GE HealthCare

How to protect your medical devices against cybersecurity risks

gehealthcare.com

Hospitals and healthcare facilities rely on connected medical devices to improve the patient experience, but these devices can also introduce cybersecurity risks.

According to “Healthcare Data Breach Statistics,” cyberattacks on medical technology are on the rise due to a massive increase in hacking incidents and ransomware attacks. Because of this, hospitals with outdated systems, unsecured networks, or unpatched software could be vulnerable.

Without a strong security framework, hospitals may risk patient data breaches, compliance failures, and even harmful disruptions to care. In this article, we explore the cybersecurity risks facing medical technology and how Medical Technology Advanced Services' (MTAS) ‘Secure’ discipline helps healthcare providers safeguard their systems.

What are important cybersecurity vulnerabilities in healthcare?

Ransomware and malware attacks

According to “Cybersecurity in Healthcare | Protecting Patient Data and Systems,” cybercriminals are targeting medical devices by encrypting sensitive data and demanding ransom payments from healthcare providers. These attacks can lead to devastating consequences such as the loss of critical patient information and financial strain on the affected institutions. Malware infections can severely disrupt hospital operations, which can cause delays in patient care and compromise the overall efficiency of medical services.

Hospitals with outdated security protocols are particularly vulnerable to these attacks, as they may lack the necessary defenses to help prevent unauthorized access and mitigate the impact of such threats. Ensuring robust cybersecurity measures can help to protect patient data and maintain the integrity of healthcare services.

Unpatched software and outdated devices

“The Cybersecurity Threat Ailing Healthcare” addresses the fact that many healthcare organizations continue to rely on legacy medical equipment with unsupported operating systems. The article states that a reliance on outdated technology can create significant security vulnerabilities, as these systems often lack regular software updates. Failure to upgrade devices not only increases the risk of cyber intrusions but it can also heighten the potential for data leaks, which can put sensitive patient information at risk.

Prioritizing the modernization of medical technology infrastructure is extremely important in safeguarding against these threats.

MTAS's "Secure" discipline helps protect healthcare systems

Medical Technology Advanced Services (MTAS) helps healthcare providers mitigate cybersecurity risks by implementing a structured security framework. The 'Secure' discipline focuses on proactive cybersecurity measures, compliance and risk management and real-time threat monitoring and response.

Proactive cybersecurity measures

MTAS helps to ensure that healthcare systems are regularly updated with the latest approved security patches and software updates, helping to mitigate vulnerabilities that could be exploited by cybercriminals.
By recommending network segmentation, MTAS helps prevent cyber threats from spreading across hospital systems, thereby containing potential breaches and helping to minimize their impact.

Additionally, MTAS recommends using multi-layered encryption and robust authentication protocols to help protect patient data, helping ensure that only authorized personnel can access sensitive information. These proactive measures can help maintain the integrity and security of healthcare systems in an increasingly digital world.

Compliance and risk management

MTAS helps ensure that all medical devices are deployed in alignment with stringent industry security regulations, including HIPAA, GDPR, and FDA guidelines. By conducting comprehensive security audits, MTAS helps to identify potential weaknesses within the healthcare system and implement corrective measures to address these vulnerabilities. Furthermore, MTAS aligns its cybersecurity strategies with hospital IT policies and national healthcare standards to help ensure a cohesive and compliant approach to protecting patient data and maintaining the integrity of healthcare operations. This disciplined focus on compliance and risk management can help safeguard sensitive information.

Real-time threat monitoring and response

MTAS implements AI-powered monitoring tools designed to detect and neutralize cyber threats swiftly. These advanced tools help enable real-time alerting and incident response, which can help minimize system downtime and ensure continuous operation of critical healthcare services. By helping to protect medical device networks from unauthorized access and cyber intrusions, MTAS helps to ensure that healthcare providers can maintain the highest levels of security. This proactive approach to threat monitoring and response can help safeguard sensitive medical data, maintain the integrity of healthcare systems, and help enhance the patient experience.

What are the best practices for securing medical technology?

Adopting a proactive security approach that includes regular updates, access control measures, and compliance-driven policies can help hospitals reduce cybersecurity risks.

Keep all medical devices updated

Regularly applying approved security patches and software updates can eliminate vulnerabilities that cybercriminals could exploit. Ensuring that all medical devices are up-to-date helps protect against the latest threats and helps maintain the integrity of the healthcare system.

Implement strong access controls

Strong access controls help ensure that only authorized personnel can access sensitive medical data, which can reduce the risk of data breaches. Using multi-factor authentication for all connected devices where supported and deployed can help prevent unauthorized access.

Conduct regular security audits

Regular security audits help identify vulnerabilities within the healthcare system. Proactively fixing these issues before they become risks can allow hospitals to maintain a robust security posture and can help protect patient information.

Train staff on cybersecurity awareness

Educating healthcare teams on recognizing phishing attempts and suspicious activity is a key component of a comprehensive cybersecurity strategy. Regular training sessions help staff stay vigilant and aware of potential threats, which can help reduce the likelihood of successful cyberattacks.

MTAS helps tackle vulnerabilities in healthcare cybersecurity

In "Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem," the authors confirm that the increasing interconnectedness of medical devices and systems makes hospitals more susceptible to cyberattacks than ever before. This reality underscores the need for robust cybersecurity measures to protect sensitive patient data and help ensure the integrity of healthcare services.

Medical Technology Advanced Services (MTAS) by GE HealthCare is stepping up to address these challenges head-on. By providing a comprehensive security framework, MTAS helps equip healthcare providers with the tools to help mitigate the risks associated with cyber threats. Through a focus on proactive cybersecurity strategies, compliance, and real-time threat monitoring, MTAS helps empower hospitals to safeguard their systems effectively.

Investing in MTAS not only helps to enhance the security posture of healthcare organizations but can also help ensure the continuity of care delivery and the fostering of patient trust. As vulnerabilities continue to grow, embracing the innovative security solutions offered by MTAS can be an effective strategy for creating a more resilient healthcare environment.

To learn more about how MTAS can help your organization strengthen its cybersecurity measures, visit the MTAS page for further insights and solutions.

GE HealthCare