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.

Purchase Login