COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 7. July 11, 2024
Privacy Briefs: July 2024

By Jane Anderson

◆ **Pennsylvania-based Geisinger Health System said it experienced a breach impacting more than 1.27 million patients when a former employee of vendor Nuance Communications Inc., a Microsoft Corp. subsidiary, accessed patient information two days after he was terminated.**[1] The breach was discovered on Nov. 29, but law enforcement asked Nuance to delay notifying patients, Geisinger said. The former Nuance employee was arrested and is facing federal charges. "Through its investigation, Nuance determined that the former employee may have accessed and taken information pertaining to more than one million Geisinger patients," the health system said. "The information varied by patient but could have included names in combination with one or more of the following: date of birth, address, admit and discharge or transfer code, medical record number, race, gender, phone number, and facility name abbreviation. No claims or insurance information, credit card or bank account numbers, other financial information, or Social Security numbers were inappropriately accessed by the company's former employee."

◆ **An emergency room physician who illegally obtained the personal health information of two individuals and shared a sensitive photo involving one of them pleaded guilty to one count of violating HIPAA in federal court in Cedar Rapids, Iowa**. Gabriel Alejandro Hernandez Roman, M.D., admitted to using his access as a resident in hospitals in Cedar Rapids and Iowa City to access medical records under false pretenses. "Dr. Hernandez Roman also admitted that, in January 2022, he sent a photograph of one of Hospital-1's patients to another individual via SnapChat," the U.S. Attorney's Office for the Northern District of Iowa said. "The photograph showed the patient in a hospital setting, wearing a gown, with the patient's rectum clearly hanging out of the body. Dr. Hernandez Roman had no legitimate medical purpose for taking this photograph or, further, for sending it via SnapChat to the individual." Hernandez Roman also admitted that he mailed a letter in June 2023 to the Iowa Board of Medicine in which he admitted to accessing confidential medical records and sharing the photograph. In his plea agreement, Hernandez Roman admitted he falsely wrote in that letter that he had sent the photograph of the prolapsed rectum to his mother to remind her of the importance of fiber intake. Hernandez Roman faces up to five years in prison and up to $250,000 in fines.[2]

◆ **Following a dip in 2022, ransomware incidents again rose in 2023, according to the FBI's Internet Crime Complaint Center (IC3) annual report**. There were more than 2,825 complaints to IC3 about ransomware in 2023, representing an increase of 18% from 2022. Reported losses rose 74%, from $34.3 million to $59.6 million, the report found. The health care and public health sector experienced the most ransomware attacks of any sector, the IC3 report said, with 249 reported incidents in 2023. The critical manufacturing sector was second, with 218 reports of ransomware attacks, and government facilities were in third place, with 156 reported attacks. "Cybercriminals continue to adjust their tactics, and the FBI has observed emerging ransomware trends, such as the deployment of multiple ransomware variants against the same victim and the use of data-destruction tactics to increase pressure on victims to negotiate," the IC3 report said.[3]

◆ **Network intrusions accounted for 51% of all security incidents across industries in 2023, according to an analysis by law firm BakerHostetler**. Business email compromise caused 23% of incidents, while inadvertent disclosure accounted for 11% and intentional access/disclosure accounted for 5%, the report said. When

BakerHostetler looked at root causes of security incidents, it found that unpatched vulnerabilities caused 23% of incidents, phishing caused 20%, misconfiguration caused 6%, brute force/credential stuffing caused 3%, social engineering caused 3%, human error/unintended recipient caused 3%, employee abuse of access privileges caused 2%, and open remote desktop protocol caused 1%. Tactics like device theft and skimmers caused 17% of incidents, and the root cause was unknown in 22% of incidents, BakerHostetler said. Data theft/exfiltration occurred in 48% of incidents, while ransomware deployment occurred in 31%, the report said. The health care industry accounted for more than one-fourth of all incidents in 2023, taking the top spot of affected industries.[4]

◆ **Hospitals may not be presenting patients and other website users with adequate information about their use of web-tracking technologies on their public-facing websites, a study in *JAMA* found**. The study, from researchers based at the University of Pennsylvania, looked at what the researchers called a nationally representative sample of 100 non-federal acute care hospitals, collecting data from November 2023 to January 2024. The research found that 96% of hospital websites transmitted user information to third parties, but only 71% of websites included a publicly accessible privacy policy. Of those 71 privacy policies, 40 (56.3%) disclosed specific third-party companies or services receiving user information, 69 (97.2%) addressed types of user information automatically collected by the website, 70 (98.6%) addressed how collected information would be used, and 66 (93%) addressed categories of third-party recipients. Named third parties tended to be familiar to users, such as Google. "Policies averaged more than 2500 words in length and were written at a college reading-level," the study said. "Given estimates that more than one-half of adults in the US lack literacy proficiency and that the average patient in the US reads at a grade 8 level, the length and complexity of privacy policies likely pose substantial barriers to users' ability to read and understand them." In addition, the study said, the lack of detail regarding third-party data recipients may lead users to assume they are being tracked only by a small number of companies that they know well when, in fact, hospital websites included in the study transferred user data to a median of nine domains. "Prior research has also shown that a wide range of companies commonly operate trackers on hospital websites, including data brokers and advertising companies with little or no consumer-facing presences," the researchers wrote. Hospitals generally are not required by law to have a website privacy policy disclosing their website trackers, but the Federal Trade Commission has said that entities that publish privacy policies must ensure those policies reflect their actual practices, the study's authors said.[5]

◆ **Winter Haven Hospital in Florida said it experienced a data breach affecting 2,101 patients when an employee emailing forms to a patient accidentally attached a cardiac rehabilitation department file containing information about other patients**. "The employee identified the error and contacted the recipient. The recipient stated the file would be deleted," the hospital said. Protected health information that was disclosed included: cardiac rehabilitation patient names, dates of birth, the procedure requiring cardiac rehab, date of service, and, in some cases, email addresses and/or phone numbers. "We have taken corrective actions to help prevent a re-occurrence of this type of incident, which included adding additional access security to the file," the hospital said in its Notice of Privacy Incident.[6]

◆ **The Advanced Research Projects Agency for Health (ARPA-H) has launched its Universal PatchinG and Remediation for Autonomous DEfense (UPGRADE) program, a cybersecurity effort that will invest more than $50 million to create tools for hospital information technology teams to better defend the hospital environments they are tasked with securing**. ARPA-H noted that cyberattacks that hamper hospital operations can impact patient care while critical systems are down and can even lead to facility closure. Meanwhile, the agency said, a major hurdle in advancing cybersecurity tools in the health sector is the number and variety of internet-connected devices unique to each facility. "While consumer products are patched regularly and rapidly, taking a critical piece of hospital infrastructure offline for updates can be very disruptive," ARPA-H said. "Delayed development and deployment of software fixes can leave actively supported devices vulnerable for over a year and unsupported

legacy devices vulnerable far longer." According to ARPA-H, "the UPGRADE platform will enable proactive evaluation of potential vulnerabilities by probing models of digital hospital environments for weaknesses in software. Once a threat is detected, a remediation (e.g., patch) can be automatically procured or developed, tested in the model environment, and deployed with minimum interruption to the devices in use in a hospital." UPGRADE will issue a solicitation seeking performer teams to submit proposals on four technical areas: creating a vulnerability mitigation software platform, developing high-fidelity digital twins of hospital equipment, auto-detecting vulnerabilities, and auto-developing custom defenses. The agency said it anticipates multiple awards under this solicitation.[7]

1 Geisinger Health System, "Geisinger provides notice of Nuance's data security incident," news release, June 24, 2024, https://bit.ly/3VU486K.
2 U.S. Department of Justice, U.S. Attorney's Office for the Northern District of Iowa, "Emergency Room Doctor Pleads Guilty to HIPAA Violation," news release, June 28, 2024, https://bit.ly/3XOFzL4.
3 Federal Bureau of Investigation, Internet Crime Complaint Center, *Federal Bureau of Investigation Internet Crime Report 2023*, accessed July 8, 2024, https://bit.ly/4bIvDpS.
4 BakerHostetler, *2024 Data Security Incident Response Report: Persistent Threats, New Challenges*, 2024, https://bit.ly/4bzRijJ.
5 Matthew S. McCoy et al., "User Information Sharing and Hospital Website Privacy Policies,"*JAMA Network Open* 7, no. 4 (2024): e245861, https://bit.ly/3zABBvx.
6 BayCare, "Winter Haven Hospital Notice of Privacy Incident," accessed June 21, 2024, https://bit.ly/45VrwFn.
7 Advanced Research Projects Agency for Health, "ARPA-H announces program to enhance and automate cybersecurity for health care facilities," news release, May 20, 2024, https://bit.ly/4cvgF7P.