COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 1. January 07, 2021 Privacy Briefs: January 2021

By Jane Anderson

◆ **The HHS Office for Civil Rights (OCR) settled its 13th enforcement action in its Right of Access Initiative**, first announced in 2019 to support individuals' rights to timely access their health records at a reasonable cost under the privacy rule.[1] As part of the settlement, announced Dec. 22, Peter Wrobel, doing business as Georgia-based Elite Primary Care, agreed to take corrective actions and pay $36,000 to settle a potential violation of the right of access standard. In April 2019, OCR received a complaint alleging that Elite failed to respond to a patient's request for access to his medical records, and OCR provided technical assistance in May 2019. However, OCR received a second complaint in October 2019 alleging that Elite still had not provided the patient with access to his medical records and initiated an investigation. In addition to the monetary settlement, Elite is required to follow a corrective action plan (CAP) for two years. The CAP includes implementation of policies and procedures governing the right of access, plus additional training and monitoring.

◆ **GenRx Pharmacy in Scottsdale, Arizona, is warning hundreds of thousands of customers of a data security incident stemming from ransomware.**[2] On Sept. 28, the pharmacy found evidence of ransomware in its system and immediately began an investigation. During the ransomware attack, the pharmacy had full access to its data and unaffected backups, it said. Together with forensic experts, the pharmacy terminated the cybercriminals' access to the pharmacy's systems the same day they were discovered and confirmed that the ransomware had been deployed the day before it was discovered. On Nov. 11, the pharmacy confirmed that the cybercriminals were able to remove a small number of files that included certain health information the pharmacy used to process and ship prescribed products to patients, the pharmacy said. Information that was removed included patient identification numbers, transaction identification numbers, first and last names, addresses, phone numbers, dates of birth, genders, allergies, medication lists, health plan information (including member identification numbers) and prescription information. The pharmacy does not collect patient Social Security numbers. In response to the attack, the pharmacy upgraded its firewall, added additional antivirus and web-filtering software, instituted multifactor authentication, increased Wi-Fi network traffic monitoring, provided additional training to employees, updated internal policies and procedures, and installed real-time intrusion detection and response software on all workstations and servers that access the company network. The pharmacy said it also is assessing further options to enhance its protocols and controls, technology and training, including strengthening encryption.

◆ **The National Institute of Standards and Technology has issued a new cybersecurity practice guide, *Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector*.**[3] PACS, which is ubiquitous in health care environments and often interfaces with a range of interconnected systems, can result in cybersecurity risks. The National Cybersecurity Center of Excellence (NCCoE) at NIST analyzed risk factors regarding the PACS ecosystem using a risk assessment based on the NIST Cybersecurity Framework and other relevant standards. Then, NCCoE developed an example implementation that demonstrates how health care delivery organizations can use standards-based, commercially available cybersecurity technologies to better protect the PACS ecosystem.

◆ **Monroe Surgical Hospital in Louisiana has begun notifying patients about a service provider security incident**

that involved the personal information of some of its patients and customers.[4] The hospital uses an IberiaBank lockbox service, which collects and processes payments from patients and customers. In turn, IberiaBank uses a third party, Technology Management Resources Inc. (TMR), to scan and process the payments and other pertinent payment data received in the lockbox. Monroe Surgical Hospital has no business relationship with TMR. In July 2020, TMR discovered that an employee's user account had been compromised. Monroe Surgical Hospital received formal notice of the incident on Oct. 13 and began investigating. TMR reported that when it first discovered the incident, it immediately secured the account and began an investigation with external cybersecurity professionals. TMR has stated that its investigation determined that the cybercriminal may have viewed images of checks and related images containing protected health information for patients of Monroe Surgical Hospital. According to TMR, the threat actor activity occurred between Aug. 5, 2018, and May 31, 2020, with most of the activity occurring between February and May 2020. The incident is believed to be part of a wider effort by an unknown cybercriminal to attack TMR customers beyond IberiaBank, Monroe Surgical Hospital said.

◆ **Presbyterian Health Plan in Albuquerque, New Mexico, said it has notified more than 3,000 members that a misdirected mailing may have exposed some of their protected health information.**[5] In a security incident notice posted on the plan's website, Presbyterian said that the misdirected mailing occurred on Oct. 1 when a letter was sent to some members under their names but with a different member's address. The letter contained member names, reminders about recommended health screenings for managing their health care treatment and contact information for care coordination. The mailing did not involve Social Security numbers, financial or credit card information, or any information contained in medical systems or any other health information. Presbyterian said it is not aware of any improper or attempted use or disclosure of health screening information.

◆ **Health care provider GBMC HealthCare in Maryland was hit in early December by a ransomware attack that affected many of its information technology systems, forcing them offline.**[6] As a result, GBMC spent some time with those systems offline, the organization said, noting that there's no evidence at this time that any patient information has been misused. "Although many of our systems are down, GBMC HealthCare has robust processes in place to maintain safe and effective patient care," the provider organization said. "We are collectively responding in accordance with our well-planned process and policies for this type of event."

◆ **Cedar Springs Hospital in Colorado is responding to requests for records from the Colorado Department of Public Health and Environment (CDPHE) after a health department surveyor lost an external hard drive with copies of patient records from the hospital.**[7] The device was not encrypted, contrary to state health department policy, according to the hospital. "In late October, in connection with a survey, the CDPHE requested Cedar Springs Hospital copy a number of records onto an external drive that CDPHE provided to the facility. Cedar Springs Hospital complied with the request. On October 28, 2020, CDPHE notified Cedar Springs Hospital that the surveyor misplaced the external device containing the documents. Cedar Springs Hospital learned at the time that, contrary to CDPHE's policy, the external device that the CDPHE surveyor provided for use was not encrypted. CDPHE could not rule out the possibility that an unauthorized individual could access the information, if that individual obtained possession of the CDPHE external device." Information loaded onto the device included names, addresses, dates of birth, Social Security numbers, medical record numbers, patient identification numbers, health insurance information (including health insurance numbers), treatment history (including dates of treatment, treatment location, and treating physician), medical diagnosis information and prescription information, according to the hospital. "Cedar Springs Hospital is working with CDPHE to obtain additional information about the incident, including why CDPHE policy was not followed and why an unencrypted external device was utilized," the hospital said.

◆ **Dental Care Alliance, based in Sarasota, Florida, a dental support organization with more than 320 affiliated dental practices in 20 states, said it was hit in October with an attack that may have revealed information from**

one million patients.[8] In its notice to patients, the company said it "became aware of suspicious activity in its environment" on Oct. 11 and initiated an investigation. The investigation showed that unauthorized individuals accessed "certain files on the Practice's network between September 18, 2020 and October 13, 2020," the company said. Information that was potentially subject to unauthorized access includes names, addresses, dental diagnoses and treatment information, patient account numbers, billing information, dentist names, bank account numbers, and health insurance information. There has been no evidence to date of misuse of the information, the company said.

1 HHS, "OCR Settles Thirteenth Investigation in HIPAA Right of Access Initiative," news release, December 22, 2020, https://bit.ly/387GtrX.
2 Business Wire, "GenRx Pharmacy Issues Data Security Incident Notice," news release, December 18, 2020, https://bwnews.pr/3aUwhVm.
3 Jennifer Cawthra et al., *Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector*, National Institute of Standards and Technology, NIST Special Publication 1800-24, accessed January 4, 2021, http://bit.ly/3rSuTIT.
4 "Monroe Surgical Hospital reports possible data breach, notifying patients," *The Ouachita Citizen*, December 9, 2020, https://bit.ly/34Z4VJU.
5 Presbyterian Healthcare Services, "Notification of Data Security Incidents," news release, accessed December 31, 2020, https://bit.ly/381eOIU.
6 GBMC HealthCare, "Computer Network Incident Update," news release, December 6, 2020, https://bit.ly/3aX067z.
7 PR Newswire, "Cedar Springs Hospital – Notice of Data Incident," news release, December 9, 2020, https://prn.to/3aWcnt9.
8 Office of the Vermont Attorney General, "Dental Care Alliance Notice of Data Breach to Consumers," December 7, 2020, https://bit.ly/38Q18zJ.