Ensuring a solid medical device cybersecurity program

Briefings on HIPAA
by Gerry Blass

August 27, 2018

Did you know that medical devices can have an average of 6.2 distinct vulnerabilities?

Unenforced password protocols, outdated data storage, unencrypted data, unsecured access to networks—these are just a few examples. This is significant because medical devices do not typically incorporate the same type of encryption as other technologies or healthcare IT systems, and they are extremely attractive to attackers as direct paths to a health system's entire network.

In the digital age of healthcare delivery, the need for appropriate medical device cybersecurity is pervasive. Networked devices that collect, examine, or store patient data, such as MRI machines and vital signs monitors, can provide access points into a health system's network, where attackers can cause device malfunction, hold patient data hostage, or take down an entire system, ultimately endangering patient care and safety.

Organizations want to get the most life possible—sometimes 20 years or more—from the devices they purchase. As a result, many medical devices in use are at or near end of life, and many were manufactured before security measures were built in.

At this late-stage life cycle, manufacturers do not typically provide ongoing support, which means patches, upgrades, or other means of protecting these devices are unavailable.

Healthcare organizations must work diligently to protect sensitive data and their patients by implementing and enforcing a solid medical device cybersecurity program.

Industry perspective: How a federal agency is addressing the problem

The FDA is "modernizing measures to improve the safety of medical devices while continuing to create more efficient pathways to bring lifesaving devices to patients."

In its recently released "Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health," the FDA outlines five steps it will take to encourage medical device innovation for improved safety, earlier risk detection, and a better-informed public:

5 STEPS

1. Establish a robust medical device patient safety net in the United States
2. Explore regulatory options to streamline and modernize timely implementation of postmarket mitigations
3. Spur innovation toward safer medical devices
4. Advance medical device cybersecurity
5. Integrate the Center for Devices and Radiological Health's premarket and postmarket offices and activities to advance the use of a "total product life cycle" approach to device safety

These five steps are meant to redefine and reorganize the FDA's approach to the oversight of medical device security throughout a product's life cycle.

Individual perspective: Using a medical device security assessment to build and enforce protocols

In addition to the FDA's broader action plan to address the security of medical devices across the healthcare industry, every organization must develop its own strategy to protect medical devices from potential attacks.

Here are six steps organizations can take now.

Editor's note:

Blass has more than 35 years of experience in healthcare information technology. In 2002, he founded ComplyAssistant to provide software and service solutions for HIPAA and IT strategic planning. As the former chief information security officer for a major health system in New Jersey, Blass built its HIPAA privacy and security programs and chaired its multidisciplinary governance team. He currently chairs the New Jersey HIMSS Privacy, Security and Compliance Committee and is the founder of and content contributor to HIPAA 411, a LinkedIn group for sharing information on HIPAA and HITECH. Blass is an active member and presents at industry association events with HIMSS, HFMA, AITP, NCHICA, NJPCA, NJAMHAA, and HCCA.

Related Topics:
HIM/HIPAA, HIPAA

1. Set up IT and compliance teams to work in collaboration with each other. The IT team is responsible for monitoring all medical devices in addition to escalating any issues or breaches to the compliance team. In turn, compliance is responsible for monitoring and addressing the organization's information security and risk management programs. Together, these departments are the core of security and compliance, and they need to be incentivized to collaborate on how best to protect the organization and its patients. Further, to avoid any conflicts of interest or potential internal political pressures between these two teams, the organization's chief information security officer should be housed outside of the IT department.

2. Complete an administrative assessment on every vendor that provides medical devices to the organization. A governance, risk, and compliance (GRC) management vendor or solution can assist with the administrative assessment, using a comprehensive questionnaire focused on the areas listed above. A GRC partner can also rate each medical device vendor and determine levels of risk. An administrative assessment must evaluate each vendor's medical device cybersecurity practices, including:
   - Documentation of HIPAA security rules
   - How data is stored and the usage of data centers
   - Use and enforcement of unique user IDs and passwords
   - Security certifications or validations from independent parties such as Service Organization Control (SOC) audits, HITRUST, or the National Institute of Standards and Technology (NIST)
   - Remote access protocols
   - Documentation and enforcement of policies for data retention, disposal, and destruction
   - Documentation of disaster recovery plans and procedures
   - Continuation of liability insurance
   - Post-sale support on the medical device—whether by the vendor or by a third party
   - Controls on physical security of the device itself

3. Complete a technical assessment on each device. A technical assessment evaluates each device to ensure it meets the technical and operational requirements of HIPAA, NIST 800-53, and FDA postmarket guidance for medical device cybersecurity. The assessment should include penetration testing, a vulnerability assessment, medical device monitoring, and breach detection as part of a holistic solution.

4. Review and update related business associate agreements (BAA). If the healthcare organization is still using legacy medical devices, it is likely that the related BAAs may be outdated. Take time to review each BAA and update per the organization's most recent medical device cybersecurity protocols. Get the compliance team involved if needed to perform any medical device security assessments and confirm that the device manufacturers have adequate cyber insurance.

5. Document and require role-based usage of medical devices throughout the system. Each medical device must only be accessed by approved clinical and technical staff. Limit access to any authorized clinician caring for the patient and authorized IT personnel who maintain the devices. Some systems even enforce a "no exceptions" policy where personnel can be terminated for breaches of policy—including accessing unapproved medical devices or sharing passwords.

6. Join an Information Sharing and Analysis Organization (ISAO). Healthcare organizations learn clinical best practices by sharing information with each other. Apply the same approach to medical device cybersecurity and risk management. Joining an ISAO provides healthcare organizations with ongoing access to threat intelligence, vulnerability disclosure, and community-based best practices and support. Medical device vendors also join various ISAOs to share their risk profiles and reduce their own medical device cybersecurity liabilities.

Healthcare is a primary target for attack due to mass migration from hard-copy to electronic health data and the high value of health and financial data. Medical devices are appealing vectors for attackers who aim to access this valuable information. While medical device cybersecurity has become critical in this age of digital health, there are actions health systems can take to protect their data—and their patients. Evaluate vendors and their devices, protect access to the devices following implementation, and have escalation procedures in place for any security events. These measures will further protect your organization from attack through a connected medical device.