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]