MEDICAL DEVICE SECURITY SERVICES

Medical device security services are designed to identify, develop, implement and manage the security protocols required for all phases of an enterprise medical device security lifecycle, used to improve the overall security and risk management practices for medical devices.

These services 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.

The distinctive clinical nature of most medical devices creates several challenges in the identification, evaluation and eventual remediation of those devices. Clinical systems generally share the same features as other devices connected to an organization's network, including potentially vulnerable operating systems, the capability for transmitting ePHI across the network to multiple other devices, the utilization of wired and wireless technologies and the typically open and available access to the internet.

However, it is important to understand there are also some unique differences between medical devices and other systems on the organization's internal network:

- Typically, there are no protections installed on medical devices, such as antivirus or end-point encryption, and many medical devices do not have the capability for third-party software installation.
- There are usually no procedures in place to patch security vulnerabilities or those procedures may be inconsistent in process and application, making them difficult to manage. Original Equipment Manufacturer approval is often required prior to the installation of security patches and may create barriers to deployment.
- Medical devices are often connected directly to patients and have a higher risk impact, with the potential of jeopardizing patient care.
- The devices' operating systems tend to be older than current supported operating systems.
- Upgrading or patching devices could render them inoperable, placing patient care (and data) at risk.

Our team of health care IT consultants can help overcome these unique challenges by providing the following services:

- Evaluating the organization's current security program, including the resources, tools and capabilities needed to align with security best practices, and recommendations for enhancements to the program.
- Completing a comprehensive risk assessment to identify technical risks and gaps in the secure management of clinical systems.
- Conducting an audit that detects the active technical vulnerabilities on clinical systems using passive network scanning and prioritization of these vulnerabilities for remediation by risk levels.
- Developing enterprise-wide policies and standard operating procedures necessary for implementing and managing a best-in-class medical device security program.
- Initiating risk mitigation planning for vulnerable devices, including providing compensating controls for end-of-life systems and recommendations for secure network management as an alternative to security patching.
- Evaluating the clinical engineering, IT security and regulatory compliance expertise required for successful performance of these processes.