ECKERT SEAMANS ATTORNEYS AT LAW

September 19, 2022

Data Security & Privacy Alert

# FBI Tips to Protect Against Cyber Threats to Medical Devices

By Matthew H. Meade, Sandra R. Mihok and Laura Decker

According to last week's Federal Bureau of Investigation (FBI) notification, cyber-industry experts are observing an uptick in cyber-attacks targeting medical devices. A recent report conducted by a health care cyber security analyst determined that insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers, and intrathecal pain pumps are at most risk. Compromise to medical devices by cyber threat actors can impact the operations of health care facilities and cause patient safety issues, including drug overdoses, inaccurate readings, and other hazards to patient health.

Threat actors perpetrate these attacks by exploiting vulnerabilities in hardware design and software management. Although medical device hardware is often designed to remain in place and functional for 10 to 30 years, its software runs on a lifecycle determined by the device manufacturer. Unless regularly patched and updated to defend against emerging vulnerabilities, these devices can become susceptible to an attack. The FBI has identified the following additional vulnerabilities related to medical devices:

- Devices used with the manufacturer's default configuration are often easily exploitable by cyber threat actors.
- Devices with customized software, which require special upgrading and patching procedures, are often delayed with vulnerability patching.
- Certain devices were not initially designed with security in mind, due to a presumption of not being exposed to security threats.

The FBI recommends that businesses implement the following practices to strengthen security for medical devices, identify and resolve vulnerabilities, and increase awareness on security issues for employees:

- Antivirus software, complex passwords and limited numbers of login attempts per user
- Vendor-developed software components, operating systems versions, and model numbers for all medical devices and software to identify the need for updates or patching
- Process for monitoring and reviewing software vulnerability disclosures from applicable medical providers as well as conducting vulnerability assessments independently
- Additional required trainings related to targeted cyber-attacks initiated through phishing, social engineering, and other means

If you experience an incident involving unauthorized access to a medical device, the Data Privacy and Security team at Eckert Seamans is prepared to assist you with understanding whether you have notification obligations under state or federal law. Please contact us to discuss your options.

ECKERT SEAMANS ATTORNEYS AT LAW