COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 4. April 07, 2022 Privacy Briefs: April 2022

By Jane Anderson

◆ **Dallas-based JDC Healthcare Management, which runs more than 70 dental and orthodontics practices in Texas, is notifying more than 1 million individuals about a breach that it says "may affect the security of some personal information."**[1] Around Aug. 9, JDC said it "became aware of a malware incident impacting certain company systems. JDC immediately worked to restore its systems and launched an investigation, with assistance from third-party computer forensic specialists, to determine the nature and scope of the incident." According to the company's breach notification, the investigation determined that "certain JDC data was subject to unauthorized access and/or acquisition during the incident between July 27, 2021 and August 11, 2021." Information that could have been accessed or acquired included clinical information, demographic information such as Social Security numbers, driver's license numbers and dates of birth, health insurance information, and financial information, the company said. It did not mention offering free credit monitoring and identity protection services.

◆ **An urgent care center in Lincoln, Nebraska, alleged in a lawsuit that a data breach at the company that handled its billing led to the discovery of a number of claims that went unpaid over several years.**[2] In the lawsuit filed in February, Urgent Care Clinic of Lincoln PC argued that after a ransomware attack on PracticeMax in 2021, the urgent care clinic discovered "a significant number of claims that were either not handled properly, not processed at all or otherwise neglected." PracticeMax, based in Arizona, provides billing, information technology, practice management and other services to health care offices. The company has a regional office in Lincoln. PracticeMax posted a notice on its website that states it discovered ransomware had been installed on some of its systems in 2021, and that there may have been unauthorized access to its systems between April 17 and May 5. The lawsuit does not link the unpaid claims directly to the ransomware attack. In fact, the lawsuit states that some of the claims date as far back as 2019 and further. However, the breach investigation led to the unpaid claims being discovered, the lawsuit said. The suit alleges negligence, breach of contract and unjust enrichment by PracticeMax, and the urgent care center said that its losses are "well in excess" of the $75,000 minimum for the case to qualify to be filed in federal court. Michael Johnson, CEO of PracticeMax, said his company has "successfully processed tens of thousands of claims" for Urgent Care Clinic of Lincoln over a number of years, and added, "in the case, they are claiming issue with a couple of hundred claims, which will have to be evaluated through due process."