COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 7. July 08, 2021 Privacy Briefs: July 2021

By Jane Anderson

◆ **Mayo Clinic is facing three lawsuits from patients who say a former surgery resident, Ahmad Alsughayer, viewed hundreds of their nude photographs in electronic health records (EHRs) despite having no professional reason to go into their files.**[1] Alsughayer was charged in April by the Olmsted County attorney's office with a single gross misdemeanor of unauthorized computer access after one of the 1,614 patients whose records he viewed filed a report with the Rochester police. The three civil lawsuits include one from a Rochester-area woman who works at Mayo Clinic. She is suing the health system for failing to use a feature in its EHR system that she said would have prevented the privacy breach by limiting access to highly sensitive medical records. Although the data breach letter she received from Mayo didn't expressly mention the naked photos, the woman told the *Star Tribune* that she figured it out based on the dates of the records. A plaintiff in a second lawsuit said she felt Mayo personnel weren't honest when they said the investigation couldn't find a medical or business reason for the breach and Mayo would never know why this happened. "This representation was false," the lawsuit said. "Mayo Clinic already knew, but did not tell plaintiff, that Alsughayer had requested access to these 1,600+ EHRs to view naked images of female patients…and that Mayo Clinic chose not to implement the fixes and protections proper to have prevented this incident." A third lawsuit is pending with similar allegations. All three cases are filed in state court, and two of the three are seeking class-action status. In court filings, Mayo has denied the allegations. The health system said that its staff investigated the incident, concluded that only one employee viewed patients' "protected medical information," and notified the authorities and affected patients.

◆ **In Canton, Ohio, "more than 7,000 Aultman Health Foundation patients may have had their private records accessed by a former worker as part of a privacy breach" that stretched for more than 11 years,** the hospital system said.[2] The former Aultman employee accessed patient information outside the scope of their job duties between Sept. 14, 2009, and April 26, 2021, the organization said. The employee may have accessed patients' names, addresses, dates of birth, Social Security numbers, insurance information, and diagnosis and treatment information. "Upon discovering this, the employee's access to Aultman's electronic health record system was suspended, and an investigation was conducted to determine the nature and scope of the incident," Aultman said in a statement. The employee, who has not been identified, has been terminated and no longer has access to patient data. The worker, who was not a medical provider but had access to patient information as part of their job coordinating patient care, is not facing criminal charges, according to hospital officials. The employee went beyond the scope of their position, hospital officials said, but so far, there's no indication that patient information was misused or will be misused.

◆ **Iowa-based Wolfe Eye Clinic experienced a cybersecurity attack that might have exposed data for some 500,000 patients.**[3] The clinic said in its breach notification letter that Wolfe Eye Clinic was the target of an attack on Feb. 8 "that involved an unauthorized third party attempting to gain access to our computer network."[4] After an investigation by independent experts, Wolfe determined that personal information, including names, mailing addresses, dates of birth, Social Security numbers and protected health information may have been accessed by the hacker. The clinic said it will provide identity theft monitoring to all affected individuals.

◆ **The Mississippi Center for Advanced Medicine said in late June that a data breach affected its internal server and may have led hackers to access health information for some patients.**[5] The Jackson organization, which integrates subspecialty medical care, clinical pharmacy services and care coordination for patients with pediatric, congenital and maternal-fetal disorders, said it was the victim of a ransomware demand in December. The organization said the data exposed could have included names, addresses and phone numbers, email addresses, dates of birth, Social Security numbers, information to process insurance claims, prescription information, prescribing doctor names, medication names and dates, medical history as well as information on certain clinical services, such as whether an influenza test was ordered. The organization said that electronic health information was not compromised and that the hackers did not gain access to financial information.

◆ **Ohio Medicaid providers' data may have been exposed from a data breach when someone gained unauthorized access to an app,** a state contractor to the Ohio Medicaid program said.[6] The data manager, Maximus, said it had a cybersecurity incident in mid-May that potentially exposed provider names, Social Security numbers, addresses and other information. The application that was accessed included Ohio credentialing and licensing data. Ohio Medicaid said it is monitoring the progress of the investigation and is working with Maximus. Maximus mailed letters to affected providers on June 18. The contractor said in a statement that it "promptly took the impacted application offline, launched an investigation with a leading cybersecurity firm, activated response protocols, and notified law enforcement." Maximus also said that "because the unauthorized activity was detected at a very early stage, Maximus believes our quick response limited potentially adverse impacts." Providers who had data that may have been exposed can receive two years of credit monitoring services and will receive a letter with credit monitoring instructions.

◆ **Prominence Health Plan in Reno, Nevada, said that personal information for some 45,000 of its members was accessed in a November data breach that involved audio recordings** from the Prominence call center, files with health care claim forms, and letters to patients with claim approvals or denials.[7] The insurance company said it learned about the breach, which allegedly did not include Social Security numbers or other final information, on April 22. Prominence said it is implementing additional security measures in the wake of the breach, and that it will provide free credit monitoring and identity theft services to affected plan members.

◆ **Coastal Medical Group in Old Bridge, New Jersey, is notifying patients of a data security incident that may have exposed protected health information.**[8] On April 21, the practice discovered that certain parts of its computer systems were being affected by a data security event that the practice believes began on March 25, according to a statement. An investigation determined that the incident resulted in the unauthorized access and acquisition of certain files on the practice's computer systems. Information affected may have included full names, home addresses, dates of birth, other demographic and contact information, Social Security numbers, insurance information, and diagnosis and treatment information. No financial information was affected. The practice is offering free credit monitoring and identity theft services.

◆ **The National Security Agency (NSA) has released a cybersecurity technical report that provides best practices and mitigations for securing unified communications call processing systems.**[9] The report, *Deploying Secure Unified Communications/Voice and Video over IP Systems*, describes potential risks to systems that are not properly secured. To complement the larger report, NSA published an abridged fact sheet to capture key takeaways and introduce the steps organizations should take when securing their systems.[10]

1 Joe Carlson, "Mayo Clinic faces lawsuits over nude patient image snooping," *Star Tribune*, June 30, 2021. http://strib.mn/2SJ9TYo.
2 Jessica Holbrook, "Aultman warns patients of privacy breach," *The Repository*, June 25, 2021,

https://bit.ly/3jsSGxg.
3 "Iowa eye clinic: 500,000 patient files may have been stolen," Associated Press, June 22, 2021, https://bit.ly/3hj0OxL.
4 "Notice of Data Incident," Wolfe Eye Clinic, accessed July 6, 2021, https://bit.ly/3qzlaHg.
5 Sharie Nicole, "Miss. healthcare organization announces data breach affecting patient information," WLOX, June 23, 2021, https://bit.ly/3623pqv.
6 Kaitlin Schroeder, "Ohio Medicaid providers' data may have been exposed from data breach," *Dayton Daily News*, June 22, 2021, https://bit.ly/3y7nOq1.
7 "Prominence Health Plan Reports Data Breach," 2 News, June 18, 2021, https://bit.ly/2SD5Htb.
8 "Coastal Medical Group notifies patients of data breach," centraljersey.com, June 18, 2021, https://bit.ly/3w6QbUa.
9 National Security Agency, *Deploying Secure Unified Communications/Voice and Video over IP Systems*, SN U/OO/153515-21, June 2021, https://bit.ly/3hesRhy.
10 National Security Agency, "Deploying Secure Unified Communications/Voice and Video over IP Systems (Abridged)," U/OO/184192-20, June 2021, https://bit.ly/3duhAsz.