COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 7. July 13, 2023 Privacy Briefs: July 2023

By Jane Anderson

◆ **A former hospital worker in Arizona was sentenced to 54 months in prison and ordered to pay restitution after pleading guilty to two felony counts involving identity theft and health information disclosure.** In the plea deal, Rico Prunty acknowledged he accessed medical intake forms, copied protected health information and personal identifying information of more than 300 individuals, and forwarded the forms to co-conspirators in Indiana. The information was used to open financial accounts in the names of those individuals without their knowledge, authority or permission, the plea agreement states. Over the course of the scheme—which took place between July 2014 and May 2017—Prunty illegally accessed the individually identifiable health information of nearly 500 patients, resulting in a total loss of $132,521.98, according to the Department of Justice. Prunty originally faced nine felony counts, including one count of conspiracy to commit identity theft, seven counts of aggravated identity theft, and one count of HIPAA violation. Three co-conspirators previously were sentenced for their roles in the scheme to prison terms ranging from 121 months to 154 months.[1]

◆ **The federal Health Sector Cybersecurity Coordination Center (HC3) is urging health care organizations to prioritize defenses against the cybercriminal group FIN11, which often runs high-volume operations mainly targeting companies with CLoP ransomware.** "The group has targeted pharmaceutical companies and other health care targets during the COVID-19 pandemic and continues to target the health sector," HC3 said in a bulletin. "The group is behind multiple, high-profile, widespread intrusion campaigns leveraging zero-day vulnerabilities. It is likely that FIN11 has access to the networks of far more organizations than they are able to successfully monetize, and choose if exploitation is worth the effort based on the location of the victim, their geographic location, and their security posture." HC3 said it could not determine exactly how many and which CLoP ransomware attacks have been propagated by FIN11; however, it said it has observed around 30 incidents involving CLoP ransomware in the U.S. health care sector since 2021. FIN11 has been involved in exploiting the MOVEit Transfer secure managed file transfer software zero-day vulnerability, HC3 said. "HC3 recommends that healthcare organizations consider FIN11 a top priority for their security teams," the agency said.[2]

◆ **An Illinois hospital has closed its doors due in part to a cyberattack two years ago, making it the first hospital to publicly link criminal hackers to its closure.** St. Margaret's Health in Spring Valley, Ill., fell victim to a cyberattack in 2021, and it was unable to submit claims to insurers, Medicare or Medicaid for months. That led the rural hospital—which also had staffing shortages—into a financial spiral, said Suzanne Stahl, chair of the hospital's parent organization SMP Health. "Rural hospitals have been struggling throughout the nation and many have already closed," Stahl said in a Facebook post. "It has become impossible to sustain our ministry. This saddens us greatly." SMP Health officials said the organization's lender cut off access to funds in early June, leading to an abrupt decision to close the hospital.[3]

◆ **An employee of MetroHealth System in Cleveland has been "disciplined" for inappropriately accessing patient medical records for the last 15 years, the health system said.** MetroHealth found that the employee accessed records that included names, birth dates and clinical information. The hospital system did not say how many patients were affected; however, it said that the employee did not have access to financial information such as Social Security numbers or banking information. MetroHealth's breach notification to HHS Office for Civil Rights

said that the breach involved 1,748 patients. Discovery of the mishandling of records on April 27 led to an investigation, MetroHealth said. "To date, we have no evidence that any information has been misused as a result of this incident," the hospital system said. "Disciplinary action was immediately taken in accordance with the System's human resources policies." The hospital system, citing employee confidentiality, did not disclose whether the employee responsible for the breach was fired. MetroHealth said it has notified all patients whose records were affected by this latest incident and that it is taking additional steps to strengthen privacy processes, procedures and training across the system to prevent similar incidents from occurring.[4]

◆ **The California Department of Managed Health Care fined Kaiser Foundation Health Plan Inc., $450,000 for violating the confidentiality of thousands of the plan's enrollees following an incident where the plan sent 337,755 mailings containing protected health information to 167,095 potentially outdated enrollee addresses.** The mailings took place from October 2019 to December 2019, and Kaiser reported to the department that an error in updating its electronic health records system caused mailings with confidential information to potentially be sent to enrollees' former addresses. The plan reported that of the 337,755 mailings, 1,788 were returned unopened, and eight recipients contacted the plan to say that they had opened the mailing and that it was not intended for them. "Due to the plan's system error, thousands of mailings could have been viewed by unauthorized persons," the department said, noting that Kaiser knew of the electronics error and data breach on Nov. 11, 2019, but did not stop the mailings to former addresses until Dec. 20, 2019—39 days later. That allowed another 175,000 pieces of potentially misdirected correspondence to be mailed, the department said. "Kaiser's error in updating the plan's electronic health records system caused the unauthorized mailings and [protected health information] data breach," the department said in announcing the enforcement action. "The plan has agreed to pay the fine and implement corrective actions, including running periodic checks of its software systems to ensure enrollee addresses are correct and up to date."[5]

◆ **In another mailing error, the Utah Department of Health and Human Services will be sending a personalized notification to 5,800 Medicaid recipients after benefit information may have been sent to the wrong addresses due to a system coding error.** State Mail and Distribution Services discovered on May 8 that some letters were stuffed in envelopes addressed to incorrect households, according to a spokesperson for the department. After an investigation, the department determined that 5,800 out of 530,000 Medicaid recipients statewide might have been affected. Letters for some of those impacted might have included their Social Security numbers, and other information, such as names, addresses, and dates of birth, also were included. Those affected will receive a notification detailing the issues, information about any personal data included in the letter, actions they can take to secure their accounts and contact information for other questions and concerns, the department said.[6]

1 U.S. Department of Justice, U.S. Attorney's Office for the Northern District of Indiana, "Arizona Man Sentenced to 54 Months in Prison," news release, May 31, 2023, https://bit.ly/3JSuTmW.
2 Health Sector Cybersecurity Coordination Center, "HC3 Threat Actor Profile," Report: 202306131500, bulletin, June 13, 2023, https://bit.ly/44BH0wr.
3 Tim Shelley, "St. Margaret's CEO blames their bank for accelerating decision to close Spring Valley hospital," *WCBU*, June 12, 2023, https://bit.ly/3NMrVkN.
4 Julie Washington, "MetroHealth employee disciplined for patient data breaches since 2008; no evidence information was misused," *Cleveland.com*, June 26, 2023, https://bit.ly/44EoTWy.
5 California Department of Managed Health Care, "DMHC Fines Kaiser Permanente $450,000 for Violating Enrollee Confidentiality," news release, June 15, 2023, https://bit.ly/44hMAo5.
6 Jenny Carpenter, "Medicaid letters sent to wrong addresses; Utah health department reports data breach," *KSL*, June 6, 2023, https://bit.ly/449Q1wZ.