COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 10. October 10, 2019 Privacy Briefs: October 2019

By Jane Anderson

◆ **A U.S. senator is demanding answers after an investigation found that medical images belonging to millions of Americans, including X-rays, MRIs and CT scans, were sitting unprotected on the internet** and available to anyone with basic computer expertise. The records are held by various companies on at least 187 servers in the United States, the nonprofit journalism outlet *ProPublica* found. Some of the records belonged to MobileXUSA, which displayed the names of more than one million patients after a searcher typed in a data query. Dates of birth, doctors and procedures were included. MobileXUSA said it tightened its security following an alert from *ProPublica*, but Sen. Mark Warner, D-Va., in a Sept. 23 letter to company CEO Andrei Soran, asked the company a series of questions about audits and monitoring tools it uses to remain HIPAA-compliant, server encryption practices, and whether it has an internal security team or an outsourced team. Read the *ProPublica* investigation at https://bit.ly/2miKEvj and Warner's letter at https://bit.ly/2nWBm98.

◆ **Sophisticated cyberattacks will place hospitals' operations and revenues increasingly at risk and could affect patient safety, according to a report from Moody's Investors Service.** This could expose hospitals to malpractice accusations and lawsuits, the report says. Small hospitals that lack the resources and modern technology to keep their security systems updated face the most risk from this problem, according to the report, written by Moody analysts Jenn Barr and Lisa Goldstein. The interconnected nature of hospital operations and IT infrastructure creates financial and operational challenges for the sector, the two say. Order the report at https://bit.ly/2nbw6ys and listen to a podcast from Barr and Goldstein at https://bit.ly/2oEs4Pn.

◆ **Provider group Premier Family Medical says it is alerting 320,000 patients about a ransomware incident that left the organization's 10 locations across Utah unable to access data.** The ransomware attack occurred on July 8 and affected all of the company's locations. "Premier was temporarily unable to access data from certain systems within its organization," the group said in its statement. "Even though our investigation has found no reason to believe patient information was accessed or taken, we are very concerned that this event even occurred and have taken steps to further enhance the security of our systems," Robert Edwards, Premier's chief administrator who oversees cybersecurity and privacy programs, said in a statement. The provider group said it would notify affected patients. Read the group's notification at https://bit.ly/2o2rIlf.