COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 8. August 11, 2022 2016 Breach Costs OK State Medical Center $875K; System Initially Missed Vulnerability

By Theresa Defino

Oklahoma State University Center for Health Sciences' (OSUCHS) breach 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, OUSUCHS found itself on the receiving end of a settlement with the HHS Office for Civil Rights (OCR) for alleged HIPAA violations, paying $875,000 and agreeing to an extensive, two-year corrective action plan (CAP) that includes the little-employed requirement to appoint an "independent" monitor to oversee those efforts.[1]

An OSUCHS spokesperson told *RPP* the settlement was the product of lengthy negotiations with OCR.

This is the second recent agreement 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.[2] Among them was Memorial Hermann Health System, which paid $200,000 related to two patients who lodged access complaints with OCR.

OCR said on July 14 its investigation found that OSUCHS violated the Privacy, Security and Breach Notification rules.[3]

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."[4]

The notice, 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 [of] 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 [you] 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.

Access First Occurred in 2016

However, the date of the breach was later changed to a full 20 months earlier than OSUCHS had originally stated. According to OCR, electronic protected health information (ePHI) "was first impermissibly disclosed on March 9, 2016."

The agreement states that on Sept. 25, 2016, OSUCHS "discovered that an unauthorized user had previously accessed the same server, with the first date of access occurring on March 9, 2016." But it also didn't believe at the time that "there was electronic PHI stored on that server," which turned out to be incorrect. As noted earlier, OCR said nearly 290,000 individuals' records were affected.

According to OSUCHS spokesperson Monica Roberts, officials "originally discovered the vulnerability in 2016 and took corrective actions. In 2017 we discovered that the corrective actions did not resolve the issue and that was the time we also discovered that PHI was vulnerable."

Roberts added that "we were never able to establish that a hacker actually accessed any protected information." Although the vulnerability was uncovered, there was "no evidence that the data was ever accessed." She confirmed that only Medicaid data was involved. "This was claims-level data like what you would see from a claims clearinghouse. We were not using it for research purposes," she pointed out.

The payment and settlement were "the result of years of investigation and negotiation with OCR," Roberts said. "While there is no evidence that any PHI was actually accessed, we look forward to working with the approved monitor to improve our policies and procedures to make sure we are meeting our obligations to our patients to protect their personal information."

Without providing specifics, OCR said that its "evidence…indicates OSU-CHS's noncompliance with the following provisions of the Privacy, Security, and Breach Notification Rules: Uses and Disclosures of PHI (45 C.F.R. § 164.502(a)); Security Incident Response and Reporting (45 C.F.R. § 164.308(a)(6)(ii)); Risk Analysis (45 C.F.R. § 164.308(a)(l)(ii)(A)); Evaluation (45 C.F.R. 164.308 (a)(8)); Audit Controls (45 C.F.R. § 164.312(b)); Breach Notification to Individuals (45 C.F.R. § 164.404) and Breach Notification to the Secretary (45 C.F.R. § 164.408)."

Within 60 days of the agreement's effective date, OSUCHS is required to hire an "independent monitor," or "designate an individual or entity, to be a monitor and to review OSU-CHS's compliance with this CAP." HHS will approve the hiring of the monitor, who must certify in writing "that it has expertise in compliance with the HIPAA Security Rule and is able to perform the reviews described [in the CAP] in a professionally independent fashion taking into account any other business relationships or other engagements that may exist."

Monitor to Aid, Report on Compliance

The monitor's duties include conducting reviews to "address and analyze OSU-CHS's compliance with this CAP. The Monitor will assist OSU-CHS in conducting assessments to ensure the implementation specifications as described in the Security Rule to prevent, detect, and respond to potential risks and vulnerabilities to ePHI within its environment. The Monitor will assist in the collection of data to serve as evidence of the effectiveness of OSU-CHS's compliance program. The Monitor will further define and recommend the tools to assist OSU-CHS in protecting the ePHI it creates, receives, maintains, and transmits. In addition, the Monitor will recommend security measures to ensure the confidentiality, integrity, and availability of ePHI received, created, maintained, and transmitted within OSU-CHS's covered components," according to the CAP.

OSUCHS can't terminate or remove the monitor without prior approval from HHS. Conversely, HHS can require such termination if it "has reason to believe that a Monitor does not possess the expertise, independence, or objectivity required by this CAP, or has failed to carry out its responsibilities as set forth in this CAP." HHS can also "conduct its own review to determine whether the Monitor reviews or reports complied with the requirements of the CAP and/or are inaccurate," which it calls a "validation review."

Security Policies to Follow Analysis

Under the CAP, OSUCHS also must undertake a "security management process," which includes a "comprehensive, enterprise-wide risk analysis of the security threats and vulnerabilities" of ePHI that it has "created, received, maintained or transmitted" and reside on "electronic media, workstations, and information systems owned, controlled or leased" by the organization. It also must "develop a risk management plan to address and mitigate any security threats and vulnerabilities identified in the risk analysis." Both the risk analysis and risk management plan must be submitted to HHS for approval.

Additional requirements include drafting "as necessary" written policies and procedures "to comply with the Federal standards that govern the privacy and security of individually identifiable health information and to address any threats and vulnerabilities to the ePHI identified in the risk analysis and risk management plan." As with the security risk analysis and management plan, HHS must approve the policies.

Another area of specific attention is breach notification policies and procedures; OSUCHS must ensure it addresses "the issue of timely notification to affected individuals to ensure that individual notification is done in addition to any necessary substitute notice or media notification." These are among the policies that must be approved by HHS and then offered to employees for training.

A version of this story originally appeared in *Report on Research Compliance*, *RPP*'s sister publication.[5] For more information, see https://www.hcca-info.org/rrc.

1 U.S. Department of Health & Human Services, "Oklahoma State University – Center for Health Sciences (OSU-CHS) Resolution Agreement and Corrective Action Plan," resolution agreement, July 14, 2022, https://bit.ly/3yUVbOU.
2 Jane Anderson, "OCR Adds Eight Access Settlements; Enforcement Actions Now Total 38," *Report on Patient Privacy* 20, no. 8 (August 2022).
3 U.S. Department of Health & Human Services, "Oklahoma State University – Center for Health Services Pays $875,000 to Settle Hacking Breach," news release, July 14, 2022, https://bit.ly/3uVoMqr.
4 Dissent, "Oklahoma State University Center for Health Sciences Notice to Medicaid Patients of a Data Security Incident," DataBreaches.net, January 5, 2018, https://bit.ly/3cHROne.

5 Theresa Defino, "Breach Costs OK State Nearly $900K; TX System Settles Access Complaint," *Report on Research Compliance* 19, no. 8 (August 2022), https://bit.ly/3zy1zMn.