COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 6. June 08, 2023 Privacy Briefs: June 2023

By Jane Anderson

◆ **Long-term care pharmacy network PharMerica disclosed a breach involving more than 5.8 million patients, making it the largest breach reported to the HHS Office for Civil Rights (OCR) in the last 24 months.** According to a privacy incident notice posted on PharMerica's website, PharMerica and its parent company, BrightSpring Health Services, learned of suspicious activity on their computer network on March 14. The ensuing investigation determined that an unknown third party had accessed PharMerica computer systems from March 12 to March 13 and that "certain personal information may have been obtained as a part of the incident." On March 21, PharMerica "identified a data population whose personal information and limited medical information (names, dates of birth, Social Security numbers, medication lists and health insurance information) were disclosed." PharMerica said it has arranged for complimentary identity protection and credit monitoring services for potentially affected individuals.[1]

◆ **The Food and Drug Administration (FDA) is warning health care providers and laboratory personnel about a cybersecurity vulnerability affecting the Universal Copy Service (UCS) software in specific Illumina devices designed for gene sequencing.** These sequencing devices are used for clinical diagnosis to sequence a person's DNA for various genetic conditions or in research. According to the FDA, an unauthorized user could exploit the vulnerability by taking control remotely; altering settings, configurations, software or data on the instrument or on a customer's network; impacting genomic data results in the instruments intended for clinical diagnosis, including causing the instruments to provide no results, incorrect results, altered results or a potential data breach. The FDA noted that it has not received any reports indicating the vulnerability has been exploited. Illumina developed a software patch to protect against the exploitation of this vulnerability, and the FDA is urging providers and laboratory personnel to mitigate the risk immediately.[2]

◆ **University of Missouri (MU) Health Care, based in Columbia, Mo., disclosed that an employee used the health system's electronic medical record to access 736 medical records between July 2021 and March 2023, potentially without reason under HIPAA.** According to the health system, "the accesses may have contained patient information including name, date of birth, medical record number, and limited treatment and/or clinical information, such as diagnostic and/or procedure information." To date, there is no indication that the information was misused or redisclosed, the health system said. However, MU Health Care began mailing notification letters to patients whose information may have been inappropriately accessed, "alerting them to the incident and advising them to be vigilant in the event of any suspicious activity involving their accounts." The health system did not disclose whether it had fired the worker in question but said it had "taken appropriate action according to applicable policies and procedures."[3]

◆ **Litigation related to data breaches increased in 2022, and lawsuits are being filed in matters affecting fewer individuals, according to law firm BakerHostetler's 2023 Data Security Incident Response Report.** In its ninth edition, the annual survey reports on data from more than 1,160 security incidents across industries. Overall, the report found that the number of incidents in 2022 was almost identical compared to 2021. Some 24% of the incidents tracked involved health care entities, the law firm found. There were fewer ransomware incidents for most of 2022, compared to 2021, until an end-of-the-year surge that resulted in a moderate increase in the

average amount of initial ransom demands, the amount of ransom actually paid and the length of time to recover from a ransomware attack. Recovery times for most industries increased in 2022, the survey found. Network intrusions remained the most common type of incident, accounting for nearly half of the incidents tracked in the report. "On a positive note, companies are getting quicker at identifying—and containing—such incidents," the law firm study found. Meanwhile, fraudulent fund transfers, which were prevalent in 2021, saw a decrease in number, total transfer amount and average transfer amount in 2022. However, the rate of success in recovering funds dropped from 42% in 2021 to 24% in 2022, the survey found. Forensic investigation costs increased by 20% on average in 2022 from 2021.[4]

◆ **A data breach last October at the San Diego Unified School District involved students' medical information, the district told families in a May letter.** Dennis Monahan, executive director of risk services for the district, said an investigation of the breach showed that students' names and medical information were compromised; staff and students were issued new passwords. San Diego Unified officials first notified families of the incident in early December and said at the time that a third party had accessed some of the school district's systems on Oct. 25. District officials said staff quickly secured the network, launched an investigation and notified law enforcement. Monahan said officials have implemented additional security measures to enhance network protocols. A district spokesperson said the investigation is continuing and that the district is working to notify those affected as it identifies them. The district did not respond to questions about how many students had been affected, whether staff data also may have been compromised and how the security measures have been enhanced.[5]

◆ **NationsBenefits Holdings LLC, a provider of supplemental benefits, flex cards and member engagement solutions to health care plans and managed care organizations, confirmed it was one victim of the security incident resulting from a zero-day remote code execution vulnerability in Fortra LLC's GoAnywhere managed file transfer (MFT) software.** In a data security incident report provided to New Hampshire Attorney General John Formella, NationsBenefits Holdings said a threat actor exploited the zero-day vulnerability on Jan. 30 to access a NationsBenefits GoAnywhere server. NationsBenefits first discovered the incident on Feb. 7 when the firm's security monitoring team received an alert regarding a potential security event on the impacted MFT server. The incident was limited to two MFT servers, the company said, with no evidence that the threat actors moved laterally to other applications or systems within the NationsBenefits environment. Overall, NationsBenefits Holdings reported to OCR that the security incident involved more than 3 million patients from a variety of different health insurers, including Aetna, Elevance Health and UAW Retiree Medical Benefits Trust. Information potentially affected includes first and last names, dates of birth, gender, health plan subscriber ID numbers, Social Security numbers and Medicare identification numbers. NationsBenefits is providing complementary 24-month membership to Experian's IdentityWorks for members with sensitive data impacted "or where otherwise deemed reasonable and appropriate by NationsBenefits' clients."[6]

◆ **Cyberattacks launched by threat actors against Veeam Backup & Replication (VBR) are rising, the Health Sector Cybersecurity Coordination Center (HC3) is warning.** VBR is a software product created by Veeam Software that is used to back up, replicate and restore data on virtual machines. "What makes this threat significant is that in addition to backing up and recovering [virtual machines], it is used to protect and restore individual files and applications for environments such as Microsoft Exchange and SharePoint," HC3 said, noting that these are used in the health care sector. "Veeam Backup & Replication also has the ability to provide transaction-level restores of Oracle and Microsoft [structured query language] SQL databases," HC3 said. In late March 2023, the agency said, threat researchers identified attacks carried out by at least one threat actor group, FIN7, against internet-facing servers running VBR software. FIN7 is a threat actor group that was discovered in the mid-2010s, HC3 said. It's financially motivated, has been connected to numerous high-profile attacks and is known for affiliating with other threat actor groups, such as Conti, REvil and BlackBasta. "HC3 recommends that all [health care and public health] sector entities be aware of suspicious activity, keep systems up to date, and immediately patch any

vulnerable systems."[7]

1 PharMerica, "PharMerica Notifies Individuals of Privacy Incident," accessed June 5, 2023, bit.ly/3IYFdJq.
2 U.S. Food and Drug Administration, "Illumina Cybersecurity Vulnerability Affecting the Universal Copy Service Software May Present Risks for Patient Results and Customer Networks: Letter to Health Care Providers," April 27, 2023, bit.ly/42qZVbN.
3 MU Health Care, "Patient Privacy Incident," accessed June 5, 2023, bit.ly/42nAhVn.
4 BakerHostetler, "BakerHostetler Launches 2023 Data Security Incident Response Report," news release, April 27, 2023, bit.ly/43pVnDY.
5 Lauryn Schroeder, "San Diego Unified students' medical data was compromised in fall cybersecurity breach, school district says," *La Jolla Light*, May 20, 2023, bit.ly/3NhbaiX.
6 Robert Duffy, "Re: Data Security Incident," letter to New Hampshire Attorney General John Formella, April 13, 2023, bit.ly/3CdFfcD.
7 U.S. Department of Health & Human Services, Health Sector Cybersecurity Coordination Center, " Veeam Backup & Replication Latest Threat Actor Target," HC3: Sector Alert, May 10, 2023, bit.ly/3Nd3xtI.