Safeguarding the NHS: Addressing threats from connected medical devices

The increasing use of Health Service (NHS) has revolutionised patient care and improved treatment outcomes. However, this digital transformation connected medical devices in the National also brings new challenges and threats to the security and integrity of healthcare systems. In this article, we will explore the threats posed by connected medical devices to the NHS and discuss strategies for securing them going forward.

Threats from Connected Medical Devices:

Vulnerabilities in device security

Connected medical devices, including infusion pumps, pacemakers, and imaging systems, are vulnerable to cyberattacks due to security weaknesses. These vulnerabilities may arise from outdated firmware or software, inadequate encryption protocols, or insecure communication channels. Exploiting these weaknesses, malicious actors can gain unauthorised access to devices, manipulate patient data, or even compromise device functionality, potentially leading to patient harm.

Lack of standardisation and interoperability

The lack of standardisation and interoperability among connected medical devices poses significant challenges to their security. Different manufacturers may utilise varying security protocols, making it difficult to implement consistent security measures across multiple devices. Additionally, the compatibility issues arising from device heterogeneity can hinder effective monitoring, patching, and updating of devices, leaving them susceptible to cyber threats.

Insider threats

Insider threats within healthcare organisations can also pose risks to the security of connected medical devices. Employees with authorised access to these devices may misuse their privileges or inadvertently expose them to security risks. Whether driven by personal motives or negligence, insider threats can compromise patient data confidentiality and device integrity. Organisations must implement strong access controls, monitor user activities, and foster a culture of cybersecurity awareness to mitigate insider threats.

Securing Connected Medical Devices:

Adopting a risk-based approach

A risk-based approach is crucial to securing connected medical devices within the NHS. Healthcare organisations should conduct comprehensive risk assessments to identify vulnerabilities and prioritise security measures accordingly. This includes evaluating the potential impact of a security breach, assessing the likelihood of threats, and implementing appropriate security controls based on the identified risks.

Implementing strong authentication and encryption

To enhance the security of connected medical devices, robust authentication and encryption mechanisms must be implemented. Strong user authentication methods, such as multi-factor authentication, should be employed to ensure that only authorised personnel can access and control the devices. Additionally, all communication channels between devices and networks should be encrypted to prevent unauthorised interception of data.

Securing Connected Medical Devices (cont.)

Regular patching and updates

Regular patching and software updates are essential to address known vulnerabilities in connected medical devices. Healthcare organisations should establish processes to ensure that all devices are promptly patched with the latest security updates provided by the manufacturers.This includes implementing a centralised system for monitoring and managing device updates to prevent any devices from being left unpatched and vulnerable.

Implementing network segmentation

Network segmentation can help mitigate the impact of a security breach by isolating connected medical devices from the rest of the network. By creating separate network segments for devices, organisations can limit the lateral movement of attackers and reduce the potential for unauthorised access to critical systems. Proper segmentation also enables enhanced monitoring and detection of any suspicious activity within the device network.

Collaboration with device manufacturers

Collaboration between healthcare organisations and device manufacturers is vital for improving the security of connected medical devices. Manufacturers should prioritise security in the design and development of devices, including robust encryption, secure communication protocols, and timely security updates. Healthcare organisations, in turn, should actively engage with manufacturers to share threat intelligence, provide feedback on device security, and collaborate on implementing best practices.

A connected future

As connected medical devices continue to proliferate in the NHS, addressing the associated threats is imperative to ensure patient safety and data security.

Contact us:

Rajvir Cheema
Partner, Digital Healthcare Advisory
KPMG in the UK
E: rajvir.cheema@kpmg.co.uk

Richard Krishnan
Partner, Technology and Cyber Risk
KPMG in the UK
E: richard.krishnan@kpmg.co.uk

Thomas Jordan
Cyber Senior Manager
KPMG in the UK
E: thomas.jordan@kpmg.co.uk

Find out more: home.kpmg/uk/cyberforhealth

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.com/uk

CREATE: CRT152957A I January 2024