COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 11. November 07, 2019 Privacy Briefs: November 2019

By Jane Anderson

◆ **The biggest threat to protected health information comes from carelessness within your organization, according to a brief from the Clearwater CyberIntelligence Institute.** The brief found that 59% of all security incidents and breaches – both malicious and inadvertent – stemmed from carelessness by trusted insiders, not from outside forces. The three top vulnerabilities created by so-called "careless users" include: endpoint data loss (data losses caused by the use of desktops, laptops, cellphones and other electronics); susceptibility to malware and phishing attacks caused by untrained and untested staff; and facilitating improper access to sensitive application and devices due to weak passwords. "Careless Users are certainly not a new phenomenon in health care," the report concludes, while noting that health care entities need to strengthen their security controls. Download the full report at https://bit.ly/31V8xbk.

◆ **The HHS Office for Civil Rights and the Office of the National Coordinator for Health Information Technology have released version 3.1 of the popular HHS Security Risk Assessment (SRA) Tool.** The tool is designed to aid small- and medium-sized health care organizations in their efforts to assess security risks and help reduce the chance of being impacted by malware, ransomware and other cyberattacks. The current version of the SRA Tool includes functionality updates based on public input. New features include: threat and vulnerability validation; improved asset and vendor management (multi-select and delete functions added); incorporation of National Institute of Standards and Technology Cybersecurity Framework references; capability to export the detailed report to Excel; addition of question flagging and a Flagged Report; bug fixes and improved stability. Download version 3.1 of the SRA Tool and view the answers to additional questions at https://bit.ly/32faqzK.

◆ **Officials at a St. Louis health center that serves needy, uninsured residents say a ransomware cyberattack caused a data breach that potentially affected 152,000 people.** The Betty Jean Kerr People's Health Center said Friday that the attack involved patient information, including addresses and Social Security numbers, but did not include patient medical records. Information on medical providers and health center employees also was breached, according to the health center. The incident locked data, but the center said it has refused to pay the ransom. The health center's CEO said there's no way to know if information was viewed or accessed. Read more at https://bit.ly/2BN29bx.

◆ **Protected information on some 130,000 patients might have been exposed following a summer phishing attack and data breach at Kalispell Regional Healthcare in Montana.** The health center said several of its employees were victims of what it called "a well-designed email" that tricked them into providing their hospital log-in credentials to hackers. Although the attack began last spring and summer, the hospital just learned a few weeks ago exactly which patients had been involved. The information exposed may have involved names, Social Security numbers, email addresses, medical history and health insurance information. See the story at https://bit.ly/2BQ3r5H.

◆ **Saco, Maine-based nonprofit mental health care provider Sweetser has notified 22,000 current and former clients that their sensitive personal and medical information may have been stolen by hackers in an email breach in June.** The organization provides a variety of mental health services to children and adults including individual and group therapy, psychiatry and substance abuse counseling services. Based on a forensic firm's findings, it

was determined that Sweetser employee email accounts were accessed from roughly June 18 through June 27. On Sept. 10, the investigation showed that data containing personal information, including names, addresses, dates of birth, telephone numbers, Social Security numbers, health insurance information and identification numbers, driver's license numbers, Medicare and Medicaid information, payment or claims information, diagnostic codes, and information regarding medical conditions and treatment could have been accessed. Notification letters have been sent to potentially impacted clients, according to Sweetser, which said it doesn't know whether the intent of the breach was to steal clients' personal information. Learn more at https://bit.ly/2MRuyne.

◆ **Researchers from the Mayo Clinic are warning that it's possible to identify patients from MRI scanning data, leading to a potential new privacy threat.** In a letter published in the *New England Journal of Medicine*, the researchers said they recruited 84 volunteers between the ages of 34 and 89, and photographed each participant's face from five slightly varying angles. Each participant had undergone an MRI of the head within the previous three months. The researchers then asked a computer to match the photos to the MRIs. For 70 of the 84 participants (83%) the software chose the correct MRI scan as the most likely match for their photos. When asked to choose the top five most likely matches, the computer was correct 95% of the time. In previous studies, 40% of human visual raters could match MRI face reconstructions to photographs with greater-than-chance success rates. "The current standard of removing only metadata in medical images may be insufficient to prevent reidentification of participants in research," the study concludes. "Further research is needed to develop improved deidentification methods for medical imaging that contains facial features." View the study at https://www.nejm.org/doi/full/10.1056/NEJMc1908881.

◆ **Ransomware attacks at three hospitals in Alabama forced the hospitals to divert to other facilities in the area before the health system reportedly paid the ransom.** The attacks on DCH Regional Medical Center in Tuscaloosa, Fayette Medical Center, and Northport Medical Center occurred early on Oct. 1. "Our hospitals have implemented our emergency procedures to ensure safe and efficient operations in the event technology dependent on computers is not available," DCH Health Systems wrote in a statement. "That said, we feel it is in the best interest of patient safety that DCH Regional Medical Center, Northport Medical Center and Fayette Medical Center are closed to all but the most critical new patients." The hospitals did not transfer patients during the incident. The *Tuscaloosa News* reported that the health system paid the hackers and obtained a key to unlock its files. See more details at https://bit.ly/2NmLst5.

◆ **Nearly 58,000 prescription records of customers at a Smith's Food and Drug store in Henderson, Nevada, were improperly thrown out in the trash, the company says.** The retailer said in a statement that an employee in late July discarded 12 boxes of pharmacy records in the store's trash compactor, which includes all waste, including food, from the store. The incident was discovered on Aug. 29, and the employee since has been terminated, according to Smith's. The discarded records were at least 11 years old and might have included a patient's first name, last name, gender, date of birth, home address, phone number, drug name, prescription number and third-party payer information. Smith's said it's unable to identify the patients involved. Read the story at https://bit.ly/2BQ12rH.

◆ **UAB Medicine in Birmingham, Ala., is notifying 19,557 affected patients that hackers recently gained access to certain employee email accounts containing patient information.** The hackers sent an email created to look like an authentic request from an executive asking employees to complete a business survey. Despite anti-phishing training, a number of employees accessed the survey and provided their username and password to the hackers. UAB Medicine discovered emails had been compromised in the phishing attack on Aug. 7. The investigation revealed the cybercriminals were attempting to divert employees' automatic payroll deposits to an account controlled by the hackers. There's no evidence the hackers were looking for, accessed or stole any protected health information, but UAB Medicine said that limited amounts of PHI including medical record numbers, birth dates, dates of service, location of service, diagnosis and treatment information, could have been viewed by the

hackers while they had access to the affected email accounts. Social Security numbers were included for a small subset of patients, who have been specifically notified. Learn more at https://bit.ly/3416IeC.

◆ **Indiana-based Goshen Health has begun notifying patients about a security incident that occurred more than a year ago after it went back and re-evaluated the incident and determined that a breach may have occurred.** According to the hospital, an unauthorized third party may have had access to the email accounts of two Goshen Health employees for 11 days in August 2018. After an investigation that stretched over a year, Goshen Health determined that the accounts contained personal information for some 9,160 patients. The information varied for each individual, but may have included names, addresses, dates of birth, physician names, health insurance information, limited clinical information, Social Security numbers and driver's license numbers. Goshen will provide complimentary identity theft protection services for those individuals whose Social Security numbers and driver's license numbers were involved. Get more information at https://bit.ly/36gq9lI.

◆ **Geisinger Health Plan has notified more than 5,000 members that some of their protected health information may have been affected by a breach at a business associate.** Magellan National Imaging Associates, a vendor hired by the health plan to manage radiology benefits, discovered in July that the email account of one of its employees had been sending out large volumes of spam email. The investigation revealed that several unauthorized mailbox authentications and connections originating from outside the United States had been occurring on this employee's email account since May. The vendor said the hackers likely obtained the email log-in credentials via a phishing attack or "other fraudulent means," Geisinger said. Geisinger was alerted to the issue in late September, and says it no longer uses Magellan as a vendor. Read Geisinger's statement at https://bit.ly/2q0ytoI.