COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 8. August 11, 2022 Privacy Briefs: August 2022

By Jane Anderson

◆ **The Department of Justice (DOJ) seized around $500,000 in Bitcoin ransom paid by two health care organizations in Kansas and Colorado to North Korean ransomware actors and their conspirators.**[1] The seizure of the two ransoms resulted from "rapid reporting and cooperation from a victim" and disrupted activities of a North Korean state-sponsored group known as "Maui," Deputy Attorney General Lisa Monaco told attendees July 19 at the International Conference on Cyber Security. The reporting also allowed investigators to identify a previously unknown strain of ransomware, Monaco said. According to court documents, hackers used Maui in May 2021 to encrypt the files and servers of a Kansas medical center. After more than a week of being unable to access encrypted servers, the Kansas hospital paid approximately $100,000 in Bitcoin to regain the use of their computers and equipment. Because the medical center notified the FBI and cooperated with law enforcement, the FBI was able to identify the ransomware and trace the cryptocurrency to China-based money launderers, the DOJ said. Then, in April 2022, the FBI observed an approximately $120,000 Bitcoin payment move into one of the identified cryptocurrency accounts. The investigation confirmed that a medical provider in Colorado had just paid a ransom after being hacked by actors using the same Maui ransomware strain. In May, the FBI seized the contents of two cryptocurrency accounts that had received funds from the Kansas and Colorado health care providers and began proceedings to return the funds to the victims.

◆ **A sweeping bipartisan federal privacy bill that already has been approved by a key House subcommittee is facing headwinds in the form of massive corporate lobbying aimed at derailing it.**[2] The American Data Privacy and Protection Act, which would restrict the types of data companies can collect from online users and how they can use that data, is the result of years of negotiations between Democratic and Republican lawmakers. Its provisions would impact companies in every consumer-centric industry that compiles massive amounts of user data and relies on targeted ads to attract customers. It would tremendously impact entities that currently collect, process and transmit health information but are not subject to HIPAA. The proposed legislation would override most state privacy laws, as Republicans have sought, in exchange for granting consumers a right to bring lawsuits against violators, which Democrats have called for.[3] However, several key senators have expressed concerns about the legislation's provisions. Some California-based representatives have said they will not support the bill if it overrides California's extensive privacy protections. In addition, the proposal has become one of the most lobbied bills in Congress, drawing attention from more than 180 corporate clients, including Amazon, the Walt Disney Corporation and Target, according to data from research group OpenSecrets.

◆ **A Colorado woman pleaded guilty to five felony counts of theft of medical records and was sentenced to 30 days in jail plus a $5,000 fine—the maximum under the plea agreement—after being accused of stealing a doctor's password** and accessing records hundreds of times.[4] Nicole Grant was initially charged with 65 felonies and one misdemeanor for accessing medical records. According to a news report, Grant used medical records to locate and then send inflammatory messages to one victim, resulting in a felony charge for stalking, which was dropped as part of the plea agreement. A total of 16 patients had their medical records illegally accessed by Grant, who will appear in court on Sept. 20 for a restitution hearing.

◆ **The number of health care breaches in the first half of 2022 impacting 500 or more records reported to the HHS**

Office for Civil Rights (OCR) fell by about 9% when compared to 2021, according to Fortified Health Security's 2022 midyear report on health care cybersecurity.[5] A total of 337 breaches were reported to OCR in the first half of 2022, compared to 368 breaches in 2021, the report said. Health care providers account for the most breaches —72%—as they did in the last report. Business associates accounted for 16% of breaches, rising when compared to the previous year, and health plans accounted for 12%, less than last year, the report said. Malicious attacks ranked as the No. 1 cause of breaches for a sixth consecutive year, with the percentage of incidents pegged to hacking/IT incidents rising from 73% to 80% so far in 2022, the report said. Unauthorized access/disclosure accounted for 15% of incidents, with 5% attributed to loss, theft and improper disposal of records or technology.

◆ **Microsoft is warning of a large-scale phishing campaign that targets Office 365 credentials and attempts to bypass multi-factor authentication.**[6] Based on the tech giant's threat data, the so-called "adversary-in-the-middle" (AiTM) tactic has attempted to phish more than 10,000 organizations since September 2021. In AiTM phishing, attackers deploy a proxy server that impersonates the website the target user intends to visit. Such a setup allows the attacker to steal the target's password and the session cookie that proves their authentication with the website. The attacker then can use the password and the session cookie to enter the site. "Using Microsoft 365 Defender threat data, we detected multiple iterations of an AiTM phishing campaign that attempted to target more than 10,000 organizations since September 2021," Microsoft said. "These runs appear to be linked together and target Office 365 users by spoofing the Office online authentication page." In one of the phishing runs Microsoft's security team observed, the attacker sent emails with an HTML file attachment to multiple recipients in different organizations. The email informed the target recipients that they had a voice message. When a recipient opened the attached HTML file, it was downloaded in the user's browser and displayed a page informing the user that the voice message was being downloaded. However, the download progress bar was fake, and no file was being downloaded. Then, the page redirected the user to an impersonation site that asked them to sign in. Microsoft noted that organizations could guard against phishing by enabling conditional access policies, investing in advanced anti-phishing solutions, and continuously monitoring for suspicious or anomalous activities.

◆ **Facebook parent company Meta is facing a second-class action lawsuit following disclosure that a tracking tool installed on hospitals' websites allegedly collects patients' protected health information**—including details about their medical conditions, prescriptions and doctor's appointments—and sending it to Facebook.[7] The first class-action lawsuit was filed on June 17 in U.S. District Court for the Northern District of California and argued that Facebook knew—or should have known—that its Meta Pixel tracking tool was being misused on hospital websites. In the latest lawsuit, Meta, the University of California San Francisco (UCSF) Medical Center, and Dignity Health Medical Foundation are targeted.[8] The class-action lawsuit, filed by "Jane Doe" in the same U.S. District Court, contends Doe began receiving emails and seeing targeted ads on Facebook related to her medical conditions after she had scheduled appointments and contacted doctors using UCSF's and Dignity's patient portals. Meta Pixel is a snippet of JavaScript code that tracks individuals' activity on a website and sends it to Facebook. According to the new class-action lawsuit, "when Plaintiff Doe logged into Healthcare Defendants' patient portal, there was no indication that Meta Pixel was embedded or that it would collect her sensitive medical information." The lawsuit also argues that Meta is violating its own policies on sensitive health information.

1 U.S. Department of Justice, "Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators," news release, July 19, 2022, https://bit.ly/3vFhB5Q.
2 Karl Evers-Hillstrom and Rebecca Klar, "Corporate lobbying could imperil sweeping data privacy bill," *The Hill*, August 3, 2022, https://bit.ly/3JxsIUh.
3 Cristiano Lima, "House panel advances major privacy bill, striking a long-awaited grand bargain," *Washington*

Post, July 20, 2022, https://wapo.st/3zw4O72.
4 Michael Logerwell, "Mesa County Women Violated HIPAA Protections, Charged with 5 Felonies," KREX, July 18, 2022, https://bit.ly/3zzRqyU.
5 Dan Dodson, "2022 Mid-Year Horizon Report: The State of Cybersecurity in Healthcare," Fortified Health Security, July 2022, https://bit.ly/3d0IACx.
6 Microsoft 365 Defender Research Team, "From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud," Microsoft Threat Intelligence Center, July 12, 2022, https://bit.ly/3PZk7fJ.
7 Jane Anderson, "In the Wake of Meta Pixel Allegations, CEs, BAs May Be at Risk Under HIPAA, Experts Say," *Report on Patient Privacy* 22, no. 7, July 7, 2022, https://bit.ly/3vFOZti.
8 Sophie Putka, "Meta, Hospitals Sued for Sharing Private Medical Info," MedPage Today, August 3, 2022, https://bit.ly/30WuiWe.