Report on Patient Privacy Volume 19, Number 12. December 04, 2019 Privacy Briefs: December 2019

By Jane Anderson

◆ **Health care data breaches will have cost the industry $4 billion by the end of 2019, and 2020 is likely to be worse, reports a new survey from Black Book Market Research LLC.**[1] The survey, which queried more than 2,875 security professionals from 733 provider organizations to identify gaps, vulnerabilities and deficiencies, found that virtually all information technology professionals agree that data attackers are outpacing medical enterprises. Health care providers continue to be the most targeted organizations, accounting for nearly four out of every five breaches, the survey found. More than 93% of health care organizations have experienced a data breach since the third quarter of 2016, and 57% have had more than five data breaches during that time frame. More than half of provider breaches were caused by external hacking, the survey found.

◆ **A private practice providing mental health services in Durham, North Carolina, says it became aware of potential unauthorized access to patient information when its practice employees were forced to evacuate their office due to a severe gas explosion next door.**[2] On April 10, the building adjacent to the office for Main Street Clinical Associates PA suffered a gas explosion. Main Street employees did not have the chance to properly store and secure patient information when they evacuated, the practice says. At the time of the evacuation, certain patient files in use were left open, and the file room containing patient records was unlocked, the practice said, adding, "Due to the nature and extent of the damage to the building, Main Street's employees were prohibited from reentering the building until September 9, 2019." Upon reentry, Main Street employees discovered that looters had unlawfully entered the office and stolen two laptop computers, a clinician's cell phone, and a printer that stored patient information. The computers and the cell phone and the client files stored on them were password protected. Main Street believes the unauthorized access to the building occurred sometime between July 15 and Sept. 9. "Although they cannot confirm whether any protected health information was actually accessed, viewed, or acquired without authorization, Main Street is providing this notification out of an abundance of caution, because such activity cannot be ruled out," the practice's notice said. Information that may have been compromised included patient names, driver's license numbers, Social Security numbers, health insurance information, and diagnosis and treatment information. The investigation into whether the devices have been accessed without authorization is ongoing.