COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 5. May 07, 2020 Privacy Briefs: May 2020

By Jane Anderson

◆ **Ambry Genetics, based in Aliso Viejo, California, has reported a data breach involving nearly 233,000 people.** In its statement,[1] the company said it identified "unauthorized access to an employee's email account between January 22-24, 2020." Ambry Genetics said it promptly initiated an investigation and brought outside experts onboard, but it was "unable to determine whether there was unauthorized access to, or acquisition of, any particular information from the email account." The information that could have been disclosed includes names, Social Security numbers, medical information and other information related to the services Ambry provides, the company said. Ambry is offering affected customers identity monitoring services.

◆ **The city of Detroit is offering free credit monitoring to around 2,000 residents after their personal information was exposed briefly through the city's health department website**. The breach occurred on March 28, and the city's Department of Innovation & Technology was able to contain it within a few hours, representatives said in a statement.[2] No Social Security numbers were exposed, and the technology department said it had strengthened security protocols as a result of the breach, which was the second breach involving governments in the metro Detroit area in a month. Oakland County officials said in mid-April that internal COVID-19 data used by the Oakland County health department was briefly exposed on the WeChat application for nearly 12 hours between April 14 and 15, when administrators secured it.

◆ **In another Detroit-area data breach, Beaumont Health revealed in April that a data breach occurring in 2019 may have exposed the personal information of up to 112,000 people.**[3] The eight-hospital system launched an investigation and worked with cybersecurity professionals immediately after learning that an unauthorized third party accessed some employee email accounts, representatives of the hospital system said in a statement. "After an extensive forensic investigation and comprehensive manual document review, we discovered on March 29, 2020, that one or more of the email accounts accessed between May 23, 2019 to June 3, 2019 contained identifiable personal and/or protected health information," Beaumont Health said in a statement.[4] "Our investigation was unable to determine definitively if any information was actually acquired by the unauthorized third party, and Beaumont has no knowledge of any inappropriate or misuse of any data. Beaumont's electronic medical record system was not impacted by this incident and remains secure." The accessed email accounts included names, dates of birth, diagnosis and codes for diagnoses, procedures, treatment locations and types, prescription details, patient account numbers and medical record numbers. "A limited number of individuals' Social Security numbers, financial account information, health insurance information, and driver's license or state identification numbers were also contained in the impacted email accounts," Beaumont Health said. The hospital system asked patients to monitor insurance statements for any transactions related to care or services they did not receive. It also said it had taken steps to avoid future breaches, including implementing additional technical safeguards as well as providing training and education to staff members on handling potentially malicious emails.

◆ **A Michigan registered nurse (RN) said he was falsely accused of a HIPAA violation and fired after he raised safety concerns about his hospital's response to the COVID-19 pandemic.** Justin Howe, who worked at Hackley Hospital in Muskegon, Michigan, for Mercy Health, told local media outlets he had spoken out in late March

about his concerns. He said that hospital officials accused him of a HIPAA violation and fired him 10 days later. "They are false allegations," he told the local ABC affiliate station.[5] The Michigan Nurses Association (MNA) labor union took Howe's side in the dispute, saying Howe was terminated "shortly after doing multiple media interviews raising concerns about the hospital's preparedness and the safety of RNs and health care professionals … The Michigan Nurses Association believes that Howe's termination is a violation of federal labor law and has filed a charge with the National Labor Relations Board."[6] According to the affiliate station's report, Mercy Health said in a statement that Howe's allegation that he was terminated for raising safety concerns is "emphatically false" and added, "Mr. Howe was terminated from Mercy Health for violating the privacy of multiple patients over a period of days by entering into their electronic medical chart without a need to do so. It's notable that the patient records that Mr. Howe inappropriately accessed were all treated at a different hospital campus than where Mr. Howe works." Mercy Health said that Howe and the Michigan Nurses Association "are well aware of the facts that led to Mr. Howe's termination as an MNA representative was included in the investigation and termination process wherein Mr. Howe was confronted with the evidence of his own acts."

◆ **Walgreen Co. is facing a proposed class action in an Illinois federal court. Plaintiffs are seeking damages for an online data breach that exposed customers' personal information, including prescription drug details.**[7] The breach, which occurred in September 2019, included personally identifiable information and protected health information of thousands of Walgreens customers, including names, dates of birth, phone numbers, email addresses, and the classification of drugs consumers purchased (e.g., beta blockers, calcium channel blockers and antihypertensives), the lawsuit states. The data also included health-related suggestions referencing certain conditions or topics (e.g., asthma, migraines and blood pressure maintenance). According to the case, Walgreens noticed "abnormal activity" on a "limited number" of online customer accounts. Upon investigation, the company discovered that unauthorized third parties had used valid login credentials from other websites to gain access to customers' data stored on Walgreens' website.

◆ **Connecticut-based Hartford HealthCare said in April that its system was the victim of a phishing attack that may have compromised patient information for some 2,651 individuals.**[8] The company said it was made aware in February of concerning activity tied to two employee email accounts. An investigation by a technology forensics team found that someone gained access to the accounts between February 13 and 14. At least one of the accounts included personal patient information, including names, dates of birth, medical records, and other health and insurance information. In 23 cases, the information included a Social Security number. The breach did not affect the company's electronic medical records system. Hartford HealthCare said it is notifying the affected patients by mail. It said it would offer two years of free credit monitoring for the patients whose Social Security numbers were revealed in the breach.

◆ **In another phishing attack, hackers may have accessed or stolen personal information for patients at Aurora Medical Center Bay Area in Marinette, Wisconsin.**[9] Bad actors used an email phishing scheme around Jan. 1 to gain access to email accounts of several Marinette hospital employees. Hospital leaders learned of the breach on Jan. 9 and alerted authorities. They also started an internal investigation and changed credentials for the affected employee accounts. Although the hackers didn't break into the hospital's electronic medical records, they accessed email accounts that included names, marital statuses, dates of birth, addresses, email addresses, phone numbers, dates of admission, discharges or treatments, Social Security numbers, medical device numbers, passport numbers, bank account numbers and photographs. The hospital is encouraging patients to review financial accounts and report any suspicious activity, and said it has implemented software to help employees identify phishing emails.

◆ **Police and firefighters in Chicago are upset because the Cook County Public Health Department is refusing to share information about whether someone in a home has tested positive for COVID-19**, *The Washington Times*

reported. First responders in other states also are fighting for such coronavirus alerts, which would help first responders plan to take extra precautions or carry extra equipment, such as N95 masks. A HIPAA exception allows health departments to warn first responders when they are responding to a home containing someone who is positive for COVID-19.[10]

◆ **An Iowa congressman is arguing that HIPAA doesn't preclude certain health information from being disclosed publicly during the COVID-19 epidemic.** Rep. Steve King, R-Iowa, told local media representatives that he wants to see more detailed information on victims in the coronavirus pandemic, including exact ages of those who have died or who are in intensive care due to the virus.[11] He also would like disclosure by health care authorities of whether individuals had pre-existing conditions, and whether they are male or female. "There's so many details that would inform us so we could decide ourselves how careful we want to be when this society starts to open up," King said. "I think it's going to take more specificity than we're getting right now from the Iowa Department of Public Health."

1 Ambry Genetics, "Ambry Genetics Corp Notice of Data Breach to Consumers," Office of the Vermont Attorney General, April 17, 2020, https://bit.ly/2KK6bpE.
2 "Breach exposed info of 2K on Detroit health department website, city says," *The Detroit News*, April 24, 2020, https://bit.ly/2zFbzs2.
3 "Beaumont: Personal info of 112K potentially exposed in data breach," *The Detroit News*, April 17, 2020, https://bit.ly/2SexXis.
4 Beaumont Health, "Notice Regarding Data Security Incident," news release, April 17, 2020, https://bit.ly/2WtJbRc.
5 13 ON YOUR SIDE Staff, "Mercy Health says nurse was fired for violating privacy of multiple patients not for talking to the media," *13 ON YOUR SIDE*, April 23, 2020, https://bit.ly/3aL6xHj.
6 Michigan Nurses Association, "Hackley Nurse Fired After Speaking to Media," news release, April 21, 2020, https://bit.ly/2W0drnI.
7 Peter Hayes, "Walgreens Hit With Class Claims Over Online Data Breach (1)," Bloomberg Law, April 21, 2020, https://bit.ly/2yOvHYn.
8 "Hartford HealthCare Data Breach May Have Compromised Patient Information," *NBC Connecticut TV*, updated April 13, 2020, https://bit.ly/2WccbNc.
9 Jake Prinsen, "Hackers may have accessed personal information of Aurora Medical Center Bay Area patients," *Green Bay Press Gazette*, April 17, 2020, https://bit.ly/2yUcm7S.
10 Jeff Mordock, "'Doesn't make any sense': First responders denied basic coronavirus alert due to privacy laws," *The Washington Times*, April 27, 2020, https://bit.ly/2KI1VHk.
11 Coltrane Carlson, "Viewpoints Differ on Using HIPAA To Report COVID-19 Cases," Raccoon Valley Radio, April 26, 2020, https://bit.ly/2Sg0tAc.