COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 21, Number 11. November 11, 2021
Privacy Briefs: November 2021

By Jane Anderson

◆ **Current and former patients of Las Vegas Cancer Center (LVCC) may have had their personal information exposed after a ransomware attack, the center said.**[1] Administrators confirmed that hackers accessed encrypted data on the center's server over Labor Day weekend. The security breach was discovered on Sept. 7 when staff returned after the holiday. Although the organization's server and computers were protected by a firewall and multiple malware defense systems, hackers may have been able to access patient names, addresses, dates of birth, Social Security numbers, medical records and insurance information as a result of the breach, according to the center. However, officials said that all patient data was stored in a proprietary format and likely was not usable by hackers. "LVCC does not believe that any data was copied or transferred from its server, and has received no ransom demand from the hackers to unlock data," the center said in a statement. Since the center could not determine what records may have been accessed, administrators advised current and former patients to closely monitor their credit activity and insurance for suspicious activity.

◆ **Oregon's central administrative agency inadvertently released the COVID-19 vaccination status of more than 40,000 employees to two media outlets.**[2] A spreadsheet sent to *The Oregonian* and the *Statesman Journal* was supposed to contain the latest vaccination rates and vaccine exemption rates for each executive branch agency. Gov. Kate Brown (D) issued an executive order in August requiring all executive branch employees—along with individuals working in educational and health care settings—to be fully vaccinated by Oct. 18. But instead of sending the vaccine and rate information, an official at the Oregon Department of Administrative Services emailed a file containing vaccination status by employee name. Oregon House Republican Leader Christine Drazan called it a "significant breach of confidentiality," and the Oregon State Police Officers Association said it had filed a grievance, and was "exploring other legal remedies."

◆ **San Diego officials announced that "the city has received federal funding to develop a San Diego Regional Cyber Innovation Center to help local agencies protect against cyberattacks."**[3] According to a news report, "The Cyber Innovation Center is intended to provide the greater San Diego region with coordinated cybersecurity awareness through collaborative access to tools, intelligence, and a trained and capable workforce," officials said. "It will use timely sharing of information and analysis and specialized training with safe environments to simulate and defend against cyberattacks." There have been several attacks on San Diego agencies and organizations, including "Scripps Health, the Port of San Diego, San Marcos, and UC San Diego Health. The city received two grants from the U.S. Department of Homeland Security totaling about $928,000 to develop a project management plan for the Cyber Innovation Center." The plan includes:

- "Collaborative information-sharing for alerts of malicious activity and emerging threats;
- "An online database of digital documents providing best practices for cybersecurity;
- "A training environment, including both virtual and physical lab space; and
- "A new website with tips and resources."

The city formed a working group that includes “cybersecurity experts, academics, local CEOs, and public officials” to develop the center with the goal of opening in early 2022.

◆ **More than 200,000 patients at UMass Memorial Health in Massachusetts have been notified of a data breach involving the health system’s email system.**[4] Some of the emails accessed by hackers included patient information, such as Social Security numbers and medical-related data. “UMass Memorial Health, in an Oct. 15 notice to patients, said an unauthorized person accessed the accounts between June 2020 and January 2021,” according to a report. “The health system said it was unable to determine to what extent the unauthorized person viewed the emails. The breach did not involve all UMass Memorial patients, only those whose information was contained in the accessed emails.” A notice from the health system said that information affected “included names, dates of birth, medical record numbers, health insurance information, and clinical or treatment information, such as dates of service, provider names, diagnoses, procedure information, and/or prescription information. For health plan participants, the information involved included names, subscriber ID numbers, and benefits election information. For some individuals, a Social Security number and/or driver’s license number was also involved.”

◆ **The Alaska Department of Health and Social Services (DHSS) is notifying all Alaska residents about a cyberattack on its systems that resulted in a breach involving an unknown number of individuals’ data.**[5] The breach first was detected in May, but notification was delayed to avoid interference with a criminal investigation, according to DHSS. Any data stored on the department’s information technology infrastructure at the time of the cyberattack might have been breached, according to DHSS. The department “urges all Alaskans who have provided data to DHSS, or who may have data stored online with DHSS, to take actions to protect themselves from identity theft. Free credit monitoring is being made available to any concerned Alaskan as a result of this breach.” Email notices are being sent to residents who applied for the state’s Permanent Fund Dividend with a code they can use to sign up for credit monitoring. A toll-free hotline also is available for assistance.

◆ **The Virginia Department of Behavioral Health and Developmental Services is investigating after families applying for assistance online in one particular program saw their personal information mixed up with data for other applicants.**[6] Families on the waiting list to receive Individual and Family Support Program funding logged onto the website on Oct. 7 in an effort to receive the grants. Regina Hodges of Mechanicsville said she was applying for funds for her autistic son, and while she was logged into the program’s website, another person’s information took the place of her son’s profile, including the last four digits of a Social Security number. “At that moment, I had someone else’s name, their address, their date of birth, everything that a less honorable person could use to steal [an] identity,” she said. The department sent a message to families notifying them about the breach. A similar breach had occurred on Oct. 1, 2019. Lauren Cunningham, department communications director, said information technology staff members had been “working to simulate and solve the issue since then. Extensive review and testing took place over 17 months prior to this program being put back into service. The program was functioning properly and it was believed the portal was clear to operate as scheduled.” According to the department, the information technology team is attempting to determine how many people were affected and is notifying each person individually.

◆ **Approximately 44% of health care and pharmaceutical organizations experienced a data breach caused by a third party within the last year, according to a report from critical access management firm SecureLink and Ponemon Institute.**[7] “Despite this threat, just 41% of healthcare and pharmaceutical organizations have a comprehensive inventory of all third parties with access to their network,” the report said. Sixty percent agreed that managing third-party permissions and remote access to their network can be overwhelming and a drain on resources, and only 44% of these organizations know the level of access and permissions that both internal and external users hold, the report said.

[1] KTNV staff, "Ransomware attack targets Las Vegas Cancer Center patients' personal information," KTNV Las Vegas, November 1, 2021, https://bit.ly/3BIG76z.

[2] Associated Press, "Oregon agency inadvertently releases 40,000 state employees' vaccine status," KTVZ, October 19, 2021, https://bit.ly/3wau2G9.

[3] City News Service, "San Diego to develop Regional Cyber Innovation Center to prevent attacks," 10 News San Diego, October 6, 2021, https://bit.ly/2ZN3PkT.

[4] Mike Elfland, "Hacker accessed medical info of thousands in email breach at UMass Memorial Health," *Telegram & Gazette,* October 28, 2021, https://bit.ly/3mELiQw.

[5] State of Alaska Department of Health and Social Services, "Cyberattack on DHSS website includes HIPAA and APIPA breach," news release, September 16, 2021, https://bit.ly/3my1CBt.

[6] Rachel Keller, "Parents furious after personal information is leaked in 2nd data breach in online program for family members with disabilities," ABC 8News, October 8, 2021, https://bit.ly/3q2nHeJ.

[7] SecureLink, "44% of Healthcare and Pharmaceutical Organizations Have Experienced a Data Breach Caused By a Third Party in the Last 12 Months," news release, October 22, 2021, https://bit.ly/3wc91e4.