COSMOS
Navigate the Compliance Universe

Report on Research Compliance Volume 17, Number 1. January 01, 2020

As MD Anderson Keeps Up Its Legal Fight, U. Rochester Pays OCR $3M

By Theresa Defino

Ah, those pesky residents. If you're a teaching hospital, you can't live without them, right? But sometimes living with them is mighty costly, as the University of Rochester Medical Center (URMC) was the most recent to discover.

Joining a long line of universities and other academic medical centers, URMC in November paid[1] the HHS Office for Civil Rights (OCR) $3 million to settle allegations that it committed five separate HIPAA violations. OCR cited the loss by two resident physicians of a USB drive (2013) and a laptop (2017) as the triggers for its enforcement action. The devices were unencrypted, which was an especially sore point for OCR—as was the fact that URMC was something of a repeat offender.

But just as URMC was agreeing to a multimillion-dollar payment and a two-year corrective action plan (CAP), the University of Texas MD Anderson Cancer Center was keeping up its fight against paying $4.358 million to OCR for nearly identical circumstances—losses of mobile devices and (alleged) lack of encryption. MD Anderson's court appeal,[2] filed in April, is still awaiting a response from HHS, following a recently granted extension.

URMC's breaches were small compared to the thousands—even millions—of records that have been inappropriately used or disclosed over time, but nonetheless proved expensive.

The Laundry Ate My PHI

Oddly, OCR did not say how many people were affected by URMC's 2013 breach, but for breaches affecting 500 or more individuals, covered entities are required to submit notification to OCR, which the agency posts on a web page. According to URMC's 2013 entry, and its public breach notice at the time, the USB drive contained protected health information (PHI) for 537 patients and probably met its fate in a washing machine.

A "resident physician misplaced a USB computer flash drive that carried PHI. The flash drive was used to transport information used to study and continuously improve surgical results. The information was copied from other files and so its loss will not affect follow-up care for any patients," URMC said.

The flash drive was "believed to have been lost at a URMC outpatient orthopaedic facility. After an exhaustive but unproductive search, hospital leaders believe that the drive likely was destroyed in the laundry. A search of the laundry service, which works exclusively with hospital/medical facilities, also failed to locate the drive," URMC reported.

Among the PHI were "names, gender, age, date of birth, weight, telephone number, medical record number, orthopaedic physician's name, date of service, diagnosis, diagnostic study, procedure, and complications, if any." Not included: addresses, Social Security numbers or insurance information.

The second incident was even smaller in terms of patients—just 43 this time, found on an "unencrypted personal laptop of one of its resident surgeons." URMC reported to OCR on Jan. 26, 2017, that the laptop "was

stolen from a treatment facility," OCR said. No other details are available.

According to OCR's Nov. 5 announcement, in 2010 OCR "investigated URMC concerning a similar breach involving a lost unencrypted flash drive and provided technical assistance to URMC. Despite the previous OCR investigation, and URMC's own identification of a lack of encryption as a high risk to [electronic]PHI, URMC permitted the continued use of unencrypted mobile devices."

OCR said its new investigation following the 2013 and 2017 breaches "revealed that URMC failed to conduct an enterprise-wide risk analysis; implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; utilize device and media controls; and employ a mechanism to encrypt and decrypt electronic protected health information (ePHI) when it was reasonable and appropriate to do so."

Safeguards Will Be 'As Strong As Possible'

URMC did not admit wrongdoing as part of the settlement and declined to answer questions from*RRC*, and instead issued the following statement:

> "URMC has agreed to pay $3 million to [HHS] to settle alleged past violations of security requirements for protecting the health information of our patients.
>
> The settlement agreement concludes an investigation into IT security practices at URMC, following two unrelated incidents that the medical center voluntarily reported in 2013 and 2017. Potentially affected patients were notified at the time both of these incidents occurred, and we have no reason to believe that any patient's personal health information was misused.
>
> The medical center is deeply committed to protecting patient privacy, and we continuously improve our IT security safeguards and staff training to reduce the risk of a privacy breach. As part of the settlement with HHS, we will undertake a comprehensive audit of security practices and implement any corrective actions needed to ensure our safeguards are as strong as possible."

CAP Mandates Security Analysis, Training

Under the CAP, URMC must conduct an "accurate and thorough" risk analysis and develop and implement a management plan to address risks and vulnerabilities. Before doing so it must get OCR's approval on a statement of work to ensure that the analysis is adequate to address "vulnerabilities to the confidentiality, integrity, and availability" of URMC's ePHI.

After conducting the risk analysis, URMC is to share with OCR a "risk management plan or plans sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level as required" per the security rule, including a "process and timeline for implementation, evaluation, and revision."

URMC also is required to develop a process to ensure that its risk analysis and management are current, and are revised to keep pace with changes in its environment as well as "HHS guidance, any issues discovered during internal or external audits or reviews, and any other relevant developments." Training materials are also to be revised with the same goal in mind.

As with other settlements, URMC must submit reports to OCR documenting its implementation of the CAP, make it aware of any incidents involving employees that "results in a presumed" breach, and submit an annual update

at the conclusion of each of the two years in the CAP.

Research Data Lost

MD Anderson, meanwhile, will have to wait at least into the new year to see if it can successfully avoid the millions in fines OCR has been trying to impose since 2015 for events that mirror URMC's.

The cancer center's tangles with OCR began as a result of breach notification reports MD Anderson made in 2012 and 2013. In the earlier year, MD Anderson informed OCR in its required annual report that, in April of that year, a laptop was stolen from the home of MD Anderson's then-director of research informatics at its Genitourinary Cancer Center. The PHI of 30,000 individuals was on the computer, which MD Anderson had purchased for him to telework.

The same report noted that a summer intern in a stem cell department lost a personal USB thumb drive containing the PHI of 2,264 individuals downloaded from the cancer center's systems. In December 2013, a visiting professor from Brazil reported a USB drive containing PHI from 3,598 people was missing from her desk. All of the cases involved research data.

In a notice of proposed determination related to the fine, OCR said it tried from Oct. 28, 2015, to Aug. 11, 2016, to reach a settlement. Failing that, OCR assessed $1.348 million for failing to implement access controls, specifically encryption (and decryption), and $3 million for the lost laptop and thumb drives, which OCR said led to impermissible disclosures.

OCR imposed a penalty amount of $2,000 per day for the violations of the encryption implementation specification and considered the period of noncompliance for encryption to be from March 2011 to Jan. 25, 2013.

Multiple Arguments Made Upon Appeal

The agency calculated the fines based on the lowest tier, with infractions found to be of a "reasonable cause." But as was its practice until April, OCR applied an annual cap of $1.5 million, which is how it arrived at such high amounts.

MD Anderson appealed OCR's findings to an administrative law judge, arguing a host of objections, including that the PHI was never shown to have been misused and thus not a true breach, that it was not responsible for the actions of a few individuals in a large organization, that the data didn't have to be protected under HIPAA because it was research-based, and that as a state entity it was exempt from OCR enforcement. Nor did it fail to adequately employ encryption, MD Anderson said.

It also contended that OCR had erred in applying the same annual cap—$1.5 million—for all levels of violations. An administrative law judge, and then a panel, ruled against MD Anderson, which led it to appeal in court.

The point about the high fines has already resulted in significant changes at OCR, however, as in May the agency said, effective immediately, it was dropping the annual maximums. Now they range from $25,000 to $1.5 million per year for identical violations.

New Fine Could Be $450,000

In its most recent filing in the case, now pending before the U.S. Court of Appeals for the Fifth Circuit, MD Anderson elaborated on its earlier arguments, noting that "there has been no harm proven by the Department [of HHS] nor any indication that any data or alleged ePHI was disclosed or accessed by any unauthorized person. The Department's action fails to offer any regulatory or evidentiary basis to support a finding that MD Anderson's

information security efforts did not meet the addressable 'encryption requirements' under HIPAA," the cancer center said. "Indeed, evidence shows that MD Anderson was HIPAA compliant and its encryption efforts met the requirements and were properly implemented."

"MD Anderson cooperated with the Department's five-year long investigations into the three incidents, responding to 12 requests for information with thousands of pages of documentation, including confidential internal compliance program and risk assessments," its attorneys said.

Regarding the December 2013 incident, MD Anderson said the researcher at issue "*disregarded* the encrypted USB device she was furnished by MD Anderson, as well as institutional policy and the training she received, and instead used her own personal USB for purposes of storing certain patient information she was extracting for research purposes."

Also, for the first time, MD Anderson disclosed that under the lowered caps, its alleged infractions would bring penalties of $450,000, not the $4.348 million OCR calculated before the reduction.

The government has yet to file a brief to MD Anderson's appeal. On Dec. 6, HHS was granted an extension to Jan. 17, 2020, to submit its response.

1 Office for Civil Rights, "Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement," HHS, November 5, 2019, http://bit.ly/2R6nrK6.
2 Theresa Defino, "MD Anderson Appeals $4.38 Million Imposed For HIPAA Breaches, Argues Exempt Status," *Report on Research Compliance* 16, no. 5 (May 2019), http://bit.ly/2soevpg.