Report on Research Compliance Volume 19, Number 8. July 28, 2022
Breach Costs OK State Nearly $900K; TX System Settles Access Complaint

By Theresa Defino

A breach of protected health information (PHI) six years ago caused by a hacker who accessed Medicaid records has cost Oklahoma State University Center for Health Sciences (OSUCHS) an $875,000 fine, and it also must undertake a litany of corrective actions, including the unusual step of appointing a monitor to oversee those efforts.[1]

The pricey settlement with the HHS Office for Civil Rights (OCR) comes despite the fact that the breach outwardly didn't seem all that serious at the time: no data is believed to have been misused, credit monitoring services were not offered and—another rarity—OSUCHS was never the subject of a class-action suit over the breach.

Yet OCR on said July 14 its investigation found that OSUCHS violated the HIPAA Privacy, Security and Breach Notification rules.[2] An OSUCHS spokesperson told *RRC* the settlement was the product of lengthy negotiations with OCR.

In addition to the requirement for a monitor, the terms of the agreement harken back to OCR's settlements in prior years that found a lack of electronic protections and unmet requirements, including security risk assessments.

The settlement is the second in July involving an academic health system. A day after the OSUCHS announcement, OCR said it had reached 11 additional agreements related to covered entities not providing patients access to their medical records—bringing the total settlements under this initiative to 38.[3]

Memorial Hermann Health System (MHHS), a 17-hospital chain based in southeast Texas, paid $240,000 and agreed to a two-year corrective action plan (CAP) for failing to provide a single patient access to her records in a timely manner, the agency said.[4]

MHHS' payment is the biggest OCR has collected under this initiative; the previous record-holder was Banner Health of Phoenix, Arizona, which paid $200,000 related to two patients who lodged access complaints with OCR.

Breach Notification Was Made in 2018

OCR refers in its documents to OSUCHS as OSU-CHS, which it described as a "public land-grant research university which provides preventive, rehabilitative, and diagnostic care in Oklahoma." OCR's documents show OSUCHS' initial discovery of the breach was marked by misinformation and missteps, although the spokesperson provided more insights into what happened.

In a Jan. 5, 2018, public breach notice by the organization, OSUCHS officials said that on Nov. 7, 2017, they "learned an unauthorized third party had gained access to folders on the OSUCHS computer network. These folders stored Medicaid patient billing information. On November 8th, we took immediate action to remove the folders from the computer network and terminated the third party access. We also launched a thorough investigation, including hiring an independent data security firm. The firm assisted us in determining whether

the folders had been compromised."[5]

The notice, which was reported by DataBreaches.net, said OSUCHS' investigation "could not rule out whether the third party explicitly accessed patient information. The information in the folders may have included patients' names, Medicaid numbers, healthcare provider names, dates of service, and limited treatment information. It is important to note these folders did not contain medical records. A single social security number was contained on the server."

Officials added that they had "no conclusive indication of any inappropriate use of patient information. However, out an abundance of caution, we began mailing letters to affected patients on January 5, 2018. We also established a dedicated call center to answer any questions our patients may have. If you believe your information was affected and do not receive a letter by February 15, 2018, or if you have questions regarding this incident, please call 1-844-551-1727, Monday through Friday, 8 am to 8 pm Central Time. For patients affected by this incident, please be alert to any healthcare services you did not receive from any of your providers. If you learn of any services you did not receive, please contact your provider and Medicaid immediately."

The notice ended with the familiar pledge to protect patient information. "At OSU Center for Health Sciences, we care deeply about our patients. Patient confidentiality is a critical part of our commitment to care and we work diligently to protect patient information. We apologize for any concern or inconvenience this incident may cause our patients. Since this incident, we have implemented additional security measures to enhance the protection of our patient information," it said.

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

Purchase Login