COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 10. October 14, 2021 Privacy Briefs: October 2021

By Jane Anderson

◆ **A data breach at University of New Mexico (UNM) Health may have allowed a third party to obtain medical records from more than 600,000 patients—more than a quarter of the state's population.** UNM Health has been mailing letters to affected patients who had been treated at UNM Hospital, UNM Medical Group or the UNM Sandoval Regional Medical Center, hospital officials said. The breach occurred on May 2 and was discovered on June 4, according to UNM Health's statement. Patient names, medical record numbers and Social Security numbers were among the information obtained during the data breach, said Michael Richards, senior vice chancellor for clinical affairs at UNM Health System. Richards added that electronic medical records were not involved, and that there was no indication that any information has been misused. UNM Health will provide complimentary credit monitoring and data protection services to patients who had their Social Security numbers taken.[1]

◆ **Indianapolis-based Eskenazi Health said a cyberattack that occurred "on or about August 4, 2021," resulted in the compromise of personal information belonging to employees and patients, including health information. Some of the information was posted on the dark web, the health system said.** Eskenazi Health's information security team took the network offline when the breach was detected. Cybercriminals gained access to the network May 19 and disabled security protections, which made it more difficult to detect their presence prior to the attack, the health system said. Investigators determined that stolen medical, financial and demographic information was posted, including names, dates of birth, ages, addresses, telephone numbers, email addresses, medical record numbers, patient account numbers, diagnoses, clinical information, physician names, insurance information, prescriptions, dates of service, driver's license numbers, passport numbers, face photos, Social Security numbers and credit card information. Eskenazi Health will provide identity theft protection for affected individuals.[2]

◆ **Improper disposal of hard drives potentially exposed personally identifiable information and protected health information for nearly 117,000 people, mainly Maine residents**, according to a data breach report filed by attorneys for HealthReach Community Health Centers, based in Waterville, Maine. The breach occurred on April 7 and was discovered on May 7, according to the report, which was filed with the Office of the Maine Attorney General.[3] Information that was breached included names, addresses, dates of birth, Social Security numbers, medical insurance information, laboratory results, medical record numbers and treatment records, according to HealthReach, which said there is no evidence any of the information was misused. HealthReach said in a press release that the hard drives were improperly disposed of by an employee at a third-party data storage facility.[4]

◆ **A California woman was sentenced in Boston to three years' probation and fined $2,500 after pleading guilty to violating the HIPAA statute**. Stefanie Hirsch, 51, of Los Angeles, sold access to a Medicare eligibility tool that allowed two others, Juan C. Perez Buitrago and Nathan LaParl, to improperly access patients' detailed personal, demographic, medical and insurance information, according to the Massachusetts U.S. Attorney's Office. Hirsch owned EI Medical Inc., a Medicare-enrolled wheelchair and scooter repair company that qualified for access to a health care clearinghouse that contains Medicare patients' personal, medical and insurance information. Hirsch improperly gave Perez Buitrago and LaParl access to that clearinghouse and charged them about 25 cents per

patient eligibility check, the U.S. attorney's office said. Using Hirsch's credentials, LaParl accessed personal and medical data for more than 350,000 patients, and Perez Buitrago's credentials were used for 150,000 patients. Both Perez Buitrago and LaParl previously pleaded guilty to federal health care crimes.[5]

◆ **UC San Diego Health faces a lawsuit over a four-month data breach that began in late 2020 that potentially exposed sensitive information from nearly a half-million.** According to a report, "Lawyers representing an El Cajon cancer patient filed legal action this week in San Diego federal court alleging negligence, breach of contract, and violation of California consumer privacy and medical confidentiality laws. It seeks class-action status and unspecified damages for all individuals whose personal and medical information may have been compromised." Jason Hartley, an attorney in San Diego, said, "Patients should trust that their most private medical results will not be made public, and that their medical visits will not leave them at risk for identity theft. … This breach was preventable—had UC San Diego Health had the right data protection protocols in place." UC San Diego Health announced in July that hackers had gained unauthorized access to email accounts from Dec. 2, 2020, through April 8. Nearly 496,000 individuals were affected by the breach, which exposed names, addresses, dates of birth, claims information, lab results, medical diagnoses and treatment information, prescription information and Social Security numbers, among other information.[6]

◆ **Data for people who received COVID-19 tests at Walgreens was left on the open web and was accessible to multiple ad trackers on Walgreens' site, according to an investigationby journalists at *Recode*.**[7] The issue appears to date to when Walgreens first offered COVID-19 testing in spring 2020, according to the site. Following publication of an article detailing the issue, Walgreens denied that its original page setup was insecure but added an authentication screen that required users to enter the patient's date of birth before viewing information. However, *Recode* reported that "multiple ad trackers are still present on the patient pages." Walgreens said "that it added 'an additional layer' to the site out of an abundance of caution, adding that it was not aware of any credible evidence of unauthorized access to patient data." Alejandro Ruiz, a consultant with Interstitial Technology PBC who first discovered the potential data leak, told *Recode* he would prefer a more secure verification method, such as a password. He also noted that the interface that allows Walgreens and its advertisers to exchange data remains active.

1 Ryan Boetel, "Thousands of UNM Health records breached," *Albuquerque Journal*, September 14, 2021, https://bit.ly/3FozGZq.
2 Elena Stidham, "Data breach on Eskenazi Health resulted in info being posted on dark web," Fox 59, October 1, 2021, https://bit.ly/3iyn3RC.
3 "Data Breach Notifications," Office of the Maine Attorney General, accessed October 10, 2021, https://bit.ly/3lmV8WR.
4 HealthReach Community Health Centers, "HealthReach Community Health Centers notifies Individuals of Data Security Incident," news release, September 14, 2021, https://bit.ly/3lhiWLw.
5 Department of Justice, U.S. Attorney's Office for the District of Massachusetts, "California Woman Sentenced in Multi-Million-Dollar Medicare Fraud Scheme," news release, September 22, 2021, https://bit.ly/3iBSU3X.
6 Mike Freeman, "UC San Diego Health sued over data breach that may have exposed records of 500,000 patients," *The San Diego Union-Tribune*, September 23, 2021, https://bit.ly/2ZWBGHX.
7 Sara Morrison, "How Walgreens' sloppy Covid-19 test registration system exposed patient data," *Recode*, September 20, 2021, https://bit.ly/3DdNPGQ.