Guidehouse

Mitigating Cyber Risks for Medical Devices in a Connected World

Connected medical devices have the potential to create more vulnerabilities via novel vectors for bad actors. Meeting this challenge requires a different approach to security.

The average US hospital room contains an estimated 15 to 20 connected medical devices.[1] Those numbers are rising due to the accelerated adoption of internet-connected devices to reduce costs for health systems, provide better care to patients, and save clinician time.

Connected devices, which are used by pharmacology, oncology, radiology, neurology, surgery, and other departments, perform essential monitoring tasks. IV pumps, wearable biosensors, connected thermometers, ECG monitors, and other innovative, useful medical devices are essential to quality care delivery. However, there are mounting concerns about their safety. In 2019, 82% of healthcare organizations experienced an IoT-focused cyberattack.[2] And as many as 53% of medical and IoT devices and 73% of IV pumps in hospitals have known critical vulnerabilities. [3]

Connected medical devices provide an opportunity for bad actors to intercept data, hijack the device, infiltrate a network, or plant malware or ransomware. In 2019, a ransomware attack disabled patient monitors for days at a Georgia Medical Center significantly affecting patient care. A lawsuit alleges that those disabled monitoring devices contributed to the death of an infant being delivered at the center.

Healthcare providers must proactively secure connected medical devices to prevent negative potential patient outcomes and other impacts to the delivery of care. It's critical to protect both healthcare providers and patients by implementing supply chain risk management practices, following FDA guidelines on procuring and managing connected medical devices, conducting cyber program capability assessments, implementing asset intelligence, creating and documenting better policies and processes, automating updates and patching, ensuring proper network segmentation, automating device isolation, and more.

Assess the Current Situation

It's essential for healthcare organizations to ensure they are following all FDA recommendations and guidelines for protecting devices. This includes updating procurement guidelines for medical devices to take into account potential cybersecurity risks, as well as working with manufacturers over the device life cycle. The latter is a vital part of making sure devices are maintained and regularly updated with patches as new vulnerabilities emerge.

[1] Healthcare Cybersecurity for Connected Medical Devices - businessnewsdaily.com

[2] 82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds

[3] Report: Fifty-three Percent of Connected Medical Devices Have a Vulnerability | Healthcare Innovation

The FDA and Connected Medial Devices

The FDA helps secure medical devices by providing the following:

- Guidance to manufacturers on the design and maintenance of secure devices
- Requirements for manufacturers to monitor, assess, and disclose vulnerabilities
- "Safety communications" about identified vulnerabilities
- Security recommendations to patients and healthcare providers
- White papers and thought leadership on improved security

Healthcare organizations should also conduct a cyber program capability assessment to understand and baseline their organization's asset intelligence capabilities and processes. This will help organizations understand the current state of their ability to identify, protect, detect, respond, and recover from threats or breaches to connected medical devices. It will also identify areas where capabilities and processes need to be improved to boost ongoing security and incident response.

Create Processes and Policies

Creating effective cybersecurity processes and policies to protect against connected medical device vulnerabilities starts by bringing together the right stakeholders. This often includes the chief medical information officer, biomedical teams, finance/purchasing teams, IT staff, and cybersecurity professionals. These key stakeholders must then work together to create processes and policies that are informed by appropriate risk management procedures and address all potential vulnerabilities throughout the device life cycle.

First, healthcare providers should create processes and policies to ensure they're following the FDA's advice on procuring connected medical devices.[4] The FDA recommends things like building the cost of mitigating device vulnerabilities into the purchase price or maintenance fees, having extra devices available in the event of an incident, setting clear expectations for vulnerability management, and outlining supplier responsibilities during incident response and recovery.

Organizations should also request a software bill of materials from manufacturers to identify vulnerable components in order to conduct supply chain risk management and better understand potential vulnerabilities and risks. Additional supply chain illumination research could also be appropriate depending on the risks of a particular device.

Creating better policies and processes for integrating medical devices into a health organization's network in a secure way, managing devices effectively, and responding to a cyberattack or breach are also critical. Doing these things well involves collaboration between device manufacturers, IT, cybersecurity professionals, and others.

Device Management

What do effective processes for integrating connected medical devices into your network, securely managing connected medical devices, and responding to a cyberattack look like? When onboarding new connected medical devices into your network, it's important to have the right access controls and check that default passwords have been removed. Ensure the appropriate network segmentation for each medical device, based on its unique requirements, risks, and vulnerabilities. This will reduce the attack surface and protect the organization's network in the event of a breach.

Securely managing medical devices involves working with manufacturers to get timely notifications about new updates, patches, and other important maintenance requirements. Organizations can then automate policy enforcement on these necessary processes by developing device asset intelligence capabilities. When these processes break down, there should also be an automated protocol to isolate devices due to increased risk and deploy the appropriate mitigations. Device monitoring can also be leveraged to isolate breached devices, in the event of an attack.

[4] Medical Device Cybersecurity Regional Preparedness and Response Playbook | Mitre

IT Maturity and Medical Devices

IT maturity around connected medical devices involves:

- Cyber capability assessments and asset intelligence
- Appropriate policies and processes
- Procurement policies and supply chain risk management
- Proactive security: device segmentation, automated patching/updates, maintenance, device asset intelligence, device monitoring, and threat monitoring
- Reactive security: device isolation, recovery processes, and backup devices.
- Automated workflows and protocols

Implementing the right processes and ensuring the appropriate security on your devices will reduce the likelihood of a cyberattack. However, it cannot fully eliminate the risk. Healthcare organizations should also have the appropriate capabilities to detect, identify, protect against, respond to, and recover from a cyberattack. Recovery would involve removing the bad actors in your network, discovering the extent of the data breach, isolating devices, working with the manufacturers to patch vulnerabilities, and having backup devices that can be deployed to support patient care and safety until your network and devices are once again secured.

Conclusion

The critical role that connected medical devices play in the delivery of healthcare both today and in the future mandates that organizations build a comprehensive cybersecurity program for their connected devices The risks are too great for patients, providers, and healthcare delivery organizations not to act.

Guidehouse has significant experience in both cybersecurity and the healthcare sector that enables the delivery of holistic solutions for medical device security. Guidehouse has helped many healthcare organizations decrease their overall cyber risk, secure their healthcare delivery model, and protect their patients and healthcare system. Maintaining proper security protocols ensures that healthcare organizations can leverage the value and savings of connected medical devices while reducing risk. This ensures that healthcare organizations are better prepared to meet the future of connected devices.

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit **www.guidehouse.com.**

Contact

Matthew Phillips
Director
maphillips@guidehouse.com

guidehouse.com/cybersecurity

@GHTechSolutions

linkedin.com/showcase/guidehouse-technology-solutions