Report on Patient Privacy Volume 21, Number 6. June 10, 2021

Privacy Briefs: June 2021

By Jane Anderson

◆ **Scripps Health in San Diego experienced what it called "an information technology security incident" from ransomware that was detected May 1, forcing some of its operations offline.** The attack crippled the health care system's networks, and the system still was struggling to bring everything back online in late May. "We suspended user access to our information technology applications related to operations at our health care facilities, including MyScripps and scripps.org," the health care system said on Twitter on May 1.[1] "While our information technology applications are offline, patient care continues to be delivered safely and effectively at our facilities, utilizing established back-up processes, including offline documentation methods. Our outpatient urgent care centers and Scripps HealthExpress locations and Emergency Departments remain open for patient care." In a letter to patients released May 24, Scripps Health CEO Chris Van Gorder confirmed the cyberattack stemmed from ransomware, but he provided few details on recovery work because "in our current situation, openly sharing the details of the work we have been doing puts Scripps at an increased risk of coming under further attack, and of not being able to restore our systems safely and as quickly as possible for you."[2] The letter stated that "other attackers" are using the information being reported in the media "to send scam communications to our organization," and added that "I know that, for some of you, the reasons why we haven't provided more frequent updates may not matter. But it was important for me to share and assure you that our patients', employees', and physicians' safety and security are our constant guides." The hospital system has not said whether the ransomware resulted in a data breach that compromised protected health information.

◆ **A ransomware attack on the Midwest Transplant Network, based in Westwood, Kansas, resulted in a data breach that affected more than 17,000 patients.** The breach occurred in February and locked the nonprofit organ transplant registry organization out of its files for a brief period. According to a letter sent to those affected, the attackers were able to obtain protected information about deceased donors and organ recipients, including names, dates of birth and types of organ donations and transplant procedures. Midwest Transplant Network spokesperson Michala Stoker said she couldn't say whether the organization had paid the ransom or not. Stoker also said that the organization had no reason to believe that the attackers had sold or otherwise distributed the data they obtained, but the network has, "out of an abundance of caution," contracted with a cybersecurity firm to address inquiries about the incident.[3]

◆ **Rehoboth McKinley Christian Health Care Services, a nonprofit with locations in Arizona and New Mexico, disclosed a data breach on May 19 that affected around 200,000 people, including both patients and employees.**[4] According to the organization, it learned on Feb. 16 that "certain patient information may have been removed from its computer network as a result of potential unauthorized activity that it had been investigating." A third-party forensic firm determined that an unauthorized party was able to gain access to systems that contained patient information and remove some data between Jan. 21 and Feb. 5. The patient information may have included five types of data: (1) information to identify and contact the patient, such as names, dates of birth, addresses, telephone numbers, and email addresses; (2) Social Security numbers, driver's license numbers, passport numbers and/or tribal ID numbers; (3) health insurance information, such as insurer names, plan numbers, and member numbers; (4) medical information, such as medical record numbers, dates of service, provider names, prescription information, treatment, and diagnosis information; and (5) billing and claims information, including financial account information. Rehoboth McKinley is providing free identity monitoring and restoration services to all individuals whose personal information may have been involved.

◆ **The city of Philadelphia said that a data breach first identified in March 2020 affected more departments than initially thought.**[5] The breach, which resulted when an employee's email account was compromised due to a phishing attack, affected people receiving services from the city's Department of Behavioral Health and Intellectual disAbility Services. It also impacted Community Behavioral Health, a nonprofit organization that contracted with the city to administer HealthChoices, a behavioral health program for Medicaid beneficiaries. The city's investigation revealed that the breach affected other city employee emails in departments outside of the health departments. Email accounts held by employees in the health department and at Community Behavioral Health were accessed without authorization between March and mid-November 2020, according to the city. Other city department emails were accessed from March 2020 to January. Philadelphia city officials have not yet said whether emails and/or confidential email attachments were viewed due to the breach. The accounts affected had access to demographic and health-related information for people receiving services through the city health department and its outside mental health contractor, and data in those email accounts included names, dates of birth, addresses, account and medical record numbers, health insurance information, clinical information such as diagnoses and descriptions of services individuals were receiving, and copies of birth certificates, driver's licenses and Social Security cards. The city has been informing affected individuals since August and is providing credit and identity theft monitoring services.

◆ **Third-party pharmacy contractor CaptureRx was targeted in a ransomware attack that exposed the data of 1.6 million patients.**[6] The breach occurred on Feb. 6 and was reported to at least 13 health systems and health care organizations affected in April. St. Lawrence Health System in Potsdam, New York, said that it learned of the data breach on April 5.[7] The breach may have affected individuals whose information was provided to CaptureRx to assist with the federal 340B drug pricing program, which provides financial help to hospitals serving vulnerable communities to manage rising prescription drug costs, according to St. Lawrence Health. CaptureRx provided compliance and cost-saving services to St. Lawrence Health System's Massena Hospital for its 340B-eligible prescriptions. The breach included limited data on 1,897 Massena Hospital patients, the hospital system said. The files breached contained first and last names, dates of birth, pharmacy information, and medical record numbers for some patients. St. Lawrence Health officials said CaptureRx became aware in February of unusual activity and then launched an investigation. Trinity Health System in Ohio also was affected by the CaptureRx data breach. The health system's Twin City Hospital in Dennison, Ohio, said that 9,500 patients were impacted by the CaptureRx security incident. The health system urged affected individuals to "remain vigilant against incidents of identity theft and fraud, to review their account statements and explanation of benefits forms, and to monitor their free credit reports for suspicious activity and to detect errors."[8]

◆ **Pennsylvania lawmakers are working to crack down on third-party vendors hired by the state after a news investigation uncovered a data breach in a vendor performing COVID-19 contact tracing.**[9] Channel 11 in Pittsburgh reported in April that Insight Global, the company hired by the state to do its COVID-19 contact tracing, had exposed the personal data of more than 70,000 state residents. The data exposed included names, addresses, phone numbers and health information. State senators held a hearing on May 24 to examine contracts for third-party vendors, and have amended proposed legislation on data breaches to include third-party vendors hired by the state. That bill would require all state agencies, counties, municipalities and school districts in the state that are involved in a data breach to alert those affected within seven days. Insight Global waited nearly a month before beginning notifications, according to state lawmakers. "We still don't have clear answers from the department of health as to what exactly happened with this contractor," said Sen. Pat Stefano. "When did the data get breached? How did it happen?"

[1] Scripps Health (@ScrippsHealth), “Scripps Health experienced an information technology security incident detected late on May 1, 2021,” Twitter, May 2, 2021, https://bit.ly/3yX4QUe.

[2] Mark Saunders, “Scripps Health ‘working around the clock’ to restore system due to ransomware,” ABC 10News San Diego, May 24, 2021, https://bit.ly/3paBPQA.

[3] Dan Margolies, “Ransomware Attack on Midwest Transplant Network Affects More Than 17,000,” KCUR 89.3, May 3, 2021, https://bit.ly/3fZagpn.

[4] Rehoboth McKinley Christian Health Care Services, “Notice of Data Breach,“ May 19, 2021, https://bit.ly/3uQlWjL.

[5] Emily Scott, “Philly data breach that impacted health employee emails also hit other departments,” WHYY, May 27, 2021, https://bit.ly/3vLOSL0.

[6] Tracey Drury, “Kaleida Health becomes sixth health-care victim of security breach,” WGRZ, May 26, 2021, https://bit.ly/34AAAkg.

[7] Bob Beckstead, “St. Lawrence Health reports data breach at Massena Hospital,” NNY360, May 29, 2021, https://bit.ly/3ccs5jx.

[8] “Trinity Twin City reports data breach, more than 9,000 affected,” WTOV9, May 26, 2021, https://bit.ly/34EHHZ8.

[9] Rick Earle, “State lawmakers have amended a bill to deal with data breaches after a Target 11 investigation,” Target 11, May 24, 2021, https://bit.ly/3cczu2j.