COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 2. February 08, 2024 Privacy Briefs: February 2024

By Jane Anderson

◆ **The American Hospital Association (AHA) has warned that information technology (IT) help desks are being targeted in a social engineering scheme that uses the stolen identity of revenue cycle employees or employees in other sensitive financial roles**. According to the AHA, the scheme is presumably a foreign-based threat actor calling IT help desks and leveraging stolen personally identifiable information of employees to answer security questions posted by the IT help desk. The threat actor then requests a password reset and requests to enroll a new device, such as a cell phone, to receive multi-factor authentication (MFA) codes, the AHA said, noting that the new device often will have a local area code. "This effectively defeats multi-factor authentication, including SMS text and higher level 'phishing-resistant' MFA, to provide full access to the compromised employee's email account and other applications," the AHA said. "The threat actor has reportedly used the compromised employee's email account to change payment instructions with payment processors and divert legitimate payments to fraudulent U.S. bank accounts. As with other payment diversion schemes, it is believed the funds are ultimately transferred overseas." The risk of this "innovative and sophisticated scheme" can be mitigated by ensuring strict IT help desk protocols, which at a minimum should require a call back to the number on record for the employee requesting password resets and enrollment of new devices, said John Riggi, AHA's national advisor for cybersecurity and risk. "Organizations may also want to contact the supervisor on record of the employee making such a request. As a result of becoming a victim of this scheme, one large health system now requires employees making such requests to appear in person at the IT help desk," Riggi said, adding that any organization that falls victim to a payment diversion scheme should notify their financial institution and the FBI.[1]

◆ **The National Institute of Standards and Technology (NIST) said it will update its Privacy Framework to Version 1.1 in 2024**. This "modest update" will support realignment with the NIST Cybersecurity Framework (CSF) 2.0 update. "The initial version [of the NIST Privacy Framework] was modeled upon the CSF so that the two frameworks could be used together more easily," NIST said in a blog post. "We want to maintain the connection by making appropriate adjustments based on CSF 2.0 changes. In addition, stakeholders have had a few years to use the Privacy Framework and have identified areas where targeted improvements can be made." In addition, NIST said it would leverage the privacy framework 1.1 update to develop a joint profile for data governance: "In talking with shareholders, we realized that data governance is the starting point for many organizations seeking to glean the benefits of data processing while managing privacy, cybersecurity, AI [artificial intelligence], and IoT [Internet of Things] risks." The profile could take many forms, such as a flow chart or a crosswalk among various NIST framework subcategories, NIST said. The agency said it anticipates releasing cybersecurity framework 1.1 concept papers in the first quarter of 2024 and releasing initial public drafts in the third quarter.[2]

◆ **Average ransom payments across all industries fell by one-third in the fourth quarter of 2023 to $568,705, whereas the median ransom payment stabilized and remained at $200,000 (no change from the third quarter of 2023), according to the ransomware response firm Coveware**. "The trend aligned with a relative decline in the size of victims impacted, and a reappearance of small game actors groups who reclaimed some market share after previously dropping in frequency during the third quarter," the company said in its latest quarterly report. Meanwhile, the proportion of ransomware victims that opted to pay ransoms in the fourth quarter fell to a record

low 29%. This is a result of two trends, the company said: 1) companies impacted by ransomware increasingly can recover partially or fully without the use of a decryption tool, and 2) reluctance to pay for "intangible promises from cybercriminals, such as the promise not to publish/misuse stolen data and the promise to exempt the company from future attacks or harassment." Coveware noted that companies keep getting "smarter on what can and cannot be reasonably obtained with a ransom payment. This has led to better guidance to victims and fewer payments for intangible assurances."[3]

◆ **New Jersey has become the 14th state to enact a comprehensive state privacy law. Gov. Phil Murphy, D-N.J., signed legislation on Jan. 16 that will require notification to consumers of collection and disclosure of personal data by certain entities, including internet websites.**[4] The law, which will take effect in January, requires a website operator that collects a consumer's information through its site for the purpose of selling that consumer's information to post a link clearly and conspicuously on its site or in another prominently accessible location, that allows the consumer to opt out of the collection of the personal data. The law also entitles the consumer to know what data the operator holds so they can correct or delete incorrect information. According to law firm Hunton Andrews Kurth, the law contains a narrow data-level (and not entity-level HIPAA exemption, exempting protected health information collected by a HIPAA-covered entity or business associate).[5]

◆ **Texas-based HMG Healthcare—which provides memory care, rehabilitation, and assisted living services—has confirmed that hackers accessed unencrypted personal data of residents and employees during a breach that occurred in August 2023**; however, the company does not know exactly what information was accessed. "The incident involved hackers gaining access to our server and stealing unencrypted files," HMG Healthcare said in a statement, adding that it first became aware of the incident in November 2023. "Files on the server likely contained medical records and personal information, including names, dates of birth, contact information, general health information, information regarding medical treatment, Social Security numbers and/or employment records." HMG Healthcare said it "quickly identified this breach and took steps to investigate the incident fully," and that it "worked diligently to ensure that the stolen files were not further shared by the hackers to other sources." The company also said, "HMG attempted to identify the specific data that was compromised but we have now determined that such identification is not feasible." On Dec. 29, HMG notified OCR of a breach that impacted 80,000 people.[6]

◆ **The United Network for Organ Transplantation, a nonprofit based in Richmond, Va., that oversees organ transplants throughout the U.S., said a "software configuration error" resulted in a data breach that impacted around 1.5 million records.** The affected data includes Social Security numbers, dates of birth and medical procedure information, the organization said. It did not include identifiers such as names and addresses, and the breach did not affect the matching or allocation of organs to patients.[7]

◆ **North Carolina-based Novant Health—which was the first health care provider system to disclose a breach involving the web tracking devices known as pixels**[8]**—has settled class- action litigation over the breach for $6.6 million**. Novant said it installed the pixel on its website in May 2020 amid the COVID-19 pandemic. At the time, the company had launched a promotional campaign to connect more patients to the Novant Health MyChart patient portal, with the goal of improving access to care through virtual visits and providing increased accessibility. The campaign involved Facebook ads and a Meta tracking pixel intended to help Novant Health understand the success of efforts on Facebook, the health system said in its August 2022 breach notification. At that time, Novant notified 1.3 million individuals that their protected health information might have been disclosed without authorization due to Novant's use of advertising and tracking pixels associated with Meta, the parent company of Facebook. In Novant's case, tracking pixels may have scooped up data from patients' electronic medical records, possibly reporting names and appointment details back to Meta. Information that

may have been shared inappropriately included email addresses, phone numbers, computer internet provider addresses, contact information entered into emergency contacts or advanced care planning and data such as appointment type and date and the physician selected. Ten Novant Health patients filed the lawsuit, and Novant patients who used the health system's patient portal or website between May 1, 2020, and Aug. 12, 2022, may be eligible class members.[9]

1 American Hospital Association, "Hospital IT help desks targeted by sophisticated social engineering schemes," blog post, January 12, 2024, https://bit.ly/3ubmRB2.
2 Dylan Gilbert "New Year, New Initiatives for the NIST Privacy Framework!" National Institute of Standards and Technology blog post, January 25, 2024, https://bit.ly/3w59TFz.
3 Coveware, "New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying," quarterly report, January 26, 2024, https://bit.ly/49ejXdw.
4 State of New Jersey Governor Phil Murphy, "Governor Murphy Signs Legislation Protecting Consumer Data," news release, January 16, 2024, https://bit.ly/3SJAGQu.
5 Hunton Andrews Kurth, "New Jersey Becomes 14th State to Enact a Comprehensive State Privacy Law," blog post, January 19, 2024, https://bit.ly/3SuqfPd.
6 HMG Healthcare, LLC, "Privacy Update: Notice of Data Breach," January 2024, https://bit.ly/3HLEhqU.
7 Eric Kolenich, "Organ transplant data breach grows to 1.5 million records,"*Richmond Times-Dispatch*, January 23, 2024, https://bit.ly/3w5k10P.
8 Jane Anderson, "Meta Pixel Woes Mount: Novant Discloses Breach Involving Tracker; Three Suits Filed," *Report on Patient Privacy* 22, no. 9, September 2022, https://bit.ly/493MDpJ.
9 Pritchard Strong, "NC hospital system settles patients' Meta Pixel lawsuit for $6.6 million," WRAL News, January 10, 2024, https://bit.ly/3SM3h7P.