COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 9. September 09, 2021 Privacy Briefs: September 2021

By Jane Anderson

◆ **DuPage Medical Group in Chicago said that the personal information of more than 600,000 patients may have been compromised in a July cyberattack.** The medical group, which is Illinois' largest independent physician group, experienced a computer and phone outage that lasted nearly a week in mid-July. When the group worked with digital forensic specialists to investigate the incident, it found that the outage was caused by "unauthorized actors" who accessed its network between July 12 and 13. The investigators determined on Aug. 17 that certain files containing patient information may have been exposed. Compromised information may have included names, addresses, dates of birth, diagnosis codes, codes identifying medical procedures, and treatment dates. For a small number of people, Social Security numbers may have been compromised, the medical group said.[1]

◆ **Hundreds of thousands of health records in a Texas county that included COVID-19 vaccination details were exposed in a data breach involving an app, officials said.** Although early estimates of the breach from Denton County Public Health put the number of exposed records at 1.2 million, county officials said many of the files were duplicates. A problem with third-party software exposed the contact and identifying information. Letters have been sent to those affected, county officials said. The breach was discovered in July, and at that time, vaccine clinics stopped using the app involved while the problem was fixed. The app is back in use, the county said.[2]

◆ **A class-action lawsuit has been filed against Sturdy Memorial Hospital in Attleboro, Massachusetts, alleging the hospital failed to properly protect personal patient information that was stolen in a ransomware attack earlier this year.** The suit was filed Aug. 26 in Plymouth Superior Court by attorneys for Barbara Ragan Bennett, a resident of Plymouth County, and on behalf of "all others similarly situated." Some 35,272 people in total may have been affected by the breach in the ransomware attack, which took place Feb. 9, the lawsuit states. The suit is seeking an unspecified amount of damages, including extended credit monitoring, "actual damages, compensatory damages, statutory damages and statutory penalties, punitive damages and attorneys' fees and costs." Sturdy Memorial Hospital paid an undisclosed ransom to the hacker to get its information back and offered all those affected two years of free credit monitoring, according to the lawsuit. However, attorneys for Bennett said that Sturdy should have prevented the theft of the information. "Defendant maintained and secured the PII (personally identifiable information) in negligent manner by failing to safeguard against ransomware attacks," the complaint said. "Had Sturdy properly maintained its IT (information technology) systems, it could have prevented the data breach." Although a ransom was paid, the complaint alleges that payment does not guarantee personal information will be protected. "Defendant cannot reasonably maintain that the data thieves destroyed the information they obtained, or more generally, that the harm to the victims has been cured," the lawsuit stated. Some of the information stolen included names, contact information, dates of birth, Social Security numbers, Medicare health insurance claim numbers, driver's license numbers and medical history. In addition, lawyers argued that the two free years of a credit monitoring service are insufficient "because misuse of the information taken in the breach is likely to last longer than two years, and further, that credit monitoring alone does not compensate victims for the consequences of the breach." Court documents said damages exceeded $50,000.[3] The hospital provided notice of the data breach on May 28.[4]