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.