COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 3. March 07, 2024 Privacy Briefs: March 2024

By Jane Anderson

◆ **Research from Guidepoint Security found that 2023 saw an 80% increase in ransomware activity year-over-year, driven in part by multiple mass exploitation campaigns impacting hundreds of organizations**. In total, the report said, 63 distinct ransomware groups were operating to leverage encryption, data exfiltration, data extortion and other tactics to compromise and publicly post 4,519 victims across 30 tracked industries in 120 countries. The top three most prolific established groups—LockBit, Alphv and Clop—continue to account for "not just the lion's share of victims but also much of the innovation and tactical changes across the ransomware ecosystem," the report said. The researchers said they expect ransomware impacts to "continue on an upward trajectory in 2024 based on established groups continuing to leverage high-severity and zero-day vulnerabilities as a reliable means of exploiting victims at scale."[1]

◆ **Data from HHS Office for Civil Rights (ORC) shows that the total number of reported health care breaches declined by 9% in 2023; however, the number of patient records exposed rose sharply to 116 million, a 108% year-over-year increase, according to an analysis from health care cybersecurity company Fortified Health Security**. Business associates (BAs) were responsible for an increasing share of breaches, according to the report: between 2013 and 2023, the number of BAs reporting a health care data breach increased by 143%. In addition, breaches directly involving BAs and breaches where BAs were present have increased by more than 217% over the past decade, the report said. Between 2022 and 2023, BA breaches increased by 22%, and breaches where BAs were present increased by 3%, the report said. "Connected technologies are now the primary locations where patient records are compromised," the researchers wrote. "For example, attacks on network servers (+1,272%), electronic medical records (+29%), and email (+457%) all rose sharply compared to 2013." OCR data from 2023 indicated that only 3% of breaches were located on electronic medical record (EMR) systems, "indicating that the majority originated from data stored on other network connected technologies waiting to be collected and exfiltrated," the report said. "Health care organizations hold vast amounts of patient data beyond their EMR systems, and much of it remains alarmingly unguarded."[2]