Report on Patient Privacy Volume 21, Number 2. February 04, 2021 Privacy Briefs: February 2021

By Jane Anderson

◆ **The Florida Healthy Kids Corporation (FHKC), a Medicaid managed care plan, said one of its vendors, Jelly Bean Communications Design, experienced a security incident spanning seven years that involved "several thousand" Medicaid applicants.** Jelly Bean Communications was responsible for hosting the Florida Healthy Kids website during the hacking incident, the managed care company said. "FHKC was notified on December 9, 2020, that several thousand applicant addresses had been inappropriately accessed and tampered with," said a statement from the managed care company. "These addresses are collected as part of the online Florida KidCare application." There is no evidence that any applicant's personal information was removed from the system, according to FHKC. After an independent investigation, "cybersecurity experts identified significant vulnerabilities in the hosted website platform and the databases that support the online Florida KidCare application," the company said. "FHKC learned that these vulnerabilities spanned a seven-year period from November 2013 until December 2020. FHKC temporarily shut down the website and databases in December 2020." The types of information that may have been exposed included full names, dates of birth, email addresses, phone numbers, addresses, Social Security numbers, financial information and secondary insurance information.[1]

◆ **Ramsey County in Minnesota, part of the Minneapolis-St. Paul metro area, has notified 8,700 clients of its Family Health Division that their data may have been accessed on or around Dec. 2 as part of a ransomware incident.** Netgain Technology LLC, a vendor that provides technology services to Ramsey County, advised the county that its security had been breached by a hacker seeking to extort payment through a ransomware scheme. Upon learning of the incident, Ramsey County said it suspended all use of Netgain's application, moved to manual backup procedures, and performed an extensive technical analysis of possible exposure of its clients' data. According to the notices sent to clients, Netgain determined that the ransomware incident affected data within an application used by Ramsey County's Family Health Division to document home visits. Information that may have been exposed in the incident included names, addresses, dates of birth, dates of service, telephone numbers, account numbers, health insurance information and medical information. For a small number of individuals, it may also have included a Social Security number. St. Cloud-based Netgain has offices and data centers in Chicago, Minneapolis, San Diego and Phoenix, and the company serves accounting firms and health care providers.[2]

◆ **Connecticut lawmakers are considering legislation that would update and strengthen the state's data breach notification statute.** The legislation, sought by Connecticut Attorney General William Tong, would broaden the definition of "personal information" to include additional categories such as medical information, online account information, passport numbers, military identification and health insurance account numbers.[3] The bill also would shorten the deadlines for entities to notify individuals and the attorney general of a data breach from 90 days to 60 days, which Tong's office said is in line with other states. "In 2005, the Connecticut General Assembly passed one of our nation's first laws protecting consumers from online data breaches, and in doing so, made our state a national leader in data privacy," Tong said Jan. 28 in testimony before the state legislative General Law Committee. "Since then, as technology and our understanding of the risks associated with living in an online world have evolved, dozens of other states passed and updated their own data breach laws to keep up

with that evolution. In 2019 alone, nine states passed new and expanded data breach notification laws and in 2020, six states passed privacy-related legislation. This underscores the importance of updating our statute; it is time for Connecticut to catch up," Tong said.[4]

◆ **Easy Healthcare Corp. unlawfully shared user data, including personal information and location data, from its fertility tracking app Premom with third-party data collection companies**, according to a proposed class-action lawsuit filed Jan. 21 in the U.S. District Court for the Northern District of Illinois. The distribution of users' personal information and location data is an alleged violation of the app's own terms of service and privacy policy, the plaintiff, identified only as "Jane Doe," told the court in the lawsuit.[5] The app allegedly was collecting a broad swath of data about its users and sharing it without their permission with three Chinese companies focused on advertising, according to research from the International Digital Accountability Council, a nonprofit that monitors and works with apps and developers to protect consumer privacy. In August, the council sent letters to the Federal Trade Commission and the attorney general of Illinois, where Premom is headquartered, alleging the data sharing was deceptive and potentially ran afoul of federal and state law. Still, there was no evidence Premom was transmitting health data to third parties, according to the council.[6]

◆ **Hackers didn't steal as much personal information in 2020 as in previous years, but they used the information to profit in new, more lucrative ways, according to a report from the Identity Theft Resource Center.** Significant trends noted in the report include a drop in the number of data breaches, coupled with a drop in the number of individuals affected, and a shift away from mass attacks seeking consumer information and toward attacks that target businesses using stolen logins and passwords. "Increased online shopping and remote work as a result of the response to COVID-19 dramatically increased the threat landscape that could lead to a data breach," but the number of data breaches did not increase, and the number of individuals affected did not grow, the report said. Instead, "ransomware and phishing attacks directed at organizations are now the preferred method of data theft by cyberthieves," the report said. "These attacks generally require only a stolen credential or for an employee to click on a link in an unsolicited email, text, or social media account. Ransomware and phishing require less effort, are largely automated, and generate payouts that are much higher than taking over the accounts of individuals. One ransomware attack can generate as much revenue in minutes as hundreds of individual identity theft attempts over months or years." The average ransomware payout was $233,000 per event in the fourth quarter of 2020, up more than 23-fold since the average $10,000 in the third quarter of 2018, the report said.[7]

◆ **The guardian of a patient whose personal information was disclosed in the 2020 Blackbaud data breach sued San Diego-based Rady Children's Hospital Jan. 20 in a potential class-action lawsuit.** The lawsuit, filed in the U.S. District Court for the Southern District of California, stated that Rady Children's "announced a second data breach within this year involving the private medical information of approximately 19,788 of its patients disclosed to and viewed by an unauthorized party between February 7, 2020 and June 4, 2020. The medical information included highly valuable and protected information including patient names, addresses, dates of birth, the names of patients' physicians, and the department the patients were admitted to." The lawsuit alleged that "plaintiff and the other Class Members' Private Information is now at risk because of Defendant's negligent conduct and unfair acts and practices," and added that "this is not the first time Defendant has failed to reasonably protect and preserve the confidentiality of medical information of its patients. Defendant was previously investigated by the California Department of Public Health for a four separate reported disclosures of unencrypted patient data of 20,421 of its patients between June 16, 2014 and July 25, 2015." This investigation resulted in penalties from the California Department of Public Health, the lawsuit noted. Another data security incident involved "the radiology-related information of 2,360 patients" between June 2019 and January 2020, and is the subject of a separate class-action lawsuit.[8]

1 Florida Healthy Kids Corporation, "Florida Healthy Kids Announces Cybersecurity Incident," news release, accessed January 31, 2021, https://bit.ly/3j4zDr1.
2 Deanna Weniger, "Ramsey County Says Illegal Ransomware Hack Compromised Info of 8,700 Clients," *St. Paul Pioneer Press*, January 29, 2021, https://bit.ly/3pAl8xt.
3 Attorney General William Tong, "House Bill 5310, An Act Concerning Data Privacy Breaches," accessed February 1, 2021, https://bit.ly/3tdnFjm.
4 Office of the Connecticut Attorney General William Tong, "Attorney General Tong Seeks Update to Price Gouging and Data Breach Notification Statutes," news release, January 28, 2021, https://bit.ly/39zrozV.
5 Porter Wells, "Premom Sued for Allegedly Sharing Fertility App User Data Abroad," Bloomberg Law, January 22, 2021, https://bit.ly/3j3GGjo.
6 Tonya Riley, "A popular fertility app shared data without user consent, researchers say," *The Washington Post*, August 20, 2020, https://wapo.st/2McKOlv.
7 Identity Theft Resource Center, *2020 in Review: Data Breach Report*, accessed January 28, 2021, https://bit.ly/39zN0wb.
8 John Doe v. Rady Children's Hospital-San Diego, Case No. 21CV0114 JM, January 20, 2021, https://bit.ly/36KPF4r.