Report on Medicare Compliance Volume 31, Number 30. August 22, 2022

Breach Costs Medical Center $875K; Vulnerability Was Initially Missed

By Theresa Defino

A 2016 breach at Oklahoma State University Center for Health Sciences (OSUCHS) might not have seemed 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.

Yet last month, OSUCHS found itself in a settlement with the HHS Office for Civil Rights (OCR) for alleged HIPAA violations, paying $875,000 and agreeing to a two-year corrective action plan (CAP) that includes the little-employed requirement to appoint an independent monitor to oversee it.[1]

An OSUCHS spokesperson said the settlement was the product of lengthy negotiations with OCR. On July 14, OCR said its investigation found that OSUCHS violated the Privacy, Security and Breach Notification rules.[2] 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."[3]