HALL RENDER ADVISORY SERVICES

MEDICAL DEVICE SECURITY SERVICES

With leadership experience ranging across the health care IT spectrum, our team of trusted advisors is available to provide practical and actionable guidance that fits your organization and needs. As health care and IT continue to become more closely intertwined, medical device security services must be considered by health systems. Our team of advisors has the dedicated industry knowledge and experience to ensure your devices remain as secure and efficient as possible.

MEDICAL DEVICE SECURITY SERVICES

Medical device security services are intended to identify, develop, implement and manage the security protocols required for all phases of an enterprise medical device security lifecycle, ultimately improving the overall security and risk management practices for medical devices. These services are needed in order to assist organizational stakeholders in meeting key security requirements for medical devices with the goal of avoiding integrity and availability issues due to device compromises and facilitating organizational change to reflect the intersection of IT, clinical and biomedical engineering and clinical practice.

CONTACT

For more information on Hall Render Advisory Services, visit hallrenderas.com or call 317.633.4884.

Medical Device Security Services

Due to the distinctive clinical nature of most medical devices, there are several challenges involved in the identification, evaluation and eventual remediation of those devices. While medical devices come with a "one size does not fit all" disclaimer, they generally share the same features as other devices connected to an organization's network, including:

- A potentially vulnerable operating system.
- Transmission of ePHI across the network to multiple other devices.
- Usage of both wired and wireless technologies.
- Access to the internet.

However, it is important to understand that there are also some unique differences between medical devices and other hosts on the internal network.

- There are usually no protections installed such as anti-virus or end-point encryption, and many medical devices do not have the capability for third-party software installation.
- There are usually no procedures to patch security vulnerabilities or those procedures are inconsistent in process and application. Often, OEM approval is required prior to the installation of security patches.
- These devices are often connected directly to patients and could put patient care at risk.
- The devices' operating systems tend to be older than current supported operating systems.
- Upgrading or patching the devices could render them inoperable, placing patient care (and data) at risk.

Medical device security services can be offered to health care provider organizations in order to overcome some of these challenges by providing:

- Risk assessment processes in order to identify gaps in secure management of medical devices.
- Identification of active technical vulnerabilities using passive network scanning and prioritizing these vulnerabilities for remediation by risk.
- Development of policies and procedures required for a foundational medical device security program.
- Risk mitigation planning for vulnerable devices, including providing compensating controls for end-of-life devices and recommendations for secure network management as an alternative to security patching.
- Clinical engineering, IT security and regulatory compliance expertise required for successful performance of these processes.

For more information about our medical device security services or for a FREE program assessment, visit hallrenderas.com or call 317.633.4884.

HALL RENDER
ADVISORY SERVICES