**Recommendation**

Adopt an enterprise scalable security and privacy strategy to protect systems and patients in an ecosystem with heterogeneous and vulnerable networked medical devices.

**Background**

Medical devices are becoming much more advanced and are increasingly networked, providing critical information to inform the care of our military and veteran patients. Previously isolated devices such as pacemakers, wearables, EKG machines, etc. are now able to provide valuable data to medical providers and increase patients’ quality of care. However, many of these devices enter our healthcare networks with little to no security consideration. In fact, 56% of survey respondents anticipated an attack on their medical devices; however, only 15% were taking significant measures to mitigate it. Worse, 43% of device manufacturers don’t conduct security testing on their devices. One concrete example was last year’s WannaCry ransomware attack, which infected medical devices, in many instances causing disruptions in service. This is why Northrop Grumman offers a scalable enterprise SECUrITt Internet of Medical Things (IoMT) Software as a Service (Saas) solution (highlighted under the “Solution” section).

Exposed medical devices create vulnerabilities that can lead to security or privacy breaches; access to medical images, protocols, databases, industrial controllers, and healthcare systems software; and potentially have an impact on patient safety and device effectiveness. These risks pose a direct threat to operational readiness. As medical devices are connected to Military Treatment Facility (MTF) networks, commercial healthcare networks, Non-classified Internet Protocol (IP) Router Network (NIPRNet), the Internet, home networks, or other medical devices, enterprise IT risk multiplies. Although there is no single solution, Northrop Grumman offers a scalable enterprise SECUrITt IoMT SaaS solution to medical device management for the operational and garrison environments to reduce these risks and fundamentally transition medical device security from an IT issue to a patient safety issue, providing increased combat support and medical readiness along the way.

**Issues**

Our experience with IoMT shows these common preventable security gaps:

- Environments and/or devices are not monitored based on agency standards for sensitive data
- Lack of medical device assessments to understand the security and privacy capabilities (i.e., default credentials, logging, password management, default configuration, communication protocols, resident data storage)
- Limited asset inventory to include data fields, communication modality, firmware and operating systems versioning, especially those with remote access and device-to-device access
- Software patches and updates are not monitored and applied as required by policy
- Medical devices that cannot conform to minimal baseline standards are not identified and isolated on the network
- No defined security and privacy review process when considering new equipment for implementation
- Remote access and vendor support is not provided based on agency standards for sensitive data
- No centralized inventory of IMDs to facilitate risk and device management, inclusive of security and privacy concerns
- Insufficient disposal procedures based on DoD standards for sensitive data
- Minimal consideration of legacy networks to support the growing number of wireless medical devices

**Solution**

To address these issues, we recommend using our SECUrITt strategy. This strategy moves an agency from a device-specific focus to an enterprise-wide strategy that emphasizes patient safety.

**Supply Chain**

We customize the National Institute of Science and Technology (NIST) Cybersecurity Framework for immediate implementation to reduce risk to the hospital supply chain, more specifically to medical devices.

**Ensure Alignment**

Given this is a patient safety issue, clinical patient safety programs within the Defense Health Agency (DHA) need to embrace and be aligned with the adopted solution. Our solution aligns IT and clinical safety while clearly defining the security boundary for IoMT to encompass military, commercial, and home interoperability.

**Continuous Education**

Those who deploy the devices must be able to answer questions and inform patients about how the devices are protected. We overlay our continuous education program within our solution.

**Universal Inventory**

With the sheer magnitude of devices the DHA has and the potential implications on patient safety, having an accurate full lifecycle identification and inventory process is paramount. This is not a simple process as many devices are not identified with a unique asset number so accurate inventory is left to manual processes. Our inventory process provides a unique Media Access Control (MAC address) and asset number allowing

---


2 From a CIA perspective: Confidentiality= breach of patient data, Integrity= data used to make treatment decisions (patient safety) and Availability= outage creates critical gaps in patient monitoring or treatment. Source: (https://www.jointcommission.org/assets/1/6/1290)

© 2018 Northrop Grumman Systems Corporation All rights reserved—Cleared for Public Release (Case #: 18-1290)
for our inventory process to be automated by using tools specifically built for medical device network identification.

Recursive Vulnerability Management – Being able to continuously and quickly determine device vulnerabilities is critical. To achieve this, we implement an active monitoring program that is infused into your vulnerability management processes. Relying on typical network monitoring tools is not sufficient as most medical devices use unique protocols such as Digital Imaging and Communications in Medicine (DICOM), Health Level 7 (HL7) and American Society for Testing and Materials (ASTM) and are too fragile to use traditional network monitoring tools so we introduce specialized network monitoring tools for IoMT devices.

Independent Risk Ranking – We rank medical devices by our predetermined criteria (type of data stored/transmitted, impact on patient well-being, physical location, replacement value, etc.) and overlay DHA risk (paying close attention to account supporting processes, staffing, training and technology).

Targeted Maintenance/Updates – Medical devices require software maintenance and updates and due to the patient safety implications, we establish a dedicated process to ensure they stay current on their maintenance/updates. Since we have a universal inventory, it allows for determination of the process in which updates will be received from entities such the U.S. Food and Drug Administration (USFDA).

Technical Isolating – There are many reasons for isolation of medical devices. Their fragile state for scanning is a critical benefit as the DHA can establish an isolated environment for medical devices and run ‘light touch’ and passive scanners within that environment. Isolation can be achieved in many forms such as micro-segmentation, containerization or cloaking (Identify Defined Networking (IDN)). We assess the Agency network to determine the most effective isolation strategy. Once the devices are isolated, then continuous monitoring is implemented during this phase through SIEM integration allowing for single pane of glass dashboard of all IoMT devices in the ecosystem.

For success the Securitt strategy requires careful implementation as each element is interdependent on the others. By using the Securitt strategy the military hospital systems can reduce their security and privacy risks posed by medical devices. For more information regarding how the Northrop Grumman enterprise IoMT SaaS Securitt strategy can support your agency patient safety and operational patient readiness, contact:

Northrop Grumman Corporation Technology Services System Modernization and Services
2340 Dulles Corner Boulevard, Mail Stop 10S018
Herndon, VA 20171
NGTSComm@ngc.com