COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 5. May 11, 2023 Privacy Briefs: May 2023

By Jane Anderson

◆ **Five former Memphis-based hospital employees and another man have pled guilty to unlawfully disclosing patient information in violation of HIPAA, U.S. Attorney for the Western District of Tennessee Kevin Ritz announced.** According to the case, Roderick Harvey, 41, paid five employees of Methodist Hospital to provide him with names and phone numbers of Methodist patients who had been involved in motor vehicle accidents. After obtaining the information, Harvey sold the information to third parties, including personal injury attorneys and chiropractors, the U.S. Attorney's office said. Harvey pled guilty on April 21 to conspiring to violate HIPAA and faces a maximum penalty of five years imprisonment, a fine of $250,000 and three years of supervised release. Sentencing is set for Aug. 1. The five hospital workers—Kirby Dandridge, 38, Sylvia Taylor, 43, Kara Thompson, 31, Melanie Russell, 41, and Adrianna Taber, 26—pled guilty to disclosing the information to Harvey in violation of HIPAA; each faces a maximum penalty of one-year imprisonment, a $50,000 fine and one year of supervised release. They will be sentenced separately later this year.[1]

◆ **Washington State has become the nation's first to codify into law broad protections for consumer health data into law.** Washington Gov. Jay Inslee (D) signed the My Health, My Data Act on April 26. The law, which takes effect in 2024, requires companies to get consent from consumers to collect, share or sell health data, which is defined broadly as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." It prohibits advertising companies from using geofence technology in particular locations, such as health care facilities, to collect and sell data. It also provides for a private right of action that enables consumers to sue companies without explicit consent to use their data. The state's attorney general can take civil action on behalf of consumers under the act. The act also seeks to fill gaps left by HIPAA since HIPAA only pertains to health data collected by health care providers. Washington Attorney General Bob Ferguson and three state lawmakers introduced the My Health, My Data bill last October in response to the Supreme Court's ruling earlier in 2022 in the abortion case *Dobbs v. Jackson Women's Health Organization* overturning *Roe v. Wade*. Ferguson cited concerns about apps used to track menstrual cycles, which can sell sensitive information to law enforcement agencies in other states where seeking abortion care is illegal or limited. Lawmakers in several other states—including Illinois, Massachusetts, New York and Nevada—are considering their own versions of new legislation that would expand health data protections beyond HIPAA.[2]

◆ **A New York City law firm will pay $200,000 in penalties to New York State to settle a case after hackers were able to break into the law firm's systems and access the private information of approximately 114,000 patients.** The law firm, Heidell, Pittoni, Murphy & Bach LLP (HPMB), represents New York City-area hospitals and maintains sensitive private information from patients, including dates of birth, Social Security numbers, health insurance information, medical history and health treatment information. "HPMB's data security failures violated not only state law, but also HIPAA, which required HPMB to adhere to certain advanced data security practices," the attorney general's office said. In November 2021, an attacker exploited a vulnerability in HPMB's Microsoft Exchange email server to gain access to HPMB's systems. Patches for the vulnerability had been released by Microsoft several months earlier, the state attorney general's office said, but HPMB had not applied these patches in a timely manner. In December 2021, the attacker deployed malware on HPMB's systems, which

resulted in a disruption of HPMB's email system. In its subsequent investigation, HPMB found that tens of thousands of files potentially had been taken from the law firm's systems. An analysis of these files determined that electronic health information and private information likely had been exposed. In its investigation, the state attorney general's office determined that HPMB had failed to adopt several measures as required by HIPAA, including conducting regular risk assessments of its systems, encrypting the private information on its servers and adopting appropriate data minimization practices. As a result of the agreement with the state, HPMB must pay $200,000 in penalties to the state and strengthen its cybersecurity measures to protect consumers' personal and private health information.[3]

◆ **Postal Prescription Services, a subsidiary of supermarket giant Kroger, has notified some 82,000 Kroger customers that a data breach resulted in improper sharing of patient names and email addresses with its affiliated grocery business.** Postal Prescription Services, also known as Healthy Options Inc., said the names and email addresses were used to create a Kroger grocery account for affected individuals. Information disclosed was limited to the patient's first name, last name and email address for patients who created an online account with the mail-order prescription service from July 2014 through Jan. 13, 2023, when the issue was corrected. No financial information or clinical information was disclosed, according to Kroger. Upon learning of the incident, Postal Prescription Services updated its website to address the problem, the company said. In addition, Kroger is reviewing its procedures to evaluate changes to reduce the likelihood of this type of incident occurring in the future. The company stressed that the incident was not caused by or related to a security incident.[4]

◆ **A new survey of more than 400 health care workers revealed that while more than three-quarters of workers agreed that keeping data safe is their responsibility, it appeared they are not consistently implementing cybersecurity best practices.** In addition, the survey—from Salesforce—found that 57% of health care workers reported that their job has become more digitized in the last two years, indicating that an even larger amount of data needs protection. A total of 22% of survey respondents said that security protocols are not strictly enforced in their organizations. In addition, 31% said they don't know what to do in the event of a breach. Around two-thirds of health care workers said their work culture is "security first," but fewer than 31% said they are "very familiar" with company security processes and protocols. In addition, 43% said they personally don't have to worry about security at work, according to the survey. Some 70% said they have the training to keep data secure, but only 54% said that security training was efficient, and almost one in five said their security training was not relevant to their jobs. The research also showed that health care workers are blending personal and corporate devices: only 40% consider their connected devices a security risk, while 61% assume that if they can access something on their work device, it must be safe. Finally, 33% use the same passwords for personal and work-related logins.[5]

◆ **More than 90% of companies responding to Sophos' annual survey on the state of cybersecurity reported being targeted by a cyberattack in 2022, so companies should assume they will be targeted again in 2023, Sophos said.** "Operationalizing threat detection and response is difficult for most organizations, with 93% finding the execution of essential security operations tasks challenging," the survey concluded. Sophos found that investigating security alerts is a widespread issue: only 48% of all alerts are investigated to determine whether they are signs of malicious activity; most organizations struggle to identify and prioritize which alerts and events to investigate. In addition, the survey found that defenders lack confidence in their processes, with security tool misconfiguration identified as the top perceived security risk in 2023. More than half of IT professionals said that cyberthreats are now too advanced for their organizations to deal with on their own, and that number rises to 64% for IT professionals in small businesses, Sophos found. The independent survey queried 3,000 leaders responsible for IT and cybersecurity in 14 countries across all industries.[6]

1 U.S. Department of Justice, U.S. Attorney's Office for the Western District of Tennessee, "Former Methodist Hospital Employees Plead Guilty to HIPAA Violations," news release, April 25, 2023, https://bit.ly/30Ucaj4.
2 Keely Quinlan, "Washington passes nation's first health-data privacy law," *StateScoop*, April 27, 2023, https://bit.ly/3LjoalN.
3 New York State Attorney General's office, "Attorney General James Secures $200,000 from Law Firm for Failing to Protect New Yorkers' Personal Data," news release, March 27, 2023, https://on.ny.gov/3Hqufvr.
4 The Kroger Co., "Postal Prescription Service Reports Incident Involving Prescription Mail Order Accounts," news release, Cision PR Newswire, March 10, 2023, https://prn.to/3VgpV7X.
5 Salesforce, "Healthcare Workers Agree Data Security Is Their Responsibility, But Survey Shows Massive Gaps in Practice," news release, April 13, 2023, https://sforce.co/3Hra28Y.
6 Sophos, "The State of Cybersecurity 2023: The Business Impact of Adversaries," white paper, accessed May 8, 2023, https://bit.ly/3ViiZXI.