PUBLICATION

Mitigating Cyber Vulnerabilities in Medical Devices

Authors: Alisa L. Chestler
September 16, 2022

Earlier this week, the Federal Bureau of Investigation (FBI) published another notification alerting health care providers of increasing cyber threats to medical devices operating on unpatched or outdated devices. In its notification, the FBI detailed specific threats and provided recommendations for health care providers to mitigate the risk posed by legacy medical devices.

Medical devices are built for long-term use. In many cases, the hardware remains in service for decades, with many devices exceeding 30 years of usage. However, operating systems and software packages running on medical devices are not designed for such a lengthy lifespan. Once software manufacturers sunset a program, they no longer provide updates or support. That leaves the devices still running these types of legacy software especially vulnerable to cyberattacks and an easy entry point for malicious acts.

Health care providers of all sizes continue to utilize risky practices including the use of default configurations and passwords, connecting stand-alone devices to the internet, and failure to apply patches to devices in a timely manner.

Legacy systems combined with poor cybersecurity practices have resulted in 53 percent of connected medical devices in hospitals having known critical vulnerabilities. Medical devices assessed to be most susceptible to cyberattacks are insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers, and intrathecal pain pumps.

The FBI recommends health care providers consider the following actions to improve medical device security, identify critical vulnerabilities, and to educate their employees on risks:

- **Endpoint Protection** – Utilize antivirus software, encrypt device data, and utilize endpoint detection and response (EDR) solutions
- **Identity and Access Management** – Use complex passwords unique to each device and never use the default password
- **Asset Management** – Maintain an accurate inventory of all medical devices and associated software; monitor all manufacturer-issued patches and updates for those devices and apply them immediately
- **Vulnerability Management** – Implement a routine vulnerability scan prior connecting a new medical device to the network; monitor and review all software vulnerability disclosures from device manufacturers
- **Education** – Train employees to identify insider threats, phishing and social engineering attacks, and business email compromise seeking their credentials

Health care providers increasingly face an onslaught of cyberattacks targeting vulnerabilities across their networks. According to one report, 89 percent of health care providers experienced at least one cyberattack in the past year alone. Legacy and unpatched medical devices pose a unique and significant risk that can have dire consequences for providers and their patients.

We recommend considering a clear policy and procedure for medical devices and the development of a strategic plan on handling the use of older devices, especially those that are not able to meet current remediation expectations.

If you have any questions about cybersecurity risks to medical devices, please contact Alisa L. Chestler or a member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Group.