COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 1. January 09, 2020 Privacy Briefs: January 2020

By Jane Anderson

◆ **A cybersecurity breach temporarily halted cancer radiation treatment services at the Cancer Center of Hawaii on Oahu,[1] the center said.** The center, which provides radiation treatment for cancer patients at two locations—Pali Momi Medical Center and St. Francis Healthcare System's hospital campus in Liliha—confirmed in December that it experienced a computer network hack on Nov. 5. In response, the center shut down its network servers, which temporarily prevented it from being able to offer radiation services to its patients. The center said it was able to retrieve all essential patient treatment information from its radiation machines and restore its network to full operation, but it did not say how long the system was disabled or how long radiation treatment was suspended. No patient data was compromised during the incident, the center said.

◆ **Minnesota Gov. Tim Walz (D) plans to propose legislation this year to tighten computer security at health insurers in the state, following revelations that Blue Cross and Blue Shield of Minnesota allowed hundreds of thousands of serious cybersecurity vulnerabilities to collect on its computer systems over a period of years,** the *Star Tribune* reports.[2] The announcement comes after the newspaper revealed that "Minnesota Blue Cross, the state's largest health insurer, is working to eliminate as many of the 200,000 critical or severe cybersecurity vulnerabilities on its network servers as it can, following sharp prodding by a whistleblower." The not-for-profit insurer told the newspaper that customers' protected information is secure, and that it complies with existing legal requirements for data privacy and security. The proposal would give the state's Commerce Department the power to investigate cybersecurity precautions and breaches at insurance companies. It also would create a requirement that insurers notify the office when they experience a breach.

◆ **Some of the nation's top health care–focused venture capital firms are banding together to form an advisory council with the technology security certification provider HITRUST** to create best practices for data security for start-ups that are developing digital health technologies.[3] The conversations, spearheaded by investment fund Frist Cressey Ventures, based in Nashville, Tennessee, "were designed to accelerate the adoption of digital technologies throughout the health care industry," according to a story by *TechCrunch*. Investors include Ascension Ventures, Bain Capital and Echo Health Ventures, among others. The idea is to protect venture capital's investments in health care startups, which can be particularly vulnerable to data breaches and lax security practices.

◆ **The Philadelphia Public Health Department concluded that the medical records of thousands of city residents with positive hepatitis test results were not compromised** after a reporter for the *Philadelphia Inquirer* found the test results on a public data tool built by the health department in October.[4] The reporter found the results shortly after the hepatitis records were posted and notified the health department, which deleted them within minutes. Therefore, "there was no risk to confidentiality," and patients will not be notified, according to a health department spokesperson. The exposure was an "oversight by an employee" who did not understand that the posted data contained personally identifiable information, the spokesperson said. The records were part of a database built by the department to track hepatitis infections in aggregate, rather than individual cases. However, the health department receives records with personally identifiable information from health care providers around Philadelphia. The information wasn't removed before the data was uploaded to Tableau, a tool for publishing databases online.

◆ **Truman Medical Centers in Kansas City suffered a data breach Dec. 5 involving more than 114,400 patients when a company laptop was stolen from an employee's vehicle.**[5] The laptop was password-protected, and a hospital spokesperson said that the odds of an unauthorized party being able to crack the password and view patient data were slim. However, the spokesperson said, the hospital will offer credit monitoring to patients concerned about the laptop theft. This was the second data security incident in four months at Truman, which agreed earlier in 2019 to pay a small undisclosed sum to unlock its computer system following a ransomware attack. Patients' personal health and financial information was kept on a different system and was not affected by that attack, the hospital said.

◆ **A "curious" hospital employee in Grand Haven, Michigan, accessed the records of 4,013 patients at North Ottawa Community Health System between May 2016 and October 2019**,[6] the hospital system said. Another employee reported concerns on Oct. 15, 2019, and the hospital launched an internal investigation on Oct. 17. The internal investigation concluded that thousands of electronic health records had been accessed, seemingly at random. According to an *MLive* report, "the employee, whose access to digital records was suspended during the investigation, was terminated." The hospital said there was no evidence suggesting that patient information had been shared or used inappropriately. The North Ottawa Community Health System includes a hospital, hospice services, long-term care, urgent care and emergency medical services, but only hospital patients were affected by the breach. Only some patients' Social Security numbers were viewed, and those patients will receive free credit and identity theft monitoring for one year. See the details at https://bit.ly/2QI6Jix

◆ **Cheyenne Regional Medical Center in Wyoming experienced a data breach involving employee emails that may have compromised some patient information.**[7] The medical center became aware of the breach April 12, when there was "suspicious activity" with some employee payroll accounts, a spokesperson said. "The data breach was due to a phishing scam that compromised employee email credentials," and there is no evidence suggesting patient information was misused due to the breach, which likely lasted from March 27 to April 8. It took the hospital until late November to identify patients whose personal information was contained in compromised emails, and the hospital intends to notify them. A forensic team hired to determine the extent of the breach reported that the emails may have contained names, dates of birth, Social Security numbers, driver's license numbers, dates of service, provider names, medical record numbers, patient identification numbers, medical information, diagnoses, treatment information, health insurance information, and for a small number of individuals, credit card information and/or financial account information.

◆ **CMS temporarily shut down access to its Blue Button 2.0 data-sharing tool after officials discovered a bug that may have exposed some beneficiary information.** CMS suspended access to the Blue Button 2.0 API after a third-party app developer reported a "data anomaly" on Dec. 4. It's unclear when the service, which allows Medicare beneficiaries to share their claims data with third-party apps, will be restored, the agency said in a blog post.[8]

◆ **Kalispell Regional Healthcare patients filed a second lawsuit against the northwest Montana health system following a data breach that may have compromised protected information for up to 130,000 patients.**[9] One of the plaintiffs in the lawsuit, filed Dec. 24, says she experienced unauthorized charges on her financial accounts, and she believes those charges were incurred as a result of the data breach. The breach itself, which involved a phishing attack, took place in May, although Kalispell Regional Healthcare did not announce the incident until October. The hospital said it "was not aware of the extent of the attack until an outside forensic firm completed a review." The first lawsuit was filed in November. Both lawsuits claim the hospital violated the Montana Uniform Health Care Information Act,[10] which states a victim of a breach can seek damages from the health care provider if the provider is found to be in violation of the act.

◆ **Human services agency Equinox, based in Albany, New York, learned of a data breach that may affect the protected health information of more than 1,000 current and former clients.**[11] The agency reported in December that staff discovered unusual activity within the company's systems on July 26. They hired independent cybersecurity firm CyberScout to investigate, and CyberScout reported in August that "it had found evidence that hackers had gained access into two email accounts belonging to Equinox employees. Equinox then hired data review experts to determine if the accessed email accounts contained any protected health information." On Oct. 9, the company was told the email accounts did contain some PHI. Information that potentially was accessed included names, addresses, dates of birth and Social Security numbers, as well as information on medical treatment or diagnoses, medication and health insurance. Equinox has notified all affected clients and is offering free credit-monitoring services to affected individuals.

[1] Eleni Gill, "Cyber Attack Halts Radiation Treatment By Oahu Cancer Center,"*Honolulu Civil Beat*, December 11, 2019, https://bit.ly/2ZPeLdv.
[2] Joe Carlson, "New data-privacy law proposed for Minnesota insurers," *Star Tribune*, December 20, 2019, http://strib.mn/2rSM03b.
[3] Jonathan Shieber, Healthcare-focused venture firms are forming a best practices group for securing health data," *TechCrunch*, December 10, 2019, https://tcrn.ch/2MT5pIu.
[4] Nathaniel Lash, "Philadelphia hepatitis data exposure posed 'no risk to confidentiality' because of Inquirer notification, city says," *The Philadelphia Inquirer*, December 20, 2019, https://bit.ly/2ZNIx2p.
[5] Lily Lieberman, "Stolen Truman Medical Center laptop holds 114,400 patients' health data,"*Kansas City Business Journal*, December 18, 2019, https://bit.ly/2ZQxiX6.
[6] Anya van Wagtendonk, "'Curious' hospital employee improperly accessed thousands of medical records," *MLive*, December 17, 2019, http://bit.ly/2sRBERx.
[7] Wyoming News Exchange, "Data breach may have compromised patient info," *Gillette News Record*, December 12, 2019, https://bit.ly/2ZQdVNJ.
[8] Kaiser Health News, "CMS Shuts Down Medicare Tool Following Discovery Of Bug That May Have Exposed Consumers' Data," *KHN Morning Briefing*, blog, December 20, 2019, https://bit.ly/2QnNzj9.
[9] Seaborn Larson, "Kalispell hospital faces second lawsuit over data breach,"*Missoulian*, January 2, 2020, https://bit.ly/2ZM9PpV.
[10] 50 M.C.A. § 16.500-16.553.
[11] Bethany Bump, "1,000 former, current Equinox clients affected by data breach," *Times Union*, December 6, 2019, https://bit.ly/35lgh8y.