COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 2. February 09, 2023 Privacy Briefs: February 2023

By Jane Anderson

◆ **DCH Health Systems, based in Tuscaloosa, Ala., said it fired an employee in December after a routine privacy audit revealed evidence that the worker had accessed some 2,530 patient electronic medical records without a legitimate reason.** The information that may have been accessed and viewed without authorization contained the following data elements: name, address, date of birth, Social Security numbers, dates of provider encounters, diagnoses, vital signs, medications, test results, and clinical/provider notes, DCH Health Systems said in a breach notification posted on its website. The initial routine audit found evidence that the employee had accessed one patient's records on Dec. 5, the health system said. "Upon identifying the initial inappropriate access, DCH Health System immediately suspended the employee and terminated the employee's access to all medical records and other information systems. Upon further investigation to assess the information impacted, DCH subsequently terminated the individual's employment one business day after initial discovery." It also engaged a data breach recovery expert and "established all required and necessary communications to the affected patients and regulatory officials," the health system said. It also will offer free identity theft protection services to all patients whose insurance group and subscriber/policy numbers may have been involved.[1]

◆ **The FBI and law enforcement officials in Europe, said they have shut down a major ransomware operation accused of extorting more than $100 million from organizations worldwide.** Attorney General Merrick Garland said the ransomware group Hive, first detected in June 2021, had attacked hospitals, school districts, financial firms and others, stealing and sometimes publishing their data. Law enforcement was able to hack Hive and infiltrate its networks for seven months, officials said, stealing the decryption keys and quietly giving them to 336 victims before taking full control of hive servers in the United States and Europe, knocking them offline and preventing new infections. Officials said they had not made any arrests and did not say they had seized any proceeds from paid ransoms, but the investigation is continuing. Only about 20% of Hive's U.S. victims notified authorities, according to the FBI; however, the FBI could identify others from the Hive infrastructure it had infiltrated and worked to help them as well. At times, it was able to contact victim organizations, including one university, before the encryption had been deployed. U.S. officials credited German and Dutch authorities, along with Europol, for helping in the case. Hive operated as a "ransomware as a service" organization, partnering with independent hackers who broke in via phishing or other means, the FBI said. Memorial Health System in Marietta, Ohio, fell victim to Hive in August 2021, forcing a move to paper charts before the health system came to a "negotiated solution" with its attackers.[2]

◆ **According to UCLA Health, "the use of analytics tools on the UCLA Health website and mobile app" led to a data breach that potentially exposed personal data from some 94,000 individuals.** Specifically, UCLA Health said in its data breach notification that the tools used on an appointment request form may have captured and transmitted "certain limited information" to third-party analytics providers, which it did not name. "In April 2020, UCLA Health began using analytics tools from third-party service providers on our public website, UCLAHealth.org, and a related mobile app to understand how our community interacted with them," the health system said in its breach notification. "Analytics tools allow organizations to review website and app activity in the aggregate to develop more effective and efficient communication. When in June 2022 UCLA Health learned of concerns related to the use of these analytics tools by health-care providers, we disabled them. Additionally, UCLA Health initiated

a review, supported by a third-party forensic firm, to complete a comprehensive analysis of the use of these analytics tools on its website and mobile apps, evaluate what data these analytic tools collected, and determine to whom the data belonged." Information that may have been collected included information about providers and Internet Protocol addresses of website visitors, UCLA Health said.[3]

◆ **A lawsuit filed Jan. 10 accused Christ Hospital in Cincinnati of communicating patient information to Facebook parent company Meta via pixels embedded in Christ Hospital's website.** The lawsuit, initially filed in Hamilton County and moved to federal court, alleges that Christ Hospital "secretly deployed" Meta pixel on its website to collect patient information. That line of code tracked and disseminated patients' activity on the website, including search histories for physicians, patients' Internet Protocol addresses, and the types of illnesses or injuries for which they were seeking treatment, according to the lawsuit. From the connection to Meta, the harvested data "can and likely will" be further disseminated to third parties for retargeted ads, to insurance companies seeking patient information for profit, or "to criminals on the dark web for use in fraud and cyber crimes," according to the lawsuit. The suit also alleges that Meta pixel could have compromised patient information from Christ Hospital's MyChart. The plaintiff in the lawsuit, identified only as Jane Doe, is requesting a jury trial and is seeking punitive damages of more than $25,000.[4]

◆ **Ransomware attacks on health care organizations more than doubled from 2016 to 2021, compromising tens of millions of patients' personal information and potentially jeopardizing their care,** investigators reported in the *JAMA Health Forum*. The study said that 374 ransomware attacks were carried out against clinics, hospitals, dental offices, diagnostic laboratories, emergency medical services and other health care delivery organizations between 2016 and 2021. During that period, the annual number of attacks rose from 43 to 91, the study said, exposing the personal health information of nearly 42 million patients. The study also found that almost half of ransomware attacks during the study period affected health care delivery, leading to downtime of electronic systems and often forcing providers to rely on pen-and-paper charting. In addition, the attacks forced health care systems to cancel scheduled procedures and divert ambulances away from hospitals' emergency rooms. Over time, the researchers found the ransomware attacks became increasingly sophisticated, and victims were less likely to be able to restore data from backup systems, stolen patient data was more likely to become public and attacks involving organizations with multiple facilities increased.[5]

1 DCH Health System, "Notice to Our Patients of Data Privacy Event," news release, January 19, 2023, https://bit.ly/3JvjKZS.
2 Joseph Menn, Perry Stein, and Aaron Schaffer, "FBI shuts down ransomware gang that targeted schools and hospitals," *The Washington Post*, January 26, 2023, https://wapo.st/3WUWVBP.
3 UCLA Health, "UCLA Health Data Notice," January 13, 2023, https://bit.ly/3jewx8l.
4 Felicia Jordan, "Lawsuit: Christ Hospital website sends patient information to Meta, other third parties," WCPO Cincinnati, January 26, 2023, https://bit.ly/3wQf7Sl.
5 Jill Pease, "Health care ransomware attacks more than double in five years, study finds," University of Florida Health Newsroom, January 17, 2023, https://bit.ly/3YekCWG.