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.