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]

◆ **The FBI is warning organizations that Hive ransomware, which uses mechanisms such as phishing emails with malicious attachments and remote desktop protocol to access and move through victim networks, exfiltrate and encrypt files, is on the rise.** This ransomware variant creates significant challenges for defense and mitigation, according to the FBI. Hive ransomware seeks processes related to backups, anti-virus/anti-spyware and file copying and terminates them to facilitate file encryption. The encrypted files commonly end with a ".hive" extension. After compromising a victim network, exfiltrating data and encrypting files, the actors leave a ransom note in each affected directory within a victim's system, which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site "HiveLeaks." The note contains a "sales department" link, accessible through a Tor browser, that enables victims to contact the actors through a live chat. Some victims reported receiving phone calls from Hive actors requesting payment for their files, the FBI said. The initial deadline for payment ranges between two and six days, but the FBI reported that actors have prolonged the deadline in response to contact by the victim company.[5] John Riggi, American Hospital Association (AHA) senior advisor for cybersecurity and risk, said the Hive ransomware is problematic. "This new strain of ransomware may be of particular concern for health care and utilizes the 'double extortion' method — demand for ransom payment for decryption key to access on-site encrypted data along with ransom payment demand to prevent public release of stolen patient information. The FBI and AHA strongly discourage payment of ransom if at all possible. Regardless of whether you or your organization decide to pay the ransom, the FBI urges you to report ransomware incidents to your local field office."[6]

◆ **The Savannah, Georgia, area's largest health care system, St. Joseph's/Candler, returned to "fully operational" status in mid-August after suffering a cyberattack on its IT network earlier this year,** hospital officials said. The ransomware attack was detected on June 17, but further investigations revealed that the unauthorized party gained access to the hospital system's IT network between Dec. 18, 2020, and June 17, 2021, according to a letter sent to patients. Although the health system did not cancel any surgeries or procedures, the attack did temporarily halt telephone communications and accessible computer systems, making certain files inaccessible. Also, cancer treatment patients were asked to verify appointments for a period of time. "We're fully operational right now," CEO and president Paul Hinchey said. "There are a few hotspots where we have to change out computers. But in terms of the hospital…we're back electronically, which was a big sea change for us, because we went from a fully integrated system to a paper system and we haven't done that in 25 years." Hinchey said he isn't ruling out the possibility that patients' personal information might have been compromised in the attack, and the hospital system is offering a free year of identity theft monitoring. In a letter to patients, St. Joseph's/Candler stated that possible information at risk includes "name in combination with address, date of birth, Social Security number, driver's license number, patient account number, billing account number, financial information, health insurance plan member ID, medical record number, dates of service, provider names, and medical and clinical treatment information regarding care you received from SJ/C." Hinchey said the health system is increasing its security to mitigate future risks. "These entities, they reinvent themselves at warp speed," he said. "So we've hired several national companies, one who does all the security for Amazon, and we put in all of these firewalls to make sure we mitigate that as best we can from ever happening again because once is enough."[7]

◆ **Indiana Attorney General Todd Rokita is warning state residents to watch their data after a ransomware attack and breach at Eskenazi Health.** It's unclear how many patient records may have been affected in the July attack, although some of the data was posted on the dark web. "As with any major breach, Hoosiers should protect and monitor their personal information closely," Rokita said. "Our Office's Data Privacy and [Identity] Theft Unit is prepared to direct consumers to data theft resources to combat further damage and prevent additional harm if they become victims of scammers and fraud." Eskenazi Health said it has seen no evidence that the data breach has resulted in bank or credit card fraud. "Through our investigation, we have learned that some data that we

maintain was obtained by bad actors and released online," the organization said in a statement. "Our forensic experts are monitoring for this, we have identified files that the hackers obtained, and we have begun the painstaking process of examining those files for any personal patient or employee information. If we find such information, we will notify the affected individuals in accordance with law and offer identity protection and credit monitoring services." The hospital has said it did not pay the requested ransom.[8]

1 Lisa Schencker, "A DuPage Medical Group data breach may have affected 600,000 patients. Here's what patients should know." *Chicago Tribune*, August 30, 2021, https://bit.ly/2WJfgZ2.
2 WBAP, "Denton County Data Breach Exposes Health Records, Including COVID Vaccination Details," August 31, 2021, https://bit.ly/3mVCqqi.
3 George W. Rhodes, "Sturdy Hospital in Attleboro sued over data breach," *The Sun Chronicle*, August 31, 2021, https://bit.ly/3t4HuK6.
4 Sturdy Memorial Hospital "Notice of Data Security Incident," news release, May 28, 2021, https://bit.ly/3BsVMae.
5 Federal Bureau of Investigation, Cyber Division, "Indicators of Compromise Associated with Hive Ransomware," MU-000150-MW, *FBI Flash*, August 25, 2021, https://bit.ly/3DwMvzM.
6 "FBI alerts organizations to new ransomware threat," American Hospital Association, August 25, 2021, https://bit.ly/3DE6ahb.
7 Nancy Guan, "St. Joseph's/Candler ransomware investigation ongoing, patients offered identity protection," *Savannah Morning News*, August 18, 2021, https://bit.ly/3zCkPHf.
8 WTHR.com staff, "Indiana AG Issues Warning for Hoosiers After Hospital Data Breach," WTHR, August 27, 2021, https://bit.ly/3gUE7R0.