JOHNS HOPKINS

Provisional Medical Device Security Standards

Approved, June 2019,

Provisional through June 30, 2022

Table of Contents

I. Summary

These Medical Device Security Standards are established on a provisional basis to communicate a sensible approach to improving device security. The Standards consider the roles and responsibilities of various stakeholders. A framework for managing risk is also formulated over the entire lifecycle of medical devices.

II. Introduction

A. Background

Medical device security has become an increasingly visible issue in the healthcare provider community. Medical device cybersecurity was ranked as #1 Health Technology Hazard by ECRI for 2019. As devices have become increasingly networked and inter-connected, security capabilities have generally not kept pace. Over the past several years, a number of security researchers have identified vulnerabilities in medical devices of various types. In addition, it has become increasingly clear that medical device security faces challenges in configuration, management and patching. Also, as organizations have experienced downtime associated with malware such as ransomware, security is now an important operational issue.

The National Health Care Industry Cybersecurity (HCIC) Task force recently characterized the problem thusly:

> ***Imperative 2. Increase the security and resilience of medical devices and health IT.***
> *The Health Care and Public Health (HPH) Sector is charged with keeping patients safe and that includes protecting patients from physical harm, as well as privacy-related harms that may stem from an exploited known cybersecurity vulnerability. If exploited, a vulnerability may result in medical device malfunction, disruption of health care services (including treatment interventions), and inappropriate access to patient information, or compromised EHR data integrity. Such outcomes could have a profound impact on patient care and safety. Some*

foundational challenges that will need to be addressed in order to enhance the cybersecurity of medical devices and EHRs include legacy operating systems, secure development lifecycle, strong authentication, strategic and architectural approaches to product deployment, management, and maintenance on hospital networks.

The relatively short lifespan for operating systems and other relevant platforms such as commercial off the shelf software is inherently misaligned in health care as medical devices and EHRs may be utilized for 10, 15, 20, or more years. This misalignment may occur for a variety of reasons. Hospitals operate on thin budgets and cannot replace capital equipment like MRIs as quickly as new operating systems are released. Product vendors have a product development lifecycle that may take several years and they may start development using one operating system and by the time the product comes to market, newer operating systems may be available. Creative ways of addressing the aforementioned challenge areas may be found by engaging key clinical and cybersecurity stakeholders, including software vendors. [1]

B. Audience

The target audience for this document is anyone who is responsible for purchasing, administering, extending or evaluating medical devices.

C. Scope

These Standards cover all medical devices used for patient diagnostics and care. This definition includes FDA-approved devices, but the guidance applies to any device used principally for treatment, and/or collection, processing or storage of patient information. While general purpose computing devices are not specifically covered under these standards, even those (e.g. including laptops, tablets, smart phones, etc.) are covered insofar as they are dual-use for purposes typically associated with medical devices. Since medical devices are also often part of integrated systems, these Standards also may include middleware, supporting devices or other system components.

[1] Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Healthcare Industry*, May 2017, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2017/cs2017_0156.pdf

The ICSC has published several Standards pertaining to Medical Device Security

1. *Clinical Wireless Device Standards* – covering the process and substance of wireless deployments of medical devices, with particular attention to bandwidth and WPA2 Enterprise requirements.
2. *Linux Security Guide* – covers security and a checklist for securing Linux and Unix hosts.
3. *Windows Server Standards* – a comprehensive approach to securing Windows servers in the Hopkins environment, including a checklist and requirements for inclusion in the enterprise JH domains. This is of particular importance for medical devices that have server controllers or interfaces.
4. *Windows Client Standards* – directed toward general purpose Windows clients, but also includes guidance for configuring logging and patching of client devices.

As with the aforementioned IT Policies and Standards, these standards apply to both Johns Hopkins University and Johns Hopkins Health System.

D. Enforcement

Failure to follow these standards may be considered a violation of *Johns Hopkins Information Technology Policies,* which are incorporated by reference.

III. Cross Functional Collaboration

A. Security Stakeholders

One of the principal challenges in medical device security is that devices are not managed through normal information technology systems management. Standard industry practice is to manage devices through highly specialized engineering groups rather than IT generalists. Even purchase and lifecycle management are handled differently than for general purpose computer hardware and software. Medical device security thus requires a move away from the IT-centric model standard for information security practice. Each component of information security has a corresponding, but slightly different, piece in a medical device security context.

1. Device Owners

Device owners are ultimately responsible for the safety and security of the devices that they acquire and use. Hopkins gives individual organizations leeway in terms of choosing appropriate technologies to fit their operational or analytic needs. Owners are therefore expected to ensure that technologies are managed in a technically competent manner. Since many owners do not have specialized technicians on staff to manage certain technologies, they must therefore arrange with engineering management or other management groups. One of the reasons for emphasizing initial configuration in these Standards is that this configuration stage will clarify the standard of care for the technology going forward.

Failures in device operations and information security issues are principally the responsibility of device owners. Preventing and mitigating incidents may fall primarily on other organizations, but it is the device owner ultimately responsible for the safety and security of the device. It is therefore incumbent upon the device owner to work with device engineers to plan for configuration, on-going support and life cycle issues.

2. Device Engineering

Typically characterized as “clinical engineering,” “biomed” and increasingly “Healthcare Technology Management” (HTM), medical device management varies from facility to facility yet with a number of common characteristics, such as testing, implementation and monitoring. The term “device engineering” is used to avoid confusion regarding management of devices, whether in a Johns Hopkins clinical engineering or another department, e.g. Radiology, Pathology, etc. In any case, device engineering crosses technical disciplines in order to ensure reliability, safety and inter-operability. As devices have increasingly become networked, device engineers have ramped up their expertise in enterprise systems management and information technology.

Ensuring the security capabilities of a medical device is the responsibility of the device manufacturer. Managing the security of devices on-site is a team effort, yet the bulk of responsibility will lie with device engineers or managing user groups as per arrangements with device owners. To ensure security, device engineers are required to spend enough time with each device and device type, and may be required to learn and practice specialized skills. One of the goals of this Standard is to impress upon the Hopkins

community the necessity of ensuring that devices are managed throughout their lifecycle by full-time professional device engineers and not as a part-time job of an IT or operational administrator.

Any security breach that causes an adverse event is required to be reported to the FDA. (https://www.fda.gov/MedicalDevices/Safety/ReportaProblem).

3. Manufacturers/Vendors

Medical device manufacturers must continue to build better security capabilities (e.g. access control, whitelisting, encryption, logging, etc.) into devices and device systems that they deliver to customers. Less obvious but just as important, customer relationships with manufacturer are likely to last longer and involve more management and configuration dependencies than they would without security requirements. Much of security practice involves vulnerability management and patching, and it is the responsibility of a manufacturer to provide configuration guidance and security updates throughout a device's lifecycle. The FDA requires manufacturers to update systems when bugs are found that may involve patient safety or performance. Security updates typically follow the same model, but security patches are usually issued with greater frequency.

From an organizational perspective, our increasing reliance on manufacturers may lead to consolidation and bulk purchases of devices of several types and models. Just as Hopkins has a small number of preferred vendor partners in systems management and security, a similar approach may be required for device manufacturers going forward. It is therefore incumbent upon prospective device owners to consider the risk of engaging with inexperienced or one-off vendors or manufacturers.

4. Supply Chain -- Capital Management, Purchasing and Legal

As expectations change to meet new security challenges, the supply chain must be able to modify requirements and assess new technical capabilities quickly. For many years, Johns Hopkins has used security checklists and contractual language to ensure that manufacturers offer sensible security capabilities. Increasingly, a similar evaluation is required to validate security capabilities of Hopkins organizations seeking to deploy and manage a device. For this reason, it is becoming increasingly critical that all medical device acquisitions proceed through standard supply chain paths. As we strengthen

security requirements, it will be tempting for some prospective owners to follow the path of least resistance.

Any acquisition or deployment of a medical device, whether for operation, research or analytic purposes, must follow these Standards and thus must be processed through a supply chain capable of conducting manufacturer/management capabilities and plans. Any department (both JHU and JHHS) for whom an individual or group that chooses for whatever reason to circumvent the processes outlined here are out of compliance with both Johns Hopkins IT and purchasing policies, unless express written exceptions are granted by supply chain executive management.

Supply chain organizations are responsible to communicate warranty and life cycle management requirements to the Hopkins community, including baselines for manufacturer support and end-of-life procedures.

As part of RFP's and medical device procurement, supply chain should ensure the following:

- Johns Hopkins organizations designated to manage medical devices have the administrative and technical capabilities to manage devices according to these Standards, and if not the case, prospective owners should be directed to an appropriately staffed device engineering groups.
- Prospective manufacturers provide a current MDS2 documentation regarding security capabilities [Note: JHH needs the resources to assess MDS2 and related documents]
- In addition to the MDS2, Johns Hopkins may require a security capabilities questionnaire, either internally developed or as a standard questionnaire from an organization such as the H-ISAC or HIMSS.
- For new or high-risk devices (defined in Section IV.B below) , prospective manufacturers must provide product security testing documentation. It is not generally Johns Hopkins practice to test medical devices; yet there may be exceptions where a manufacturer may be required to collaborate on testing with a Hopkins management or information security group.
- Devices that rely on platform technologies (e.g. operating systems, Java frameworks) that are both potentially vulnerable and near end-of-life will be treated as high-risk devices and may require additional documentation or a justification exception in order to remain in operation.

- Prospective manufacturers must be able to substantially meet these Standards, specifically to provide Manufacturers Documentation as discussed below.
- In cases where security capabilities are not included in the core product, it may be appropriate to require additional features prior to deployment.
- Johns Hopkins does not generally require provision of Software Bill of Materials (SBOM) but may choose to require this documentation for complex or high risk devices.
- For bulk purchases or RFP's, security documentation and consultation should take place as early as possible in the planning and review process.

5. Information Technology

The role of information technology staff in medical device security is complicated by the number and varied types of information technology staff potentially interested in a device's operations. In some cases, a device, often a dual-use device on commodity hardware and software, may be managed by IT in conjunction with device engineering or departmental operations. In other cases, the only continuing interaction with IT would involve data integration with electronic health records, research or data warehouses. Still in other cases, the only interaction with IT would be with initial configuration and registration of IP addresses.

6. Information Security

Information security departments typically write enterprise security policy, identify vulnerabilities and conduct surveillance at scale. Regarding medical devices, information security at Johns Hopkins assesses emerging threats and vulnerabilities. It also works with supply chain and device engineering groups to review security capabilities of new devices. Information security's principal purposes, however, are to monitor the JH Network and its many systems for anomalies and potential mischief and handling incident response. Information security and IT are responsible for informing engineers of network or other security-related changes that are likely to cause operational issues for medical devices.

IV. Security Risk Framework

Medical device security consists of several enterprise components that together form an over-arching risk framework.

A. Asset Inventories

It is the responsibility of each device engineering group to maintain a current inventory of all devices under its management. For security purposes, inventories should include at least the following data elements:

- Device owner if different than device engineering group
- Device administrator and support organization
- Manufacturer
- Type and Model
- Facility and floor location
- Connectivity (wireless, cellular, wired – DHCP or static)
- MAC Address IP Address (if static)
- Network segment
- Operating system
- Original deployment date or in-service date Most recent update (can be expressed through model number)
- Major data interfaces
- Software/firmware versions Type of data stored or transmitted
- End-of-life or end-of-support
- Model risk register rating.

The information security group has a number of network surveillance tools to identify medical devices and maintains an inventory of these devices. It also polls departments to merge device engineering inventories into a comprehensive inventory and risk register. Such a network-centric inventory would not have some of the other information for a comprehensive inventory.

As the device security program matures, the goal would be for systems to provide near real-time inventory capabilities as JH has with workstations and servers.

B. Risk Registers and Remediation Planning

Risk Registers are repositories that can be used to easily report on efforts across the framework activities, track remediation, and map new known vulnerabilities or potential risks. Device engineering groups should maintain a Risk Register based on information from Manufacturer Documentation discussed below, types of data, business criticality and interfaces.

Based on HCIC Guidance, we recommend the risk rating system[2]:

- None to Low Risk means negligible or no impact to clinical workflows, safety or patient data loss.
- Medium to High Risk introduces the potential for adverse events, but that the risk is either relatively Low or mature security controls (e.g. application whitelisting, rapid patching) are in place.
- Critical Risk introduces potential for injury or harm to patients or users of products including impact to patient data, safety or workflows. Critical risks obtain when the device has specific, difficult to manage, vulnerabilities, such as poor manufacturer support, out-of-date operating systems or services.

Storage and transmission of PHI is also a factor when determining these risks. Device engineering groups may establish more elaborate risk assessment methods to incorporate deeper security controls, legacy systems, safety considerations and the like. The principal purpose of risk assessment and registers are to form the basis of prioritization and sequencing of controls.

C. Manufacturer Documentation

Just as with other operational components of a device, ensuring security requires communication between a manufacturer and device engineers. While communication typically occurs between

[2] https://www.nist.gov/sites/default/files/documents/itl/preliminary-cybersecurity-framework.pdf

manufacturer and engineering group, ensuring that manufacturer documentation meets minimum requirements is also the responsibility of Supply chain. At the time of installation, manufacturers should have provided to device engineering documentation on each of the issues. This initial configuration should represent reasonable best practices for securing a device at the outset and should be maintained throughout the device lifecycle: All components provided or required for use:

- Compatibility with systems management tools and vulnerability scanning
- Data Flow diagrams, network ports and services, as well as any requirements for network connectivity
- Remote access methods and tools
- Access control design including privileged access controls and manufacturer support maintenance and/ or service accounts
- Patch management processes (e.g. including analysis of how patches are made available and responsibility for testing and deployment)
- Required cybersecurity controls including malware protection, such as anti-virus, advanced endpoint protection and/or whitelisting
- Logging and audit capabilities, including those logs enabled by default and the operational impact of enabling additional logging
- Assumptions and requirements at installation and in use to maintain security
- Summary of known security risks and considerations
- Contact information to report incidents, vulnerabilities, or for general inquiries regarding security

D. Configuration Management

Working from manufacturer documentation, IT network engineers and device engineers will have a number of JH-specific configuration issues to consider:

- Assess connectivity mechanisms, and if wireless, follow the *Clinical Wireless Device Standards* and confer with IT wireless support team as needed for guidance on bandwidth and encryption protocols.
- Validate and certify wireless access, if applicable, including: certificate request and generation, and validation of WPA2-Enterprsie, EAP-TLS, and SHA-2 256 bit certificate compliance.

- Wireless tests should assess whether device will connect to the Clinical Wireless network segment. Certify connectivity to all available 5GHz channels.
- Register for network IP's based on connectivity and domain requirements
- All server deployments should follow ICSC Windows and Linux standards and guidance[3].
- Identify appropriate network segment (e.g. Medical Device, Radiology, etc.) and deploy in consultation with Johns Hopkins Networking or Network Security groups (nsi@jhmi.edu).
- For open vulnerabilities, identify specific compensating controls, such as closing ports and services, setting alerting triggers, conferring with Network Security on specific firewall settings.
- If allowed by manufacturer and appropriate for product type (i.e. device runs commodity Windows or Linux), install management software.
- If allowed by manufacturer and appropriate for product type (i.e. device runs commodity Windows or Linux), install JH malware protection (e.g. Windows Defender).
- Catalog systems and data interfaces.
- If remote access is required, set up and test remote access through accepted Johns Hopkins mechanisms (e.g. Site to Site VPN).
- Check logs during configuration and for some time afterward to ensure that logs are complete and log caches are capable of maintaining at least four (4) weeks events.
- If allowed by manufacturer and appropriate for product type, run configuration security script for automated checks on the device if made available by information security.

E. Vulnerability and Patch Management

It is typical for device engineering groups that handle a number of models, to have nearly as many approaches to patching. Patching timeliness, completeness and tracking are all core considerations for a patching program. It may be helpful for device engineering groups to create a taxonomy of patching approaches and map to device risk and other operational concerns:

- *Remote Update* -- Patches applied via secure authorized remote service and support platforms provided by manufacturer.
- *Johns Hopkins Administered* – manufacturer-validated patches made available for device engineer retrieval and installation from a designated external source including direct download

[3] https://it.johnshopkins.edu/policies/standards.html

from the third-party entity that provides the product or component. Typically, this would not involve JH's standard patch management program, because manufacturer validation would not likely adhere to JH patch deployment schedules.

- *Ad-hoc Patching* – for Low risk or dual use devices, engineers may choose to accept engineering and technical risks of deploying patches not validated by manufacturers. These may be applied through the standard Johns Hopkins patching program or applied in a truly ad hoc manner by the device engineer.
- *Service Visit* -- local service by manufacturer or designate physically administering patches. This method is generally less preferable due to the time required to deploy local service personnel Hopkins. It may be preferable where patching is complex, such as frameworks, and hands-on testing is required.

Device engineers should remain current on patching practices for each device, so that emergency patches for instance can be applied rapidly and with minimum disruption.

F. Periodic Checkups

It is customary for device engineering groups to periodically (often annually) check devices for general operational effectiveness – secondary power sources, interfaces, missing components, etc. Information security checks should be incorporated into this practice. In general, such checks would require some communication with the manufacturer and possible device users. While these checkups do not replace real-time systems monitoring, they are designed to catch some of the more common security issues that may arise. The checkup should include the following:

- Review of access accounts and rights to ensure that temporary or expired accounts are removed.
- Check logs for completeness and accuracy, as it is common for logging configurations to change with patches.
- Confer with manufacturer to ensure that:
    - Manufacturer documentation is current
    - Version and patch levels are current
    - Assess any changes in remote access requirements, if applicable

  - Ask whether there are any outstanding threats or vulnerabilities associated with this device
  - Determine whether there are imminent end-of-life or support issues
- Confer with application groups that receive data feeds from device to ensure that feed is still accurate and complete.
- When a vendor remotely manages multiple devices through a site to site VPN arrangement, it is incumbent to follow procedures establish by the Johns Hopkins Network Security team for enabling and/or troubleshooting connectivity associated with this arrangement. It is also expected that the vendor will advise the network security team when devices are de-installed and IP addresses can be removed from the network configurations.
- When an onsite visit by the vendor is required to apply critical security updates, acquiring departments and/or clinical device support teams should ensure that there is a financial arrangement available to accommodate any costs associated with this effort.
- Any security issues that may be uncovered should be reported to the device manufacture and the FDA.

G. Lifecycle Planning

Lifecycle management is one of the least technical yet most effective controls. Out-of-support devices are nearly impossible to adequately secure and are just as problematic during incident response. Ensuring that support models for devices are adequate across their lifecycles is the responsibility of device owners, device engineers and supply chain. With increasing attention by manufacturers on the cyber-security implications of deprecated technologies, we should expect that support cycles will change in substance and duration.

- Consideration for End-of-Support also trigger when third-party products and components are no longer supported by their manufacturers or developers and when known common vulnerability and exposures are identified but not remedied by a third party component vendor. End-of-Life and End-of-Support dates should be provided as part of their documentation discussed above and communicated clearly throughout the support period.
- For devices which will receive an End of Life or End of Support date for the first time, a reasonable amount of time must be provided for Johns Hopkins to take any necessary action

including removal of network connectivity, transition to a supported product, and to implement compensating controls. It is generally considered that three (3) years is a reasonable amount of time between communicating and making effective End-of-Life or End-of-Support.

H. Network Surveillance and Incident Response

It is the responsibility of the information security group to conduct network information security surveillance, including where applicable vulnerability scanning, anomaly detection and incident prevention. Using its standard operational tools and in addition to its role in supply chain and standards maintenance, information security is responsible for the following functions:

- Network surveillance inventories as a backstop for inventories provided by device engineering groups.
- Network segmentation analysis regarding the principal medical device segments and potential issues traversing those segments.
- Maintaining a risk register including medical devices as part of its Governance, Risk and Compliance (GRC) functions.
- Working with third party critical threat intelligence organizations to identify and communicate potential threats to medical devices.
- Implement advanced anomaly heuristics to differentiate threats from unusual but benign traffic.
- Manage incidents according to JH practices and procedures so as to escalate to appropriate levels and mitigate damage to devices themselves and other Johns Hopkins IT Resources.
- Incident analysis and potential enterprise remediation steps should be communicated in a timely fashion to device engineering groups and other stakeholders.

V. Governance

A. Capital Planning

The structure of capital planning may need to be re-assessed to capture consolidation of vendors, and changes in on-going support models.

B. Peer reviews

Information security of medical devices involves collaboration between device engineering / IT groups in a collaborative model for standards development and assessment of controls. It is the collective responsibility of these groups to ensure that security practices are being maintained throughout the enterprise. They should request periodic audits and reviews from clinical IT, information security and the Office of Hopkins Internal Audits.

C. Security Liaisons

Device engineering groups should be represented on the JHM Security Liaisons committee. This group is a primary mechanism (along with the Clinical Wireless Standards Review Committee and ICSC) for communicating standards and practices. Security liaisons also serve as the points-of-contact for incidents and emerging vulnerabilities associated with specific medical technologies.

VI. References

A. Books

None

B. Web Sites

None