COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 12. December 07, 2023 Privacy Briefs: December 2023

By Jane Anderson

◆ **Northwell Health in New York and Cook County Health in Chicago each experienced impacts from a breach at Nevada-based transcription company Perry Johnson & Associates (PJ&A) that affected nearly 9 million patient records in multiple states overall.** According to PJ&A's cyber incident notice, an unauthorized party gained access to the company's network between March 27 and May 2 "and, during that time, acquired copies of certain files from PJ&A systems."[1] The transcription company determined that the files involved contained personal health information that potentially included names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses and dates and times of service. For some individuals, the impacted data may have included Social Security numbers, insurance information and clinical information from medical transcription files, such as laboratory and diagnostic testing results, medications, the name of the treatment facility and the names of health care providers. Cook County Health reported that records of 1.2 million patients were affected by the breach and said it had terminated its relationship with PJ&A upon learning of the data security incident.[2] Northwell Health reportedly may have had more than 3.8 million affected patients.[3]

◆ **Truepill, a digital health startup that provides pharmacy fulfillment services for health care organizations, confirmed that hackers accessed the personal data of more than 2.3 million patients.** In a data breach notice published on its website, the company said that Postmeds, the parent company behind TruePill, experienced a "cybersecurity incident" that allowed unnamed attackers to gain access to files used for pharmacy management and fulfillment services between Aug. 30 and Sept. 1. The company's investigation found that the accessed files contained sensitive customer information, including patient names, unspecified demographic information, medication type and the name of the patient's prescribing physician. Truepill said Social Security numbers were not involved. The company's website said that Truepill has served more than 3 million patients and delivered 20 million prescriptions since it was founded in 2016. In response to the breach, Truepill said it was enhancing its security protocols and rolling out additional cybersecurity training for employees.[4]

◆ **Four U.S. senators on the Senate Health, Education, Labor, and Pensions Committee launched a bipartisan working group to examine and propose potential legislative solutions to strengthen cybersecurity in the health care and public health sector.** Sen. Bill Cassidy, R-La., the ranking member on the committee, along with Sens. Mark Warner, D-Va., John Cornyn, R-Texas, and Maggie Hassan, D-N.H., said that their effort comes at a time of record cybersecurity attacks on health care entities. "Health records, unlike other personal records like credit card numbers, are more valuable on the black market since health conditions are permanent and cannot be reissued," the four said in their announcement.[5]

◆ **Hospitals in multiple states were forced to divert patients from their emergency departments after a major cyberattack hit their parent company, Ardent Health Services, on Thanksgiving Day.** "We continue to care for patients in our 30 hospitals, as well in our emergency rooms [ER] and clinics," Ardent said in a Nov. 30 statement.[6] "At this time, all of our 25 [ERs] are accepting patients by ambulance. In some cases, we continue to ask local EMS [emergency medical services] services to transport patients in need of certain emergency care, such as stroke or trauma care, to other area ERs. All hospitals continue to provide a medical screening exam and

stabilizing care to any patients arriving at our ERs. The vast majority of our clinics have resumed operations at this time. Out of an abundance of caution, some non-emergent procedures have been temporarily paused while we work to bring systems back online." Ardent said it had shut down a significant number of its systems, including clinical programs and its electronic medical record system, as a result of the attack. Spokespeople at three Ardent-owned hospital chains across the U.S.—Hillcrest HealthCare System in Oklahoma, Lovelace Health System in New Mexico and UT Health in Texas—each told NBC News that at least some of their ERs were diverting patients to other hospitals. Patients also were diverted in New Jersey, reports said.[7]

◆ **Cyber criminals obtained medical records and naked patient photos from a Las Vegas plastic surgery office and posted them online for ransom, an investigation found.** 8 News Now said the stolen information included sensitive personal information such as names, Social Security numbers and nude photos of patients taken before and after surgery. Many of the photos, which show breasts and other sensitive areas, contain patients' faces. About a dozen women filed a lawsuit against the office, Hankins & Sohn Plastic Surgery Associates, claiming the office did not do enough to protect their private and personal information. Four women interviewed by 8 News Now reported that they had breast augmentations at the plastic surgery practice between late 2020 and early 2022. All four said they were happy or satisfied with the work performed. In February, cybercriminals obtained access to the office's network, downloading patient information, the lawsuit and a letter to patients said. The hackers then posted the photos, along with full names, addresses, emails and other private personal information, including medical records. One woman interviewed said hackers had obtained her bank account information and stole more than $1,000. In some cases, the hackers sent the information, along with nude photos, to family and friends through patients' email accounts. Documents reviewed by the 8 News Now team indicate that records for more than 12,000 patients may have been involved. A breach notification was sent out to patients in April, and the website with patient photos and data appeared in July, according to the investigation. One of the women interviewed said the FBI was able to shut down the hackers' website once, but since then, a new website has come online, with a note from the hackers saying the surgeons were ignoring them and they planned to add more patient information and photos. Hankins & Sohn Plastic Surgery provided a statement saying the practice is "devastated" by the data breach and that it continues "to work with the FBI and other agencies to protect patient information and also to bring these bad actors to justice."[8]

◆ **The Cybersecurity & Infrastructure Security Agency (CISA) has released a guide to defensive mitigation strategy recommendations and best practices to combat pervasive cyber threats affecting the health sector.** The guide also identifies known vulnerabilities for organizations to assess their networks and minimize risks before intrusions occur. CISA's Mitigation Guide: Healthcare and Public Health (HPH) Sector is a supplemental companion to the HPH Cyber Risk Summary, published in July, the agency said. Mitigation strategies detailed in the guide include asset management and security, identity management and device security, vulnerability, patch and configuration management. The guide also provides information on how to make systems secure by design. According to CISA, the agency has identified common vulnerabilities and insecure configurations across the health care and public health sector, such as web application vulnerabilities, encryption weaknesses, unsupported software, unsupported Windows operating systems, known exploited vulnerabilities and vulnerable services.[9]

1 Perry Johnson & Associates, "Cyber Incident Notice," November 2023, https://bit.ly/3R6V8c6.
2 Cook County Health, "Cook County Health Notice of Data Security Incident," accessed December 4, 2023, https://bit.ly/3t9hlxZ.
3 Kevin Vesey, "Cyberattack targets Northwell Health vendor; patient data compromised," News 12 Long Island, November 9, 2023, https://bit.ly/3Nc63zU.
4 Carly Page, "Digital pharmacy startup Truepill says hackers accessed sensitive data of 2.3 million patients,"

TechCrunch, November 15, 2023, https://bit.ly/3TaITh3.
5 U.S. Senate Committee on Health, Education, Labor & Pensions ranking member's newsroom, "Ranking Member Cassidy, Warner, Colleagues Launch Bipartisan Senate Health Care Cybersecurity Working Group," news release, November 2, 2023, https://bit.ly/3Tb8WF0.
6 Ardent Health Services, "Cybersecurity Incident: Latest Update," webpage notice, November 30, 2023, https://bit.ly/3Rtz392.
7 Kevin Collier, "Emergency rooms in at least 3 states diverting patients after ransomware attack," NBC News, November 27, 2023, https://bit.ly/3RsIqpk.
8 David Charns, "Hackers target Las Vegas plastic surgeons, post patient information, naked photos online," 8 News Now Investigations, November 6, 2023, https://bit.ly/3GroMnt.
9 Cybersecurity & Infrastructure Security Agency, "CISA Releases The Mitigation Guide: Healthcare and Public Health (HPH) Sector," news release, November 17, 2023, https://bit.ly/3Ta9Cur.