Report on Patient Privacy Volume 23, Number 10. October 05, 2023 Privacy Briefs: October 2023

By Jane Anderson

◆ **Kaiser Foundation Health Plan Inc. and Kaiser Foundation Hospitals will pay California $49 million to resolve allegations that they unlawfully disposed of hazardous waste, medical waste and protected health information at Kaiser facilities statewide.** California Attorney General Rob Bonta, in partnership with six district attorneys, announced the settlement, saying Kaiser will be required to take "significant steps" to prevent future unlawful disposals. The settlement results from undercover inspections of dumpsters from 16 different Kaiser facilities conducted by the district attorneys' offices. During those inspections, the district attorneys' offices reviewed the content of unsecured dumpsters destined for disposal at publicly accessible landfills and found hundreds of items of hazard and medical waste, along with more than 10,000 paper records containing the information of more than 7,700 patients. The California Department of Justice subsequently joined the district attorneys and expanded the investigation of Kaiser's disposal practices throughout the state. In response to the joint law enforcement investigation, Kaiser hired a third-party consultant and conducted more than 1,100 trash audits at its facilities in an effort to improve compliance, Bonta said. Kaiser also modified its operating procedures to improve its handling, storage and waste disposal.[1]

◆ **FBI and the Cybersecurity and Infrastructure Security Agency have released a joint cybersecurity advisory on Snatch ransomware, which provides organizations with signs of a compromise associated with Snatch ransomware.** Snatch recently attacked a hospital in Maine and also claimed responsibility for attacking the Florida Department of Veterans Affairs. According to the agencies, Snatch threat actors operate a ransomware-as-a-service model and change their tactics according to current cybercriminal trends and successes of other ransomware operations.[2]

◆ **The Department of Justice (DOJ) has charged nine Russian nationals who allegedly used Russian-based malware in cyberattacks on various U.S. entities, including a 2021 attack on Scripps Health that resulted in weeks' worth of computer downtime and breached information** for more than 150,000 patients. DOJ charged the nine Russians with using the malware tools Trickbot and Conti to infiltrate Americans' devices. The defendants are behind "one of the most prolific ransomware variants used in cyberattacks across the United States, including attacks on local police departments and emergency medical services," Attorney General Merrick Garland said in a statement. The nine men allegedly infected victims' computers with Trickbot malware designed to capture victims' personal data such as banking credentials as well as passwords and personal identification for things like credit cards and emails, according to an indictment unsealed in the Northern District of Ohio. The hackers then infected other computers and used the login credentials to steal funds from victims' bank accounts and then installed ransomware on the victims' computers, the indictment said. According to the indictment, the defendants sent phishing emails to companies with an embedded malicious link or attachment in the email. Several defendants face indictments for cybercrimes in Tennessee, California and Ohio.[3]