COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 1. January 11, 2023 Privacy Briefs: January 2023

By Jane Anderson

◆ **The Centers for Medicare & Medicaid Services (CMS) said a data breach at a Medicare subcontractor impacted the personally identifiable information and protected health information (PHI) of up to 254,000 Medicare beneficiaries.** The data breach occurred at Healthcare Management Solutions LLC, a subcontractor of ASRC Federal Data Solutions LLC. ASRS Federal Data Solutions provides services to CMS that involve resolving system errors related to Medicare beneficiary entitlement and premium payment records. The contractor's services also support the collection of Medicare premiums from the direct-paying beneficiary population, according to CMS, which reported that the contractor does not handle Medicare claims information. CMS is notifying Medicare beneficiaries whose information may have been put at risk due to the breach and will issue them updated Medicare cards with new Medicare beneficiary numbers. Those whose information was involved in the breach will be offered free-of-charge credit monitoring services, according to CMS.[1]

◆ **Amazon has notified developers that it has decided to no longer support the HIPAA-eligible skills offered for digital voice assistant Alexa, ending the sole opportunity for independent developers to build voice experiences if HIPAA-eligible data can be collected.** "We kindly ask that you remove your skill from the skills store," Amazon wrote to developers. "Alternatively, we will suppress your skill for you on December 9, 2022. Once the skill is removed/suppressed, any existing users who try to use the skill will get a message that the skill is no longer supported. Alexa responds by default to these types of utterances with, 'Sorry, I didn't get that.' After the skill is suppressed, Amazon will delete all associated PHI. Alexa does not plan to contact users of your skill but we encourage you to reach out to your skill users if you anticipate user frustration or questions." This doesn't mean Amazon is abandoning the idea of using Alexa in HIPAA-protected environments; however, the tech giant can still develop HIPAA-compliant Alexa skills in-house. In its message to developers, Amazon stated: "We continue to grow our Alexa Smart Properties for Healthcare business," and an Amazon spokesperson said that the company is "continuing to invest heavily in developing healthcare experiences with first and third-party developers." Amazon first launched its HIPAA-compliant feature for Alexa in April 2019, and six health care organizations signed on at the time.[2]

◆ **The Federal Trade Commission (FTC), in conjunction with the HHS Office for Civil Rights, the HHS Office of the National Coordinator for Health Information Technology (ONC), and the Food and Drug Administration, has updated its Mobile Health App Interactive** Tool. The tool is designed to help developers of health-related mobile apps understand what federal laws and regulations might apply to them. The guidance tool asks developers a series of high-level questions about the nature of their app, including its function, the data it collects and the services it provides to users. Based on the developer's answers to those questions, the guidance tool will point the app developer toward detailed information about certain federal laws that might apply to the app, which can include: the FTC Act; the FTC's Health Breach Notification Rule; the Children's Online Privacy Protection Act; HIPAA; the Federal Food, Drug and Cosmetics Act; and the 21st Century Cures Act and ONC Information Blocking Regulations. The FTC first released the online tool in 2016.[3]

◆ **UC Davis Health in Sacramento, California, is notifying 408 patients that an employee accessed their electronic medical records without a work purpose between Nov. 2, 2017, and July 18, 2022.** UC Davis Health first confirmed

the inappropriate access on Aug. 5, 2022. The employee accessed demographic information, including names, dates of birth, medical record numbers, addresses, phone numbers and clinical information contained in medical records, according to the health system. No financial or billing information was accessed, and Social Security numbers were not viewed, the health system said. "We do not believe that the intent of this access was to obtain financial information, and we have no evidence that any information was removed from the records or shared with anyone else." The health system noted that it has reviewed the incident and is "taking appropriate corrective action including reporting the breach both internally and externally to mitigate risk to affected patients and prevent similar future events." Affected patients were notified in August by first-class mail, according to UC Davis Health.[4]

◆ **Avem Health Partners, a company based in Oklahoma City that provides administrative and technology services to health care organizations, has notified around 271,000 patients that their personal information may have been compromised** due to a breach on servers owned by subcontractor 365 Data Centers. "According to 365 Data Centers, on May 16, 2022, they determined that information stored on their servers may have been subject to unauthorized access prior to May 14, 2022," Avem said in a statement. "Subsequently, Avem conducted a review of the Avem files that were stored on the 365 Data Centers server. Based on this review, which was completed on October 6, 2022, Avem determined that the files contained patient information, including patient names, dates of birth, Social Security numbers, driver's license numbers, health insurance information, and diagnosis and treatment information." Avem is notifying breach victims and said that those patients whose Social Security numbers or driver's license numbers may have been involved in the incident would be offered complimentary credit monitoring and identity theft protection services.[5]

◆ **The HHS Health Sector Cybersecurity Coordination Center (HC3) is warning that the Royal ransomware variant —which has demanded ransoms up to millions of dollars—is increasing in appearance and has been seen targeting the health care and public health sector.** "Royal is an operation that appears to consist of experienced actors from other groups, as there have been observed elements from previous ransomware operations," HC3 said in an analyst note. "While most of the known ransomware operators have performed Ransomware-as-a-Service (RaaS), Royal appears to be a private group without any affiliates while maintaining financial motivation as their goal. The group does claim to steal data for double-extortion attacks, where they will also exfiltrate sensitive data." Once Royal has compromised a network, "they will perform activities commonly seen from other operations, including deploying Cobalt Strike for persistence, harvesting credentials, and moving laterally through a system until they ultimately encrypt the files," HC3 said. Ransom demands have ranged from $250,000 to more than $2 million, the agency said.[6]

◆ **The Rhode Island Department of Health (RIDOH) said that a recent data breach compromised PHI for nearly 9,000 people.** The state agency said a link to a spreadsheet was accidentally included in emails sent by a staff member between July 28 and Oct. 30, 2022. "The file contained information about people receiving food box deliveries while in COVID-19 isolation or quarantine," said Annemarie Beardsworth, a department spokesperson, who added that the file contained information for around 8,880 people. "To RIDOH's knowledge, this file was inadvertently emailed to 46 people, all of whom were on the list to receive food box services," she said. "No medical information or financial information was included in the breach." The spreadsheet contained names, addresses, personal specific needs, household information and date of contact by the RIDOH.[7]

◆ **Officials with the Arkansas Department of Human Services reported that they had discovered a data breach that exposed Medicaid client data.** The officials said the breach occurred on Sept. 16 when an employee sent emails from her state government account to her personal Yahoo email account.[8] The emails had attachments of spreadsheets that listed 925 Medicaid clients who had been diagnosed with the flu. Listed in the attachments were the patients' Medicaid IDs, dates of birth, gender, county of residence, zip codes and diagnoses. Names,

Social Security numbers, full addresses and financial information were not disclosed in the breach, the agency said. In a press release announcing the breach, state officials said that staff members are trained on security issues, including patient privacy. Part of that training includes using secure and encrypted email and not using personal email for client health information. State officials said the department had taken steps to prevent a similar data breach from occurring in the future.

1 Centers for Medicare & Medicaid Services, "CMS Responding to Data Breach at Subcontractor," news release, December 14, 2022, https://go.cms.gov/3vDZ0Xy.
2 Bret Kinsella, "Amazon to End Support Next Week for Third Party Healthcare Alexa Skills with HIPAA Requirements," Voicebot.ai, December 6, 2022, https://bit.ly/3ifKn9K.
3 Federal Trade Commission, "Mobile Health App Interactive Tool," December 2022, https://bit.ly/3ZemYWU.
4 UC Davis Health, "Substitute Notice of Unauthorized Access to Personal Health Information," December 6, 2022, https://bit.ly/3X6PvMs.
5 Avem Health Partners, "Notice of 365 Data Centers Data Security Incident," accessed January 9, 2023, https://bit.ly/3WN0xX8.
6 U.S. Department of Health & Human Services, Health Sector Cybersecurity Coordination Center, "HC3 Analyst Note: Royal Ransomware," Report: 202212071400, December 7, 2022, https://bit.ly/3jTvDy5.
7 Heather Sillins, "Protected health information of nearly 9K compromised in Department of Health data breach," ABC6.com, December 7, 2022, https://bit.ly/3ictEEj.
8 Alex Kienlen, "Data breach at Arkansas Department of Human Services releases Medicaid information," KNWA News, November 16, 2022, https://bit.ly/3ieq3W7.