COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 7. July 10, 2019
Privacy Briefs: July 2019

By Jane Anderson

◆ **The Food and Drug Administration is warning patients and health care providers about cyberthreats from using certain Medtronic insulin pumps, which have been recalled.** Security researchers found vulnerabilities in some Medtronic MiniMed insulin pumps that could enable unauthorized users to connect wirelessly to a nearby pump. This could allow a hacker to alter or stop the insulin delivered to the patient. The specific pumps recalled were Medtronic's MiniMed 508 and the MiniMed Paradigm series insulin pumps. Medtronic wrote in a letter to users that it recommended switching to a different type of insulin pump. In addition, it recommended taking additional security steps, including making sure all devices related to the pump were kept in patients' sight at all times, and monitoring blood sugar levels closely. Read more at https://bit.ly/2L4Ftug.

◆ **The health care industry does not have an accurate picture of the sensitive data it acquires, maintains and transmits, according to the results of a survey conducted by Integris Software.** The survey of business executives and IT decision makers at mid- to large-sized companies found that most organizations expressed overconfidence in their technical maturity. Despite the health care industry's history of stringent privacy regulations, it has the second-largest number of cybersecurity breaches when measured across industries, and the highest exposure per breach in 2018, the survey found. More than half of respondents said they needed to access 50 or more data sources to get a defensible picture of where their sensitive data resides, the survey found, even though 70% of respondents said they were "very" or "extremely" confident in knowing where sensitive data resides. Access the survey at https://bit.ly/2YLyYjj.

◆ **An online database of more than 5 million records apparently belonging to the website MedicareSupplement.com was left open and accessible to the public, according to UK-based security firm Comparitech Limited.** The database appeared to be part of the website's marketing leads database, Comparitech says. Records exposed contained full names and addresses, email addresses, dates of birth, genders, and marketing-related information. Around 239,000 records also indicated interest in a particular area of insurance —for example, cancer insurance. Data was spread around several categories, including life, auto, medical and supplemental insurance. The IP address of the database first was accessed on May 10 by public search engine BinaryEdge. MedicareSupplement.com disabled access as soon as it was notified. Get the details from Comparitech at https://bit.ly/2XzGqN2.