Healthcare Cybersecurity Concerns During COVID-19

by Tesch West

Cybersecurity is a continual concern in the healthcare space. Hospitals are particularly vulnerable due to complex systems and medical devices that offer multiple entry points for cybercriminals to exploit. In the past four years, 1,500 healthcare entities have been attacked by ransomware designed to prevent access to critical systems in order to extort payment. Studies estimate that the attacks affected 6.6 million patients and cost $157 million. The majority of attacks (74%) targeted hospitals or clinics. In October 2019, the Food and Drug Administration (FDA) warned healthcare providers about a set of 11 cybersecurity vulnerabilities that may pose risks for certain medical devices and hospital networks.

Unfortunately, as with so many things, cybersecurity issues have been exacerbated in 2020 by the COVID-19 pandemic. Crowded hospital emergency rooms and ICUs are particularly vulnerable. In February, a California hospital paid a $17,000 bitcoin ransom to unlock its data following an attack. In April, a nonprofit critical access hospital in Colorado lost access to 5 years of medical records when its database was infected with ransomware. As of June 16, the hospital had not paid the ransom and continues to attempt to regain access. In March, a Kentucky Hospital was attacked but was able to rely on backup systems to restore operations. This trend has escalated to the point where Interpol issued an alert this past April to all 194 member countries warning that cybercriminals are targeting healthcare organizations (hospitals in particular).

Concerns related to cybersecurity also extend to medical devices. On March 3, 2020, the FDA warned that cybersecurity vulnerabilities may allow an unauthorized user to wirelessly crash, tamper with, or access functions of certain Bluetooth-enabled medical devices. Examples of vulnerable devices include pacemakers, blood glucose monitors, and insulin pumps.

This is not the first time the FDA has issued cybersecurity warnings about insulin pumps. Insulin pumps are used by people with type 1 and type 2 diabetes to deliver insulin continuously throughout the day and in anticipation of meals. Insulin pumps work by using wireless radio frequencies to communicate with other devices, such as blood glucose monitors and glucose sensor transmitters. The pumps also come with remote controls that allow caregivers or medical professionals to administer medication from a short distance.

On June 27, 2019, the FDA alerted healthcare providers to a recall of 11 Medtronic MiniMed insulin pump models due to cybersecurity risks. The recall was prompted by security vulnerabilities that would allow an unauthorized person to wirelessly connect to a nearby MiniMed insulin pump and change the settings. The unauthorized user could over-deliver insulin to a patient, leading to unconsciousness and severe hypoglycemia; or stop insulin delivery, leading to a coma from high blood sugar and diabetic ketoacidosis. Such interference with the pump could be life-threatening.

Medtronic was first made aware of potential issues in late 2011 when concerns were raised that the pump's radio frequencies were not encrypted. In August 2018, two researchers gave a widely publicized talk attempting to raise awareness about the issue. Then, in 2019, a research group demonstrated to the FDA a

proof of concept smartphone app that could override the insulin pump's settings and repeatedly give a patient doses of insulin or withhold insulin. Medtronic issued the recall a week later.

The FDA's 2019 recall was likely the first time a medical device has been recalled because of a cybersecurity risk. However, it is unlikely to be the last. The FDA's 2020 cybersecurity warning stresses that connected medical devices have inherent risks, and software to exploit these vulnerabilities is publicly available.

Cybersecurity in this context is important not only for the wearers of medical devices and hospital healthcare professionals and patients, but also for those designing our interconnected cities and communities of the future. When we consider the "Internet of Things," we think about smart phones, laptops, billing systems, traffic sensors, and parking meters; we don't often think about healthcare or the host of devices that also depend on a smart and secure system.

In February, a California hospital paid a $17,000 bitcoin ransom to unlock its data following an attack.

Sources:

https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0

https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities

https://www.bankinfosecurity.com/hospital-ransomware-attacks-surge-so-now-what-a-8987

https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/

https://www.healthcaredive.com/news/hospitals-clinics-most-likely-to-be-hit-with-ransomware-attack/572091/

https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/

https://www.healthcareitnews.com/news/ransomware-attack-leaves-5-years-patient-records-inaccessible-co-hospital

https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0

https://www.npr.org/2020/01/07/794144007/hospitals-are-encouraged-to-do-more-to-avoid-medical-device-hacking

https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware

https://www.medtechdive.com/news/coronavirus-chaos-ripe-for-hackers-to-exploit-medical-device-vulnerabilitie/575717/

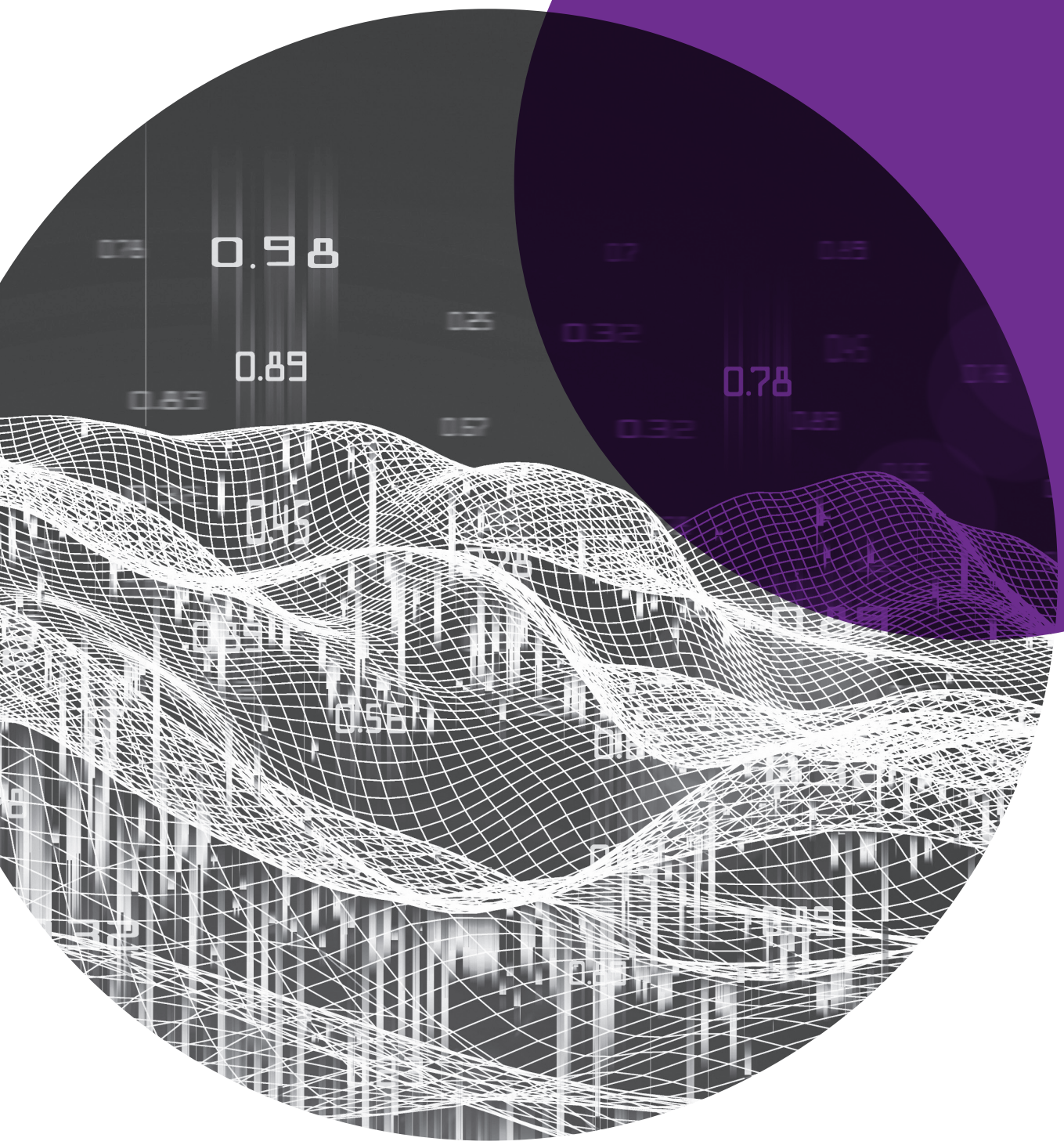
https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication

https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice11-letter

https://www.lexology.com/library/detail.aspx?g=14ebf748-6468-45b5-bdf3-3a59baa105b1&utm_source=lexology+daily+newsfeed&utm_medium=html+email&utm_campaign=ahla+subscriber+daily+feed&utm_content=lexology+daily+newsfeed+2019-07-09&utm_term=

https://essentialhospitals.org/quality/fda-announces-medtronic-insulin-pump-recall/

https://www.wired.com/story/medtronic-insulin-pump-hack-app/



Tesch West is an associate in Dentons Health Care practice and a resident of the New York office. Tesch's practice focuses on helping clients navigate a variety of federal and state regulatory issues, including Medicare, Medicaid, and Medicaid managed care coverage, compliance and reimbursement issues. She regularly represents hospitals, clinics, nursing homes, physician groups, health plans and associations. A member of the Environment, Health & Safety Pillar of the Dentons Smart Cities & Connected Communities Think Tank, she writes frequently on issues at the intersection of technology and healthcare. She also was the recipient of the American Cancer Society Cancer Action Network's Judicial Advocacy Initiative award.