

Layered security provides back up in case something goes wrong with encryption, such as employees finding workarounds for encrypted email messages. “You can’t rely on one solution to be the absolute safe harbor,” Laham says.

OCR 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).