COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 12. December 10, 2020 Privacy Briefs: December 2020

By Jane Anderson

◆ **Suspected North Korean hackers have tried to break into the systems of British drugmaker AstraZeneca in recent weeks as the company races to deploy its COVID-19 vaccine, *Reuters* reported.**[1] The hackers posed as recruiters on networking site LinkedIn and WhatsApp to approach AstraZeneca staff with fake job offers, *Reuters*' sources said. They then sent documents purporting to be job descriptions that were laced with malicious code. The hacking attempts targeted "a broad set of people," including staff working on COVID-19 research, according to one of *Reuters*' sources, but are not thought to have been successful. The tools and techniques used in the attacks indicated that they were part of an ongoing hacking campaign that U.S. officials and cybersecurity researchers have attributed to North Korea, according to the article. Cyberattacks against health entities, vaccine scientists and drugmakers have soared during the COVID-19 pandemic. Microsoft also said it has seen two North Korean hacking groups target vaccine developers in multiple countries, including by "sending messages with fabricated job descriptions."

◆ **Personal information of thousands of patients treated at Louisiana State University-operated centers around the state may have been compromised in a data breach, LSU Health New Orleans said.**[2] The breach stemmed from an intrusion into an employee's email account, which reportedly occurred on Sept. 15. Potentially compromised patient information included names, Social Security numbers, dates of birth, phone numbers, addresses and health insurance information. Seven LSU Health facilities were affected, the organization said. "When the intrusion was discovered, the LSU Health Care Services Division's Compliance and Privacy Department began the difficult and laborious process of identifying any patients whose information may have been compromised," LSU Health said in a statement. "While the exhaustive investigation has found thousands of patients, work continues to discover any others. Affected patients and the public are being notified." Although there's no indication that the intruder accessed or misused any patient information, anyone who received care at any of the affected facilities is being told to monitor their credit reports for any signs of potential identity theft.

◆ **Colorado nonprofit health care provider AspenPointe has notified more than 295,000 patients of a September cyberattack that removed personal information from AspenPointe's network.**[3] "We recently discovered unauthorized access to our network occurred between September 12, 2020 and approximately September 22, 2020," AspenPointe said in a letter to affected patients. "We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network. Based on our comprehensive investigation and document review, which concluded on November 10, 2020, we discovered that your full name and one or more of the following were removed from our network in connection with this incident: date of birth, Social Security number, Medicaid ID number, date of last visit (if any), admission date, discharge date, and/or diagnosis code." AspenPointe said it is not aware of any reports of identity fraud or improper use of patients' information as a direct result of the incident, but it is offering patients 12 months of credit and CyberScan monitoring, a $1 million insurance reimbursement policy, and identity theft recovery services.

◆ **A security threat at Hendrick Health System's main campus in Abilene, Texas, along with some Hendrick**

clinics, forced the shutdown of the health system's networks in mid-November.[4] "Our primary goal is to maintain patient safety while administering downtime procedures," the health system said in a statement. "Be confident that we have been working around the clock to assess and resolve the issue. Like many other healthcare organizations, network security threats are an unfortunate reality in our industry and we have coordinated with industry experts and law enforcement to address the issue to get our networks back up and running." Some outpatient services had to be rescheduled as a result of the security threat, the health system said.

◆ **The Delaware Division of Public Health said that it is mailing letters to individuals who were affected by a recent data breach incident.**[5] On Sept. 16, the Department of Health and Social Services discovered that a temporary staff member mistakenly sent two unencrypted emails in August to an unauthorized user. These emails contained COVID-19 test results for approximately 10,000 individuals tested in July and August. The emails were meant for internal distribution to call center staff who assist individuals in obtaining their test results. They contained test dates, test locations, patient names, patient dates of birth, phone numbers if provided, and test results. The unauthorized user who received the two unencrypted emails alerted the Division of Public Health and reported deleting the emails, along with the files attached to them. There's no evidence to suggest that there has been any attempt to misuse any of the information, the state agency said. As a result of the incident, Division of Public Health staff were retrained in HIPAA policies and procedures, and additional HIPAA training policies were put in place for temporary staff members. The temporary staff member responsible for the breach is no longer employed with the Division of Public Health, the agency said.

◆ **Unauthorized access to a hospital email account may have revealed the personal information of more than 60,000 Iowans, according to Mercy Iowa City.**[6] The hospital said that data for 60,473 patients may have been involved in the security breach. Mercy Iowa City discovered an issue with an employee's email account on June 24 after the hospital detected that the account was sending out spam and phishing emails. The account was compromised from May 15 until June 24, an investigation showed. In early October, a security firm that Mercy hired to conduct a more in-depth investigation confirmed that the account could have revealed sensitive customer data. According to the hospital, personal information contained in the account contained patient names, Social Security numbers, driver's license numbers, dates of birth, medical treatment information and health insurance information. Mercy Iowa City officials said they have not been made aware of any instances of identity theft related to the data breach. In cases where a Social Security number or driver's license number was potentially revealed, the hospital is providing a year of free identity theft protection.

◆ **The HHS Assistant Secretary for Preparedness and Response (ASPR) is warning that ransomware attacks in the health care sector are ongoing.**[7] "At this time, we consider the threat to be credible, ongoing, and persistent," ASPR said in a bulletin. "Of note, some recent healthcare sector victims have experienced very short periods of time between initial compromise and activation—even under a few hours." Federal agencies have described techniques to protect against malware such as Trickbot and BazarLoader, the ASPR bulletin said. "In general, maintaining anti-ransomware best practices like the 3-2-1 backup system or conducting regular vulnerability scanning to identify and address vulnerabilities will help protect your organization against future treats from other ransomware operators," the bulletin said. "Organizations should balance their operational needs with the current threat level and develop processes and postures for normal operating status and higher threat periods. The threat from ransomware is ongoing and entities should develop effective deterrent procedures while maintaining effective care delivery."

◆ **Luxottica of America, a global conglomerate that primarily makes and distributes eyewear but also operates a web-based appointment scheduling application**, reported a HIPAA data breach involving more than 829,000 patients.[8] Luxottica learned of the incident on Aug. 9 and concluded later that the attacker may have accessed and acquired patient information that included full names, contact information, appointment dates and times,

health insurance policy numbers, and doctors or appointment notes that may indicate information related to eye-care treatment, such as prescriptions, health conditions or procedures. Luxottica said it is not aware of any misuse of the information and urged patients to watch for any suspicious activity on their accounts. Patients whose Social Security numbers or payment information were involved will receive complimentary credit monitoring for one year.

1 Jack Stubbs, "Exclusive: Suspected North Korean Hackers Targeted COVID Vaccine Maker AstraZeneca – sources," *Reuters*, November 27, 2020, https://reut.rs/37rhRZA.
2 WBRZ staff, "Breach at LSU Health New Orleans may have exposed thousands of patients' information," WBRZ, November 20, 2020, https://bit.ly/3lwdbGS.
3 AspenPointe, "Important Information, Please Review Carefully," letter, November 19, 2020, https://bit.ly/39yUmQX.
4 Hendrick Health, "Hendrick Medical Center Network Security Threat," news release, November 10, 2020, https://bit.ly/3luxMen.
5 Delaware News, "Delaware Division of Public Health Announces Data Breach Incident," news release, November 15, 2020, https://bit.ly/2VvaHxE.
6 KCRG News staff, "Mercy Iowa City reports data breach, over 60,000 Iowans affected," KCRG, November 17, 2020, https://bit.ly/3mxRWpk.
7 ASPR, "Ransomware Activity Targeting the Healthcare and Public Health Sector (Update 2)," Healthcare and Public Health Sector Notification, November 2020, https://bit.ly/3lyQkKu.
8 Luxottica of America, "Important Information Regarding Security Incident," news release, November 2020, https://bit.ly/33BvF2h.