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

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

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."

This document is only available to subscribers. Please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.