MEDICAL DEVICE CYBERSECURITY LIFECYCLE MANAGEMENT

October 2020

Abstract

This document provides an overview of a lifecycle-based approach to managing medical device cybersecurity from the perspective of Medical Device Manufacturers and Healthcare Delivery Organizations. It provides a high-level overview of the four main lifecycle phases and the relationship between them. Further, it provides references to key regulations and standards as well as other leading practices provided in the literature.

In light of the importance of medical device cybersecurity, and in consideration of the growing complexity of our medical device ecosystem on one hand and the increase in the number and sophistication of cyber threats, following a programmatic and repeatable set of security processes is a requirement for any medical device manufacturer and healthcare delivery organization. We hope that this whitepaper lies the foundation for a better understanding of such approach.

We encourage MDMs and HDOs to use this document as the basis of their own Cybersecurity Lifecycle Management processes. Organizations can customize the content provided here for their own environment.

H-ISAC™ HEALTH - ISAC

www.h-isac.org

Table of Contents

Medical Device Cybersecurity Lifecyle Management

1 Contributors

This document was developed in cooperation of Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturer (MDMs). Contributors include members of the H-ISAC Medical Device Security Information Sharing Council (MDSISC) as well as IHE PCD working groups.

H-ISAC would like to thank the respective individuals for contributing their expertise and time:

Tola Amusan, Mayo Clinic
Jean Desire, ICU Medical
Phil Englert, Deloitte
Christopher Gates, Velentium
Ed Heierman, Abbott
Mat Jones, Intermountain Healthcare
Tara Larson, Abbott
Robert Smigielski, B. Braun
Axel Wirth, MedCrypt

2 Introduction

2.1 Objective

This whitepaper has been produced by a group of volunteer representatives from Healthcare Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs), sharing their respective experience and best practices for the typical lifecycle management processes required to assure and maintain the cybersecurity posture of regulated medical devices. It is intended to act as a blueprint that can be applied by HDO's and MDM's, as well as other stakeholders, and describes their respective tasks and roles as well as the interaction between process steps.

This document does not attempt to provide legal or regulatory guidance; rather it will outline generally accepted engineering best practices.

2.2 Target Audience

The intended audience of this document is HDOs, MDMs, service providers, regulators, and other organizations responsible for developing, producing, distributing, and maintaining the security posture of medical devices in a healthcare environment. The information contained in this document may be

useful to any stakeholder wishing to understand the challenges and strategies medical device stakeholders may employ to deliver and operate secure devices.

2.3 Definition of Scope

Per section 201(h) of the Food, Drug, and Cosmetic Act, the FDA defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article … intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease …." (FDA, 2019)

For this whitepaper, this includes devices and software which may otherwise be described as: machines, instruments, monitors, or diagnostic devices found in direct and indirect patient care settings (e.g., ventilators, infusion pumps, diagnostic imaging devices, clinical diagnostic analyzers, surgical robots), small wearables (if regulated medical device), implantable medical devices, medical device supporting IT infrastructure (servers, cloud, access points, etc.), medical device supporting applications, software as a medical device (SaMD), and home care devices.

Further, for this whitepaper, the equipment listed above must: 1) contain software, firmware, or programmable logic; or 2) be software that is regulated as a medical device, including mobile medical applications. In addition, this whitepaper applies to medical devices that are considered part of, or may become part of, an interoperable system and devices that are already on the market or in use. It does not intend to be applicable to consumer or unregulated devices, although the described engineering best practices could be applied there as well.

It should be understood that a) international regulations, although somewhat aligned, may vary in their specific requirements for security controls, processes, reporting, or approval and b) applicable regulations are still evolving and that new requirements, updates, or changes may occur after this paper is published. For example, the International Medical Device Regulators Forum published its “Principles and Practices for Medical Device Cybersecurity” in March 2020 (IMDRF, 2020).

2.4 Main Lifecycle Phases

Figure 1 outlines the typical phases and relationships of medical device cybersecurity lifecycle management. In addition to the main areas that are managed by the MDM and the HDO, the diagram also shows the phases as they relate to “Medical Device Manufacturer Supply Chain” management (for more detail on Supply Chain management refer to “Health Industry Cybersecurity Supply Chain Risk Management Guide” (HSCC, 2019)), as well as the “Medical Device Manufacturer Maintenance” activities and how these relate to the HDO as the main communication channel.

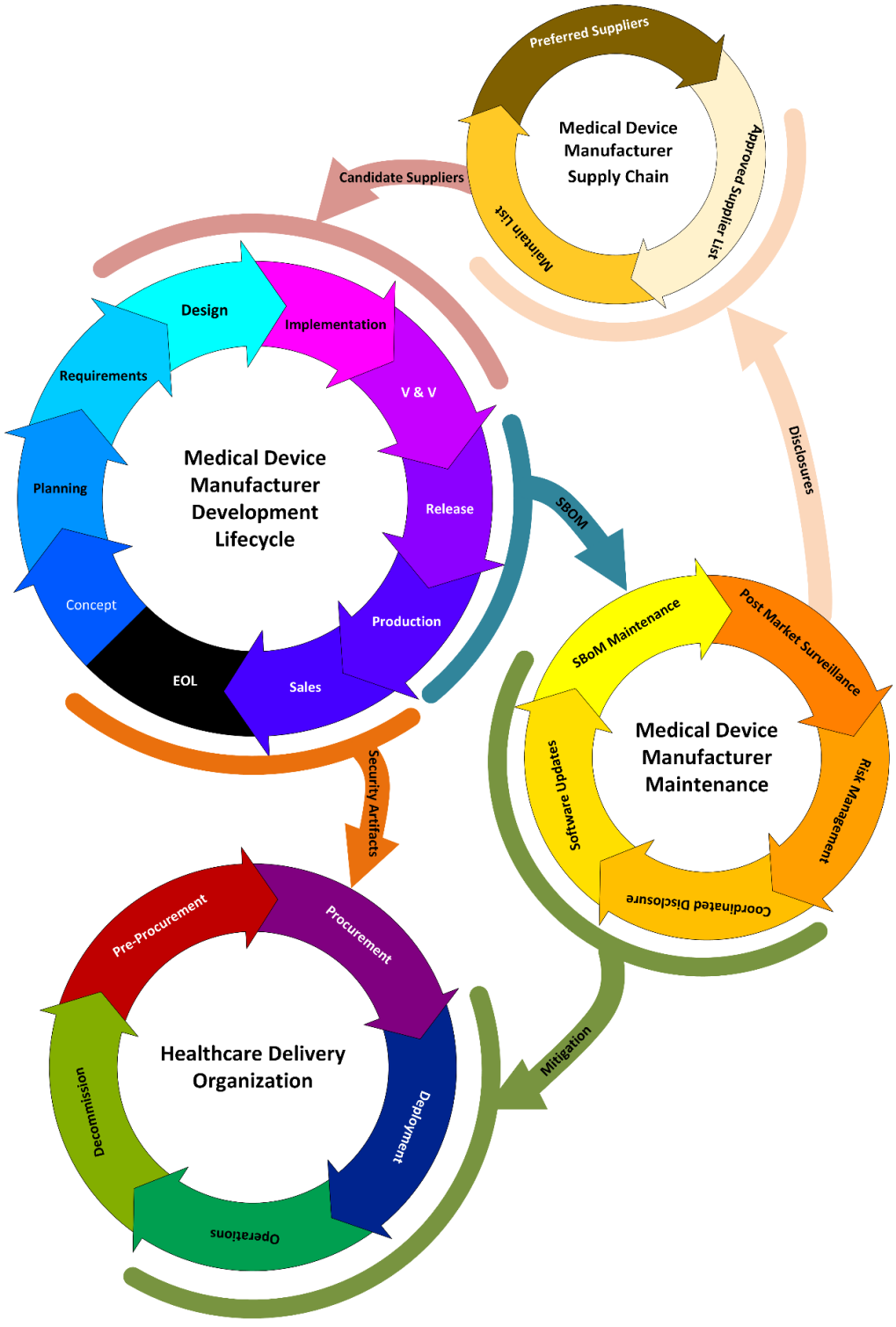

Figure 1: Main Areas and Phases of Lifecycle Management

3 Main Lifecycle Phases - Manufacturer

It is assumed that the reader is familiar with general software development best practices defined elsewhere, e.g., IEC 62304 (IEC, 2006). This document is supplemental and specifically addresses practices to include cybersecurity in the development lifecycle. A much more in-depth discussion of manufacturer practices regarding the design, development, delivery, and support of cybersecure medical devices is provided in the literature (Wirth, Gates, & Smith, 2020).

It should be assumed that throughout the Lifecycle activities formal reviews are being performed and documented; however, these are not explicitly called out in Figure 1.

3.1 Concept Phase

Specifically focused on cybersecurity during the Concept Phase, the manufacturer typically will:

- Define the security requirements for a new product, which may include user ("voice of customer") and regulatory requirements; intended use and use cases; and business ("voice of business") or legal requirements.
- Evaluate new product concepts against the criteria of meeting these initial requirements.
- Demonstrate that critical security features of one or more of the selected concepts can perform as intended.
- Identify areas of project risk: business, technical, clinical, and regulatory

This phase can also be used to analyze changes to an existing product and define desired improvements or a next generation product. This also is a time to perform a security gap analysis against that existing product. However, within the given economic limitations and design constraints, it may not be possible to implement all indicated security controls.

During the Concept Phase a manufacturer typically performs the following activities:

- Identify intended markets and security regulatory requirements; determine the regulatory strategy.
- Define restraints that could impact or could be impacted by security measures (usability, effectiveness, resource limitations, use case, etc.).
- Define development and connectivity anticipated needs (to enable consideration of future enhancements).
- Develop preliminary design concepts including cybersecurity measures.
- Research available security technologies to address identified requirements.
- Evaluate the impact of security controls on device usability and effectiveness.
- Identify user requirements for decommissioning strategy.
- Define and initiate security process and documentation requirements, e.g., risk management plan, vulnerability management, threat modeling, SBOM, etc.

- Evaluate alternative design concepts for compensating controls.
- Identify critical design features and potential security risks.
- Define critical manufacturing processes, such as security of the production environment, secure source code management, key and certificate infrastructure, etc.

As an outcome, the Concept Phase will define and document: business case, market requirements, user needs, security risks, system requirements, infrastructure requirements (production, field support, etc.), security-relevant processes, and documentation requirements.

3.2 Planning Phase

The Planning Phase supports the creation of security design inputs for both functional and non-functional requirements, system security plan, software architecture, development plan, secure development lifecycle plan, detailed hazard analysis and mitigation plan, and a marketing plan. It further should define configuration management and versioning, traceability, secure SW design best practices.

Specifically, the System Security Plan would define:

- Security activities to be performed during the development lifecycle.
- The responsible parties that will be performing and reviewing each of the activities.
- The estimated phase or time period when each of the activities will be performed.
- Regulatory security requirements.
- Security goals.
- For each of the computer languages to be utilized in a project, standard secure coding conventions (CERT Secure C; MISRA 2012 and CERT Java) should be utilized defined here and enforced later via static analysis.
- Security requirements for processes, tools, infrastructure, supply chain, training, certifications, etc. to be utilized in the development process.

3.3 Requirements Development and Analysis Phase

The primary cybersecurity objectives are the protection of Confidentiality, Integrity, and Availability (the “CIA Triad”) and should be applied as widely as possible throughout the design and implementation of software and hardware for the device/system. This enables that use-case specific security requirements are met, e.g., assurance of safety, effectiveness, and privacy.

3.3.1 General Considerations

Security should not be 'brittle', i.e., it should allow inspection or interrogation to detect outlying conditions and events not present in the normative conditions and expectations. Where possible, security measures should be layered with other security measures. This type of layered approach is referred to as "Defense in Depth".

Modes of operation should be considered in the system, especially where non-normative functionality is performed. The usual example of this is production line configuration and testing support in a device/system. While manufacturing functionality may need to be active in a device/system which is currently in the process of being manufactured, this functionality should not be present in a device/system in the field as that could be exploited as an attack vector.

The system design should ensure that in case of a compromise, the information learned cannot be used in other similar systems to facilitate additional attacks, especially additional 'larger scope' attacks, e.g., passwords, shared secrets, and keys should not be the same across systems.

Confidentiality, integrity, and/or authenticity considerations apply to clinical data (e.g., dosages or diagnostic results), patient data (e.g., PHI and PII), as well as technical data (e.g., calibration data, safety limits, log files, or firmware updates). Any vulnerability of the underlying data translates to a risk to the application and entire device and therefore a risk to safety, care delivery, privacy, and business.

Devices should be capable of detecting security compromise or an attempted attack. Interruptions to 'essential clinical performance' shall be logged and, at a minimum, be reported to the user. Delays of received or transmitted data shall, at a minimum, be reported to the user.

3.4 Design Phase

3.4.1 Secure System Design

TIR57 (AAMI, 2016) expects the Medical Device Manufacturer (MDM) to design a device within the context of a medical system such that methods are used to perform security risk management. TIR57 Chapter 3 defines the need to perform security risk management to identify assets, to identify vulnerabilities, evaluate security risks, mitigate security risks, monitor the effectiveness of risk control, and identify the linkage to safety risks.

A secure system design process formalizes the steps necessary to specify the identified security, use cases, capabilities, requirements, and mitigations. Protection of confidentiality, integrity, and availability should be applied as widely as possible throughout the design and implementation of software and hardware for the system security design. Exposing vulnerabilities in design and implementation can be done at this point, so areas of concern can be identified.

Figure 2 'Design for Security' point 1 depicts 'System Design' and defines it as the process which formally decomposes a set of requirements into a list of potential vulnerabilities. This is done by using a defined formal process which is used to score the potential, unmitigated vulnerabilities.

Vulnerabilities which impact the business model and vulnerabilities which are a potential impact to patient safety and efficacy are both indicated.

The goal of security is to identify and control risks related to safety, care delivery, privacy, and business. Design for security is the process of identifying business risk to the MDM and the customer. The vulnerability impact score is used to prioritize potential vulnerabilities for the implementation of mitigations.

Both of the areas of business impact and patient safety and efficacy are scored in consideration of severity and exploitability. Scoring methods can help determine the severity and exploitability when performing an analysis of a vulnerability.

AAMI TIR57 recommends the creation of a separate risk analysis process focused specifically on impacts that are identified by a security analysis. It describes various security risk assessment processes used to establish a set of threats, vulnerabilities, analyses, and assessments. TIR57 blends security and safety risk management by showing how to apply the principles presented in ANSI/AAMI/ISO 14971 (ISO, 2019) to security threats that could impact the confidentiality, integrity, and/or availability of a medical device or information processed by the device.

3.4.2 System Design

How can design for security be transformed from a state of paranoia to a formal process with explicit traceable goals? System Design is the ideal time in the process to formally assess the security of the design. This is medical device security by design.

Regulations, guidance, and customer expectations demand that the system design can be shown to be both safe and secure. In this way the HDO can accept the device's impact on their business IT infrastructure system and the clinical staff can expect both safety for the patient and security for the patient, clinician, and the HDO. This also allows the MDM to protect their business model from loss of intellectual property, loss of reputation, loss of business due to cloning, etc.

Figure 2 shows milestones as enumerated points in the figure labeled 1 through 8. These points highlight the key milestones in the process of the overall system design. The entire process is informed by the details in TIR57 with a focus on the lifecycle aspects of system level design. Here we take on the lifecycle view to describe the larger process required to manage a device/system.

Note that this concept applies to the vulnerability triage during the design phase and that it typically does not (yet) include "inherited" vulnerabilities from third party software components as these may be addressed later in the development phase.

In addition to the actual device or system requirements, the design phase should also consider security requirements for the supporting infrastructure, e.g., production needs, deployment, and secure maintenance and update.

3.4.3 Threat Modelling during the Design Phase

Threat modeling is a security analysis process that can be applied to identify design vulnerabilities during product design. The threat model decomposes product topology, data flows, processes, and data stores down to a list of potential vulnerabilities for purposes of scoring by a separate process. The

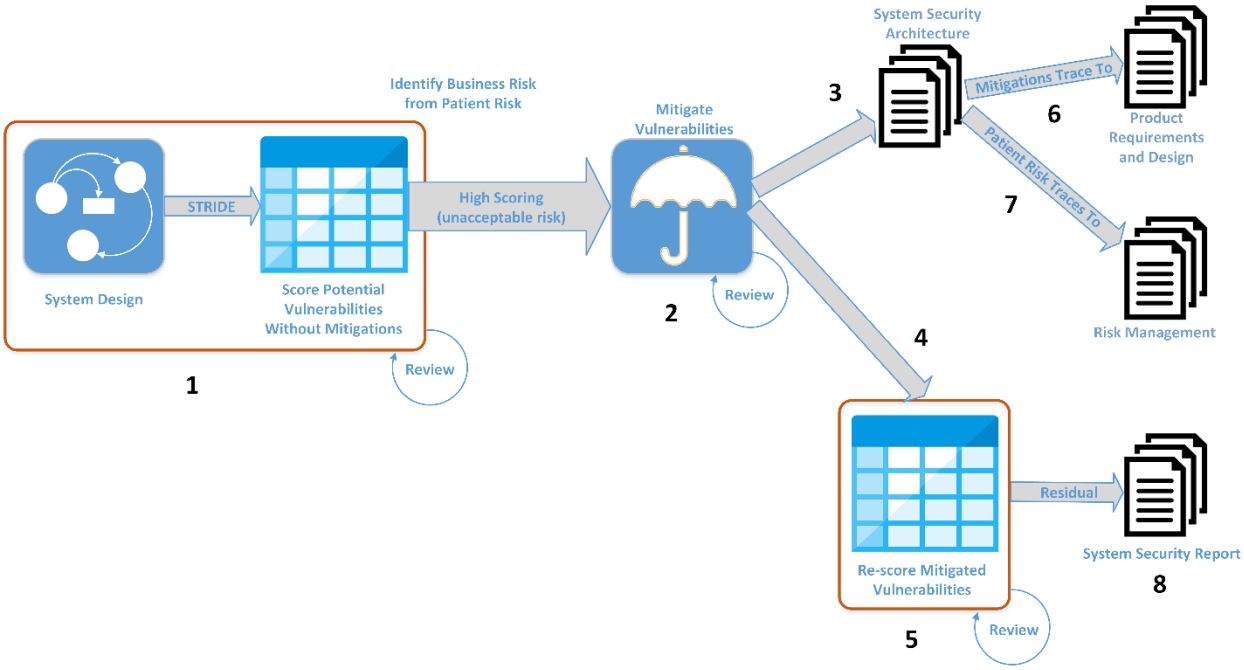

Figure 2: Design for Security

goal of using threat modeling is to identify high risk vulnerabilities for mitigation. The result is a list of vulnerabilities that are not yet mitigated but should be addressed (or accepted if the risk is sufficiently

low[1]). For each vulnerability the designer can select the appropriate mitigation technique and document the mapping. This formal review process output is provided as input to the development team to implement the mitigations as part of normal and typical development activities. These documented mitigations are then traced into the normal development document tree, including requirements, detail design, and hazard analysis.

This process is performed in two steps:

- The first assessment does not consider the effectiveness of any mitigating controls. This is indicated by point 1 in Figure 2.
- The second step includes the effectiveness of implemented mitigating controls. This is indicated by point 5 in Figure 2.

Vulnerability scoring can be done by any number of scoring metrics including a well suited and established one named the Common Vulnerability Scoring System (CVSS), which is discussed in AAMI TIR57. This list of "potential vulnerabilities" are scored utilizing a vulnerability scoring method in light of the unique use case of each medical device. While not mandated, CVSS is a practical scoring method which takes into account the severity and exploitability of the vulnerability as important elements of developing the score. Note that CVSS has some limitations with regards to scoring vulnerabilities in the context of a finished device and the actual use context and variations or alternative scoring methods are known in the industry and can be used to calculate the metric. (Note: CVSS v4 will improve on this as it will add in the "collateral damage" rating. Further, a more context-aware and rubric-based version of CVSS has been proposed (MITRE, 2019)).

CVSS "Collateral Damage" metric is included in the "Environmental" grouping. This metric is semantically equal to "Severity" of the vulnerability being exploited, and this is the single most important metric when applied to a medical device. Scoring during the design phase metrics is used to create an overall score that is inclusive of severity, exploitability, as well as impacts to confidentiality, integrity, and availability. Scoring rubrics that do not work well at design time are those which focus on the fielded device by using the category of the "likelihood" of an event. A device under design cannot yet exist in the marketplace so there cannot be any relevant concept of an attack likelihood (except when historic data from a predicate device exists). The resulting documentation is evidence of the vulnerabilities, scores, priority, and proposed implementation. That data is then formally reviewed to become a part of the Design History File (DHF).

Concurrent with vulnerability scoring, an assessment should be performed on each vulnerability if there is a potential for this vulnerability to impact patient safety of treatment efficacy. In cases where this is found to be true, then this vulnerability should be communicated to the normal Safety Risk Management process.

[1] Note that the MDM and HDO may apply different risk criteria or have different risk tolerance and therefore an HDO may still decide to take action (mitigation or use of an alternate device) even if an MDM classifies risk as acceptable.

The assessment of the vulnerability should include an impact on the device functionality and if altered, whether that change creates a patient safety hazard or impact device efficacy or performance. If true, refer to your company's Safety Risk Management process.

3.4.4 Mitigate Vulnerabilities

Mitigating vulnerabilities is indicated by point 2 in Figure 2. The input is the listing of high-scoring vulnerabilities. The high-scoring vulnerabilities are reviewed to determine if further action is required (e.g., via a design decision) to reduce the vulnerability to an acceptable level.

Vulnerability mitigations are treated in the same way as typical product implementation issues. This provides traceability to the origin of the issue and provides the tools necessary to prioritize the effort. Investigate ways to mitigate the high-scoring vulnerabilities and in cases where this is not possible then "accept" the risk. In the cases where the risk is accepted, then a residual vulnerability is documented and a risk/benefit analysis (FDA, 2016) should be performed to justify allowing this residual vulnerability to remain in the medical device. This step in the process represents the effort to find mitigations, document mitigations, and document non-mitigations.

The ideal situation is to mitigate a vulnerability with a strong, well-understood security solution. The security solution and the reasoning behind its application should be documented. A documented (typically in the Design History File (DHF)) review will be performed at this step in the lifecycle to show traceability of the high scoring vulnerabilities to their respective mitigations and to determine if there is a possibility that the planned mitigation could create a patient safety risk.

3.4.5 System Security Architecture Document

The System Security Architecture Document is indicated by point 3 in Figure 2. At this point in the design process, business decisions affect the level of acceptable security risk defined in the System Security Architecture documentation. The level of acceptable security risk and design mitigations are documented in the System Security Architecture artifact. This set of documents traces the system design components, vulnerabilities, mitigations, and results of the formal review. Based on the analysis of the vulnerabilities, the mitigations described in the System Security Architecture can be written in a way that ordinary developers can use to implement the mitigations, without necessarily being experts in cybersecurity.

3.4.6 Rescore Mitigated Vulnerabilities

The rescoring of Mitigated Vulnerabilities step is indicated by point 4 in Figure 2 and leads to the documentation of residual vulnerabilities (steps 5 and 8). The output of the mitigation formal review is the gate to the process of re-scoring vulnerabilities after mitigation has been designed. The implementation of each mitigation is mapped to testable requirements and stored in the security requirements document as per AAMI TIR57 section 6.3. The primary function of this step is to review

the vulnerabilities that have been mitigated. Each mitigated vulnerability must be reviewed to determine the vulnerability score with the mitigation in place. Each score must take into account the impact on the business model and potential impact on safety and efficacy. Additionally, each mitigation should be assessed to determine if it introduces new risks. The results are stored in the Design History File (DHF).

3.4.7 Review of Mitigated Vulnerabilities

The review and documentation of mitigated vulnerabilities is indicated by point 5 in Figure 2.

TIR57 section 7 speaks to residual risk so that during the review the decision pertaining to vulnerabilities with impacts on safety/efficacy can be justified in a risk/benefit analysis. The output of this review is a document defining the decisions on vulnerability mitigations with any deviation from established criteria being documented as well. The output document is part of the System Security Report (see 3.4.10).

3.4.8 Design Outputs

The Design Outputs are indicated by point 6 in Figure 2. The output of System Security Architecture includes the typical design documents such as product requirements, product design, and the risk management plan. The classic system design artifacts are presented as normal items in the DHF.

3.4.9 Risk Management File

The Risk Management File is indicated by point 7 in Figure 2. In the Risk Management File, the linkage of data flowing from the design side where cybersecurity is managed to the classic risk management activities are documented and, as applicable, mapped to the software requirements. This document is used to describe items that are not necessarily cybersecurity topics but which need to be examined for safety/efficacy in the traditional risk management workflow.

3.4.10 System Security Report

The System Security Report is indicated by point 8 in Figure 2. This document brings together the scored vulnerabilities and decisions on corresponding mitigations. The documentation is used to inform the implementation process of the system security needs and inform the development teams about required mitigations.

The Design Outputs combine to produce the product requirements, product design, risk management plan, and System Security report of secure design.

3.4.11 Software Bill of Materials

Several standards such as the Joint Security Plan (JSP) (HSCC, 2019) and TIR57 as well as FDA Cybersecurity Guidances are recommending that new medical device designs include some form of a bill of materials describing the software used in the device (commercial, open-source, and application software). The Software Bill of Materials (SBOM) is a listing of the medical device software component names, manufacturers, versions, and supply chain relationships between them. The current state of the SBOM specification and format remains an evolving field with the NTIA leading the way in standards development (NTIA Framing Working Group, 2019). The SBOM should be included as part of the product Design History File (DHF) and made available to the HDO, regulatory bodies, and applicable stakeholders as required.

Please refer to section 4.5 SBOM Monitoring and Maintenance for more information.

3.5 Implementation

Implementation of the design, including the security requirements defined during the design cycle, requires not only following software engineering best practices and previously established secure coding conventions, but also includes a security-focused approach to continual testing.

Common testing techniques include:

- Application Security Testing (static or dynamic – SAST or DAST): analyze application source code, byte code, and binaries for coding and design flaws that could indicate an underlying security vulnerability.
- Fuzz Testing: exposing communication mediums and software interfaces to invalid, unexpected, or random data.
- Boundary Value Analysis (BVA): specifically testing a software interface against the boundary values of the specified range.
- Penetration testing: simulation of a cyber-attack through a friendly team (internal or contracted) that uses tools and experience to uncover device vulnerabilities.

It is critical that these types of software testing techniques are applied as early as possible during the implementation process and are repeated at every major milestone. Of the above testing methodologies, many can be performed using automated tools that typically get tuned to the respective test case. Penetration testing usually is more reliant on an experienced human tester that should be part of a separate organizational entity or even an externally hired resource.

Once software components and the final build have successfully passed this series of tests (with an acceptably low residual risk for unmitigated implementation vulnerabilities that have been discovered), the product formally enters the verification and validation (V&V) stage for final system level testing.

3.6 Verification and Validation

Verification and validation are very important activities to ensure that the medical product is built correctly, addresses stakeholder and user requirements, meets the intended use, is safe and secure, and is suitable to be used in the intended environment. Unfortunately, it has been common practice to start verification and validation (V&V) activities at the end of the development lifecycle. This means the V&V team may not have sufficient time to influence the requirements and development of the medical device.

Starting cybersecurity verification and validation at the end of the development lifecycle is not a recommended practice. These types of activities should start early in the product development lifecycle and continue until the obsolescence of the medical product. Starting V&V activities early in the development lifecycle would enable the team to establish early verifiable cybersecurity requirements and security risk control measures, as outlined in TIR57.

Verification and validation activities (such as testing and analysis) should also be conducted to ensure proper implementation of cybersecurity requirements. In accordance with Health Canada's Pre-Market Requirement for Medical Device Cybersecurity guidance (Health Canada, 2019), cybersecurity testing should be conducted against known vulnerabilities, malware, malformed inputs, and structured penetration. Additionally, static source code, binary, and bytecode analysis should be conducted to identify weaknesses in the code that can be exploited. The Australian Department of Health (Therapeutic Goods Administration, 2019) also recommends the use of penetration testing to evaluate the effectiveness of the medical product to manage malicious attacks. In addition, V&V activities should be conducted to ensure applicable risk controls are properly implemented.

The environment in which a medical product will be deployed can also play an important role in ensuring the security and safety of the medical product. As such, the MDM should assess the security of third-party operating systems and hardware platform environments. Assessment of environmental factors can show weaknesses that should be addressed as part of the product security control.

3.7 Release

Releasing a medical product is a very important milestone for MDMs and HDOs. The new product may contain important features that can enhance and improve patient safety. However, to take advantage of the new features, MDMs should make available appropriate documentation that details the new features, bug fixes, and the security posture of the medical product. Providing proper release documentation can help HDOs establish appropriate measures to ensure the safety of their patients and security of their IT infrastructure.

Release documentation should include the list of known vulnerabilities uncovered (vulnerability disclosure) but that were not mitigated during the development lifecycle activities. The MDM should assess the severity of each of the vulnerabilities identified in the list. The Common Vulnerability Scoring System (CVSS) is one of the tools that can be used to assess the vulnerabilities. The MDM

should also determine the appropriate discloser of those vulnerabilities to agencies such as FDA, ICS-CERT, National Vulnerability Database (NVD), etc., as well as an ISAO such as H-ISAC, Sensato, or MedISAO.

In addition to the known vulnerabilities list, the MDM should make available a system security test report, Software Bill of Material (SBOM), manufacturer disclosure statement for medical device security (MDS2), disclose residual security risks, and provide plans for postmarket surveillance, software security maintenance, and end of support/life (EOS/EOL) activities. These are important documents to help HDOs in their effort to secure their medical device infrastructure, understand possible vulnerabilities in the devices, and establish applicable security measures that support the HDO's cybersecurity strategy.

3.8 Production

Upon completion of design, implementation, V&V activities, and approval by the FDA, the product is transferred to production. The following are cybersecurity considerations for this stage of the product lifecycle that assure:

- Software integrity of the released build and verify that no changes, accidentally or intentionally, are introduced after engineering release and regulatory approval. This includes all software components that make up the released version: application, open source, and commercial.
- That software integrity is maintained in the production vault and during the production process and that there is a formal process being followed for any version updates to the released build.
- Full traceability of the build process and enable phase-in of any critical updates or patches that may be required during the production process (based on production stage as well as update criticality).
- Integrity of the production process, including supply chain integrity, to prevent unauthorized changes to the software build that could result in a compromised product (e.g., unapproved version, introduction of malware, etc.)
- Integrity of the key/certificate management infrastructure and deployment process (if cryptographic security is used).
- Confidentiality of key information such as software, supporting documentation, and cryptographic keys to protect intellectual property.
- Preparation of devices for warehousing and distribution (e.g., disable all test and debugging functions, put device in low power mode, etc.)

Assurance of build software integrity and the overall production environment is critical. Many MDMs rely on manual processes to do so but considering the complexity of today's medical device manufacturing processes as well as the increasing sophistication of cyber threats, we suggest that tools and a programmatic approach are required.

Further, the production environment (production servers, workstations, industrial control systems (ICS), robots, etc.) needs to be protected from cyber compromise to avoid costly shutdowns of the manufacturing line, compromised products, and potentially costly recalls. This requires both a security technology approach (deployment of the right security tools to device and across the production network) as well as security processes (to address security training, auditing, incident response, etc.).

3.9 Sales

As our understanding of the culture around medical device security changes, so too will the interactions that Sales has with customers about cybersecurity. Sales must be a constructive partner in the security communications process, which includes:

- Providing upfront information on the company's security strategy, device security posture, and MDM processes.
- Providing security documentation (SBOM, MDS2, etc.) upon request such as during an incident response process, the presales (RFI, RFP) information requests or the procurement (bid, contracting) process.
- Assessment and negotiation of the security requirements stipulated by the HDO in the contract.
- Helping customers gather information on specific security questions and, as needed, connect customers with MDM SME resources.
- Supporting customers with security incidents (in cooperation with MDM SME resources).

However, we need to be aware that cybersecurity related information is highly technical, is typically generated by engineering, should be formally approved as part of the release process, and resides in the Design History File (DHF). Even though listed as part of the sales process, it should not be treated like other sales collateral and should be backed up by the appropriate cybersecurity expertise and document management processes.

As such, the sales role has been changing to that of a partner on all cybersecurity matters, helping customers to assess a product's cybersecurity capabilities, and allowing them to purchase with confidence.

3.10 Medical Device End-of-Life (EOL)

The End-of-Life phase and concept are often not well understood nor well defined and may be treated differently by different people. To complicate matters further, medical devices are complex systems of systems with individual components that have their own lifecycle. However, it is recognized that medical devices often out-live their components and additional guidance for EOL management would be beneficial. No clear best practice is provided on how to define and communicate the measures taken by the MDM to mitigate the risk of the use of a component that has reached EOL. Clear definition of the respective phase steps as well as communication to the HDO is required to establish

how the MDM is managing end-of-life. Currently, there is no industry consensus on the acceptability of EOL management for the entire product or individual software components by an MDM.

For example, JSP section VII:C:vii “End of Life/End of Support and Decommissioning” includes the following considerations:

- End of life support includes identification when third-party products are no longer supported.
- At a minimum, providing 3 years advance notice when a medical device will reach end of life (end of support).

A more granular definition is provided by TIR97 section 7 “Retirement/obsolescence” highlighting the following end-of-life phases, and providing guidance on general considerations and customer communications:

- End of development
- End of production
- End of guaranteed support
- End of support

Another formal step that is applied by some MDM’s, the end of sale, following more or less closely after end of production.

In summary, EOL management can be complex, may require technical, contractual, licensing, and communication activities, and may vary widely by device type and market. Also, it should be understood that HDO decommissioning may occur at a later date than the MDM’s EOL.

4 Main Lifecycle Phases: Cybersecurity Maintenance

Cybersecurity Maintenance is a joint effort, where HDOs and MDMs are expected to take appropriate measures to prevent unauthorized access to the medical device and the environment where the medical device resides. To facilitate this effort, the MDM should coordinate cybersecurity efforts with the HDO by sharing updated information, such as version number, impacted features, applicable requirements, and known vulnerabilities of third-party software incorporated as part of the medical device. This type of information can also help the HDO to establish cybersecurity measures to ensure the safety of the medical device and prevent events that could lead to patient harm.

Planning for the required activities to maintain an effective medical device in the market should start early in the medical device lifecycle, preferably during the concept (section 3.1), requirements (section 3.3) and design (section 3.4) phases. MDMs should properly plan required activities to maintain the trustworthiness of the medical device during its lifecycle and design the product to be maintainable. The maintenance activities should focus on ensuring the medical device is operational and secured per its intended use.

The maintenance plan, at a minimum, should include required activities for (1) post-market surveillance, (2) incident and vulnerability management, (3) software updates, (4) coordinated disclosure management, and (5) SBOM Maintenance. Based on the nature of the medical device, contractual requirements, and applicable regulatory requirements, MDMs and HDOs may conduct additional activities to ensure the safety and effectiveness of the medical device in the market. Regulators, like the FDA or Health Canada, also emphasize the need for a maintenance plan that describes post-market processes to ensure the safety and effectiveness of a medical device during its lifecycle.

Figure 3, Maintenance Cycle, depicts typical activities conducted to maintain a secure medical device in the market. Item 1 includes listening systems, such as the National Vulnerability Database (NVD), vulnerability scanners, ISAOs, manufacturers and suppliers, threat streams, and media outlets that can be used to monitor threats and vulnerabilities that may impact the items in the SBOM and effectiveness of the medical device. Item 2 identifies the ongoing activities of monitoring items in the SBOM for disclosed vulnerabilities, reviewing the impact of the vulnerability to the medical device, and post-market reporting activities. Finally, item 3 depicts internal activities (e.g., CAPA, Tiger Team) manufacturers may take when vulnerabilities are identified that may associate a risk to patient harm and/or influence the effectiveness of the medical device.

TIR97 (AAMI, 2019) section 6 “Postmarket management of fielded devices” discusses an overall process for post-market management of medical devices. The HSCC Medical Device and Health IT Joint Security Plan also provides guidance for maintaining a secure medical device in the market in section VII, C. “Complaint Handling and Reporting” and subsection vi. “Vulnerability Management and Patch Management”.

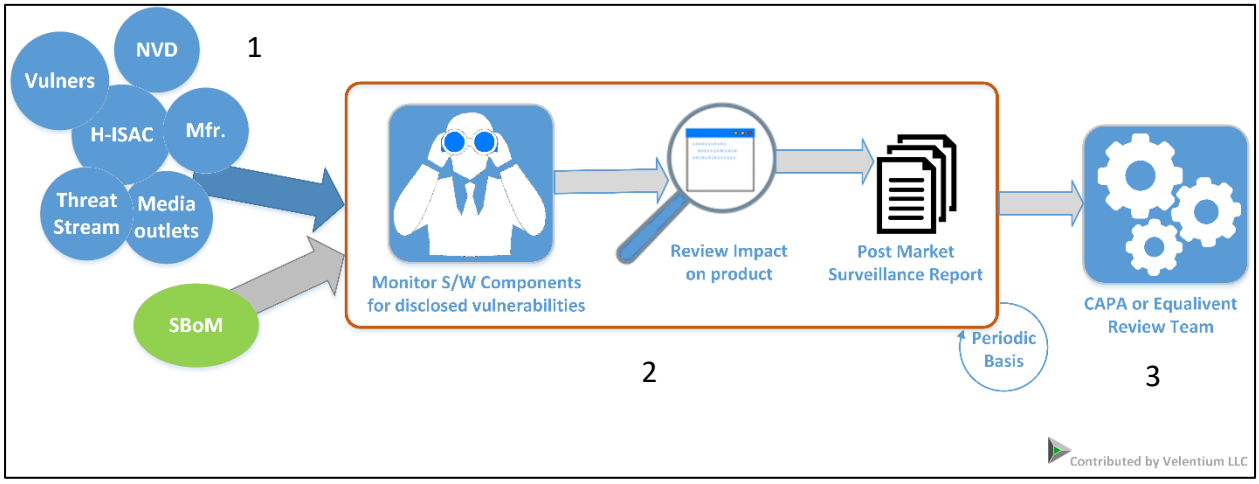

Figure 3: Maintenance Cycle

4.1 Post Market Surveillance

A cybersecurity signal is information that indicates the potential for or confirmation of, a vulnerability, exploit, threat, or threat event that affects, or could affect a medical device. Post-market vulnerability surveillance is the action of identifying cybersecurity signals related to the medical device and determining if the signal represents a vulnerability with the medical device.

The MDM is primarily responsible for post-market vulnerability surveillance and should implement security monitoring procedures. When implementing post-market vulnerability surveillance:

- If possible, leverage established IT resources such as threat intelligence and vulnerability scanning. For example, perform platform vulnerability scanning on the products by deploying them in an MDM environment configured for customer use.
- Make use of the SBOM to monitor third-party components. The SBOM information can be used to check vulnerability repositories such as the National Vulnerability Database to identify cybersecurity signals.
- Incorporate multiple sources in the monitoring system, including customer complaints.
- Clearly communicate the responsibilities of the HDO.
    - For a closed-system medical device, the HDO will almost completely rely on the MDM for monitoring and remediation. For these devices, it may not be possible for the HDO to perform platform scanning or to apply patches.
    - For an open-system, the HDO may be able to perform some monitoring and remediation activities, such as platform scanning and applying patches. It is important to communicate when these activities can or cannot be performed as some devices may not respond favorably to this type of interrogation.
    - In almost all cases, the HDO will be responsible for monitoring their environment while ensuring compatibility and security with the medical devices.

See TIR97 section 6.1 “Observation and transmission” for additional guidance.

4.2 Vulnerability Management and Incident Response

Vulnerability management involves assessing risk when a new cybersecurity signal is identified, and determining if a risk treatment decision is needed. TIR97 section 6.2 “Assessment” provides guidance for assessing a cybersecurity signal for a cybersecurity impact.

An assessment is performed on new cybersecurity information to determine if the product is impacted. It is possible that the cybersecurity signal has no impact. For example, assume a vulnerability is discovered with a third-party component used by the product. If the functionality associated with the vulnerability is not used, then that vulnerability does not impact the product. When the cybersecurity signal impacts the device, then the cybersecurity risk assessment process is performed to establish the risk value, make risk treatment decisions, and implement a risk treatment plan. The outcome may require updating an existing risk or creating a new risk.

Currently, there is no clear approach for communicating to the HDO when a cybersecurity signal associated with a third-party component does not impact the medical device. It is an on-going discussion within the industry on establishing a common reporting mechanism for this information. For example, it may be possible to provide supplemental information to the HDO that aligns with the SBOM and identifies when a vulnerability of a third-party component does not impact the product.

TIR97 section 6.3 “Action” provides guidance on determining actions to take based on the outcome of the assessment.

It is important to capture relevant information and provide traceability from cybersecurity intake through resolution, as noted in section 6 of AAMI TIR97. These activities can be managed through the defect tracking process, like traditional product defects. The security risk assessment information can be documented as part of the defect tracking process, and the cybersecurity risk management report can be updated based on the outcome of the assessment.

4.3 Coordinated Disclosure

Effective reporting of newly discovered cybersecurity issues (threats, potential vulnerabilities, design weaknesses, security events, etc.) and the impact of actual vulnerabilities is an important element of the Medical Device Maintenance Lifecycle. TIR97 section 6.3.3 “External communication” highlights multiple external communication paths to report the severity and scope of impact of a vulnerability. Stakeholders include the customer/HDO, Information Sharing and Analysis Organizations (ISAOs), and government agencies. When communicating with an HDO, existing communication channels between the manufacturer and the HDO should be leveraged. It is recommended that these existing communication channels be extended to include cybersecurity, rather than the creation of new communication paths and contacts.

Communication is extremely important during a Coordinated Vulnerability Disclosure (CVD) event where an independent security researcher has reported a potential vulnerability with the medical device. Multiple internal and external stakeholders will need to be kept informed.

The Medical Device Innovation Consortium (MDIC) *Medical Device Cybersecurity Report on Advancing Coordinated Vulnerability Disclosure* provides guidance for an MDM on establishing a CVD process. The report highlights:

- The need to establish a respectful relationship with the security researcher; and
- The importance of establishing CVD policies and the involvement of the entire MDM organization; and
- The collaboration with government agencies, such as the FDA and DHS; and
- The best practices to follow when establishing a CVD process.

The Joint Security Plan also provides communication guidance and a Coordinated Vulnerability Disclosure Workflow, in section VII, C. "Complaint Handling and Reporting" and subsection iii. "Security Incident Management, Response, and Communication" as well as through "Health Industry Cybersecurity Information Sharing Best Practices" (HSCC, 2020).

4.4 Patching and Software Updates

TIR97 section 6.3.2 "Software maintenance" and JSP VII, C. "Complaint Handling and Reporting" and subsection vi. "Vulnerability Management and Patch Management" provides specific guidance for patch generation and distribution.

When implementing patches and software updates to mitigate a vulnerability:

- It must be clearly understood and communicated on whether cybersecurity patching is a responsibility of the MDM or the HDO. Typically, when a medical device is a closed system, the MDM is responsible. If the medical device is an open system but all patches must be approved by the MDM, then the HDO will need to obtain approved patches from the MDM. Finally, if it has been communicated that the HDO is completely responsible, then the HDO can apply patches as necessary.
- The speed of response can also be driven by the impact of the signal. If a signal has no impact, then an immediate application of the patch may not be required. In that case, the patch can be implemented as part of the standard release cycle.
- To improve the speed of response, an MDM should create a regular patching release schedule. This supports cybersecurity hygiene and decisions to update as part of the next scheduled release when it is not necessary to immediately apply a patch.
- It is advisable that MDMs establish practices that can be driven:
  - by need (e.g., release critical patches within xx days), or
  - by schedule (e.g., perform SBOM review and release applicable updates/upgrades at a minimum of once every xx months).

4.5 SBOM Maintenance and Monitoring

Maintaining the SBOM is critical in ensuring the safety of the medical device in the field. An MDM should update the SBOM as needed to ensure it includes up-to-date supported third-party software, COTS (commercial off-the-shelf software), SOUP (software of unknown provenance), and version numbers.

The SBOM should be used by the MDM to monitor the SBOM components for new vulnerabilities. It is important that new vulnerabilities are identified and assessed so that unacceptable risks are not introduced to the medical device. When suppliers of the SBOM components release fixes that address vulnerabilities, these fixes should be evaluated and included in future device patches/software updates (see section 4.4 Patch and Software Updates) as appropriate.

MDMs should use appropriate listening systems, such as a complaint reporting system, an ISAO NVD, ICS-CERT, and applicable databases to maintain awareness of published vulnerabilities related to the SBOM components. Medical devices often do not use all features available in a third-party software or SOUP to perform its intended use. Therefore, cybersecurity vulnerabilities or risks associated with the third-party software or SOUP may or may not be exploitable in the given implementation and therefore, may or may not impact the safety and security of the medical device. The MDM should conduct appropriate assessments to identify if the vulnerability impacts the safety, security, and functionalities of the associated medical device. The assessment should include, but is not limited to, assessing the severity of the cybersecurity vulnerability (CVSS scoring may be used but may need to be adjusted for the use case context) in the medical device, and whether or not the vulnerability can contribute to an unacceptable cybersecurity residual risk of patient / user / operator harm. In cases where the vulnerability does not impact the medical device in question, cybersecurity-countermeasures are in place, or the device does not use the vulnerable feature, the MDM should advise the related customers and HDOs of the assessment result.

Medical device manufacturers are responsible for the safety, security, and functionality of their medical devices. In addition, to identify cybersecurity vulnerabilities in third-party software items, the MDM should also work with the manufacturers of those items to ensure that appropriate structures are in place to prevent, identify, and respond to cybersecurity vulnerabilities in the product. In cases where the MDM cannot coordinate with the manufacturers of the third-party software items, the MDM should establish appropriate measures to ensure vulnerabilities in those items are addressed as part of the medical device.

5 Main Lifecycle Phases – Supply Chain

The concept of a manufacturer developing a list of preferred suppliers is nothing new. These are the "superstar" suppliers you have thoroughly assessed and reviewed, and who are willing to negotiate on your terms. Focusing on just a few selected suppliers can streamline purchasing overheads; negotiate advantageous pricing; improve quality; and reduce upfront costs via payment terms.

Managing cybersecurity of the supply chain has become more important than ever as sophisticated adversaries are increasingly using the software supply chain as an attack vector (Schneier, 2020). More guidance on managing third party suppliers is provided by NIST (NIST, 2015) and the following provides a summary of some of the key points.

5.1 Preferred Suppliers

Suppliers are an important part of maintaining an effective cybersecurity capability for product development, production, and support. Evaluation of suppliers and supplier products from a cybersecurity perspective includes a number of areas that should be addressed. In general, agreements with suppliers include security practice expectations (for product as well as development and production environments), provision of evidence of compliance, and notification of vulnerabilities, breaches, and security incidents:

- Secure development and design:
    - Provide evidence that design processes follow a secure lifecycle process and are documented, repeatable, and measurable.
    - The product is tested for code quality and vulnerabilities.
    - Tools and processes that perform malware protection and detection as they may be used on the product are described.
    - Product and component SBOMs including all sub dependencies are documented and have a known distribution and update mechanism.
- Security management:
    - Provide evidence that vulnerabilities are identified and mitigated.
    - Vendor stays current on emerging vulnerabilities and has documented methodology to address newly discovered and "zero day" vulnerabilities.
- Secure Production and Distribution:
    - Provide evidence that security of the production environment is actively managed and monitored.
    - Provide evidence that configuration and change management processes are documented.
    - Tools and processes that perform malware protection and detection to protect development, production, and remote access environments are described.
    - Provide evidence that the integrity of software code is assured (tamper protection).

    - Physical and network security measures, including e.g., access control, are in place, documented and audited.
- Other:
    - Employee background checks are conducted.
    - Distribution process security is addressed in policy and practice.
    - Approved and authorized distribution channels are clearly documented.
    - Component end of support / end of life process are addressed in policy and practice.

5.2 Approved Supplier List

The ASL should be utilized to inform future purchasing decisions, as well as drive code reuse for future projects at the manufacturer. Areas that should be addressed are:

- Security requirements are included in every Request for Proposal (RFP) and contract.
- The manufacturing security team works to address vulnerabilities and security gaps.
- Discovered vulnerabilities and breaches are communicated between parties.
- Secure Software Lifecycle Development programs are established.
- Access by service vendors is controlled.
- Additional business arrangements may be required, e.g., escrow of source code.

5.3 Maintain List

The ASL should be constantly maintained and informed via:

- Audit results.
- Outcome of post market surveillance and discovery of vulnerabilities.
- Timely addressing of vulnerabilities and release of workarounds/patches/new versions.
- Suppliers compliance with defined security requirements.

Supplier management is a critical, security relevant task that requires the attention of every MDM.

6 Main Lifecycle Phases – Healthcare Provider Organization (HDO)

6.1 Introduction

Analogous to the MDM lifecycle, there is a device lifecycle that relates to the owner or operator of a medical device, i.e., the healthcare delivery organization, or other care services entity) – see Figure 1. There are distinct touchpoints where information flows between the MDM and HDO lifecycle, e.g., at the time of procurement (HDO specifying security requirements, MDM providing security documentation such as MDS2, SBOM, secure configuration) or during vulnerability disclosure (HDO) and device maintenance activity (MDM).

6.2 Pre-Procurement

Ideally, cybersecurity of the medical device and networked clinical environment begins at organizational leadership and governance with a formalized and defined Medical Device Security Program (MDSP), as for example defined in the ISO/IEC 80001 (ISO/IEC , 2010) series, addressing the following areas:

1. Governance: Governance should define the purpose, goals, and scope of the medical device security program. The MDSP should have a defined span of control, decision rights, and reporting requirements and typically defines policies, roles and responsibilities, performance metrics, etc.
2. Risk Management process: The MDSP should be aligned with the overall business and environment of care risk management processes. This may overlap with patient safety, compliance, IT Security or business risk management processes. Communication and coordination between related processes are a must to avoid duplication, gaps, or conflicts.
3. Risk acceptability criteria: A risk assessment model, including defined risk acceptability criteria, should cover considerations around patient safety, operational impact, financial impact, regulatory and legal risks, and privacy and should be utilized to help the organization to assess and manage the risks associated with medical device technology.
4. Roles and responsibilities: roles and responsibilities should be clearly defined and understood. Roles may include membership from the following: Chief Information Security Officer, Healthcare Technology Management, Clinical Quality, Infrastructure, Information Security, Supply Chain, End Point Support, Communications, Risk Management, Privacy, Legal, and MDSP.
5. Additional considerations that may require attention are:
    a. Documentation and tools requirements
    b. Budgets, staffing, training
    c. Auditing and enforcement
    d. MDM capability to support HDO incidents

e. Replacement Planning (inclusive of cybersecurity)

As part of the pre-procurement process, an organization should perform a general needs and requirements analysis, identifying both short-term tactical security needs, as well as long-term strategic goals for the larger ecosystem.

An HDO may collect vendor input through a formal Request for Information (RFI), a defined information gathering process specific to medical device security. Artifacts and management information should be defined, including when and how requests are communicated to the vendors and how the information is utilized in the review and decision-making process.

General publication of requirements is helpful when setting process expectations and defining the required level of detail. These may include a minimum set of expected security controls, template Business Associate Agreements (BAA), third-party hosting requirements, and post purchase support requirements.

6.3 Procurement

Procurement is the key step during which an HDO can assure that its technical and procedural security requirements are being met. Key steps during the procurement phase include:

1. Requirements definition
    a. Security process requirements provide assurance that the vendor has the willingness, ability, and demonstrated capability to design, develop, and support secure medical devices. This may include inquiries about the Secure Development Life Cycle, code review processes, penetration testing, and vulnerability scanning during development and production.
    b. Security technical requirements provide assurance that the vendor delivers devices that meet the HDO's security needs.
    c. Security support requirements to assure that i) the device security posture can be maintained, and ii) that the vendor performs its service activities in a way that does not compromise the device's (or larger system's) security capabilities.
2. Vendor and device selection
    a. Clinical and security requirements to shortlist vendors and devices.
    b. Vendor and device risk assessment (Cybersecurity):
        i. Initial device risk determination / exception management as well as a risk assessment framework informed by the following vendor information deliverables:
            1. MDS2, SBOM, Information on PII, PHI, and credentials stored on the device.
            2. Deployment Guide (e.g., network diagrams, security architecture and recommendations, ports needed, etc.)
            3. Vulnerability Disclosures, Residual Risk acceptance
            4. Installation and configuration instructions/manuals

ii. Contracting:

1. General contracting for medical devices may include Business Associate Agreements (BAAs) and Information Security Agreements (ISAs) that cover:
    a. Technical security requirements such as application upgrades, antimalware maintenance, configuration specifications, component obsolescence, etc.
    b. Procedural security requirements such as incident response, disaster recovery, etc.
    c. Vulnerability management and communication processes as well as mitigation (e.g., patch release).
    d. Maintenance tools and processes such as remote access requirements.
    e. Responsibility agreement (e.g., per ISO/IEC 80001) as well as other legal obligations and liability clauses or terms.
2. Installation support, including e.g., site assessment, integration, configuration, maintenance planning, network architecture, and monitoring requirements.
3. End of Life (EOL) requirements – prior to the device leaving your control, all sensitive data should be removed:
    a. Sanitization process, i.e., removal of any critical or otherwise sensitive data such as PII, PHI, network and user credentials, intellectual property, or research data.
    b. In case electronic data purge is not possible or supported, physical destruction of the device data carrier is an option.

6.4 Deployment

During the deployment phase the HDO has the opportunity to assess and assure that the specified security requirements and configuration settings are met, that the device's pertinent security properties are logged in the inventory management system (CMMS, CMDB, or other), and that it is deployed in a secure manner, including:

1. Perform pre-deployment testing to assess / assure:
    a. Conformance with agreed upon (contracted) security requirements
    b. SBOM review
    c. External scanning capabilities (e.g. vulnerability and discovery scans)
    d. Additional security testing as needed, e.g., sample pen testing
    e. Device or change acceptance and release
2. Installation in production (clinical) environment
3. Integration (from a cybersecurity perspective) with enterprise security management systems that may be in use:
    a. Asset management systems (CMMS, CMDB)
    b. Vulnerability scanning system

c. Cybersecurity integration and management (with SIEM, SOC)
d. Remote access management
e. ID and credential management (e.g., Active Directory)
f. Risk management system

4. Implementation
    a. Implement security segmentation and firewall protection based on device criticality
    b. Training, as required, for technical and clinical personnel
    c. Clinical go-live

6.5 Operation

Once deployed, medical devices are expected to operate to meet clinical and operational performance criteria, as defined in the procurement phase. This includes identifying and documenting the procedures for applying and maintaining controls. This is typically based on documentation provided by the MDM, however, HDOs may add to this based on their own needs, experience, and risk tolerance.

A complete and accurate inventory is foundational to the management and support of a medical device during its operation, including continuously monitoring the inventory of software components (SBOM) running on the device. Further, maintaining patch processes and a regular patch cycle can enable more secure operation.

During the device's operation (i.e., its useful clinical life) and to assure its continued secure use, it is important to maintain the device's security posture, as well as respond and mitigate security incidents.

6.5.1 End-user "best practices" training

Clinical staff like doctors, nurses, or technicians, or other device users have an important responsibility with regards to cybersecurity. First and foremost, they need to operate the device per instructions for use to minimize the exposure to security risks. Secondly, as the everyday user of the device, they are the first ones that may observe abnormal operation that may indicate a security compromise. They should be trained to have the awareness to recognize such events and escalate as appropriate. Therefore, role-appropriate security training, for clinical staff is important.

6.5.2 Maintenance

All maintenance activities on regulated medical devices, be they conducted by the HDO, MDM, or third party, are required to be documented according to federal, state and local accrediting agencies. This includes activities related to establishing and maintaining the security posture or in response to monitoring or alert activities. For example, for JCAHO accredited HDOs, the Medical Equipment Management Plan (MEMP) should specify where this documentation is maintained regardless of the

maintenance provider. This may include any or all of the following (as supported by the device / system in question):

1. Maintain operating system, clinical application, or other patching cycle as recommended by MDM and determined by organizational security requirements.
2. Maintain all necessary software and security updates as recommended by MDM and as determined by mitigation priority.
3. User account management - maintaining accounts for current employees or other accepted accounts; removing or revoking all others.
4. Implement secure authentication. Access to the device must be secured to prevent a bad actor from gaining access to the device. For example, consider multi-factor authentication mechanisms for high privilege access, e.g., remote support.
5. Install, configure and maintain commercial endpoint security products (antivirus or HIDS/HIPS) in accordance with manufacturer instructions, if applicable.
6. If vendor remote access is required, ensure such access occurs through a secure connection (e.g., VPN, virtual desktop, private link) and secure authentication (e.g., multi-factor authentication). Assure that access occurs through a temporary session that is terminated after maintenance tasks are completed.

Depending on the HDO's security policies and practices and for lower level risks, some updates, patches, or changes can be phased in during regular device preventative maintenance (PM) activities.

Typical maintenance tasks include the following.

6.5.2.1 Configuration Management

As part of the security lifecycle, the HDO should establish and maintain a secure configuration knowledgebase for each device type, make, version and model:

1. Establish a security baseline configuration and operating characteristics.
2. Document any approved deviations from the baseline configuration.

6.5.2.2 Change Management and Planning

All device updates, including security, configuration and communication or other network impacting changes must be planned for and accepted prior to implementation. This includes: configuration changes, workarounds, patches, updates, and new versions.

A formal change management process provides risk management oversight. Elements that should be included:

1. A change request including rationale, impact, risk assessment, risk analysis, timeframe, and resources.

2. The change request is submitted to, reviewed and approved by appropriate oversight group, i.e., Change Advisory Board (CAB).
3. Oversight review may consider:
    a. Impact on security posture.
    b. Confirmation that the change passes security testing.
    c. Dependencies, interactions, or impact on other components or systems.
    d. Determine urgency and priority.
    e. Assess risk of scheduling and interruption to care delivery.
    f. Assure rollback options.
    g. Support, approval, or endorsement of purposed change by the MDM.
    h. Resource requirements including staff, 3rd parties, hardware, or technical.
    i. Type of change:
        i. Product updates / patches: Perform routine security updates and patches.
        ii. Change deployment: Ensure the approved mitigation is deployed on all applicable devices.
        iii. Re-testing (if required): Security mitigation applied to the system should first be tested before being applied in production.
    j. Required changes to:
        i. Operations and integration.
        ii. Operating instructions and procedures.
        iii. Training and training material.
    k. Testing: The HDO must perform various types of testing including functional, performance, integration, and security testing. Technical security testing of the device may be needed to determine known vulnerabilities.
        i. Pre-deployment: Create a manual or automated checklist for approved changes in the staging environment prior to production deployment.
        ii. Post-Deployment: A checklist to validate the approved change is operating as intended in the production environment. This includes verifying system logs and other device components before release for operation.
        iii. Conformance testing (assurance that nothing broke – smoke testing): Apply selected use cases to conduct a walkthrough of the device to validate a successful change.

Technical support staff should be trained on the change management process including rationale, how to initiate a change request, change justification, conducting a risk assessment and performing risk analysis. A checklist of the change management process steps is helpful.

6.5.2.3 Monitoring

The HDO should establish formal processes for ongoing security monitoring, including:

1. SBOM review (ongoing): Both MDM and HDO maintain an inventory of software components included on the device. The SBOM should be machine readable for ingestion by HDO. The HDO will develop a process to monitor vulnerabilities and threats associated with each component for the life of the device.
2. Event / incident / notification review: monitor device operations; establish operational baseline; monitor alerts to track and identify suspicious behavior.
3. Notification as required (e.g., MDM, regulators, ISAOs, law enforcement, or other third parties).

6.5.2.4 Incident response

NIST Cybersecurity Incident Guide NIST SP 800-61 R2 (NIST, 2012) provides an approach for the management of cybersecurity incidents, including: establishing, organizing, handling, coordinating, and communicating. Key steps are:

1. Planning
2. Training
3. Execution
4. Continual improvement
5. Reporting requirements:
    a. Incident reporting (e.g. breach notification to HHS)
    b. Adverse event reporting (e.g., per FDA 21 CFR Part 806)
    c. Other State or international regulations reporting requirements
    d. Vulnerability reporting (manufacturer, ISAC / ISAO)
    e. Law enforcement
    f. HDOs may use the manufacturers' Coordinated Vulnerability Disclosure submission process (a link to manufacturer security sites is provided by H-ISAC (H-ISAC, n.d.)).

6.6 Decommission

Today's complex and evolving technology environment has resulted in a change of what actually constitutes a medical device and as a result HDO EOL management is getting more complex. In the most traditional case, we can look at the removal of a piece of hardware (mobile device, workstation, server, or medical device), which requires purging the data contained on the device.

Modern devices utilizing evolving technologies such as commercial mobile platforms or cloud data storage may require a more complex handling of EOL as it may require purge of data on components that are not owned by or are not under physical control of the HDO.

Regardless of storage location, the data types that should be removed from the device at EOL include:

1. Clinical data, PHI, and PII.
2. Research data, intellectual property (IP), clinical trial data.

3. Other sensitive information including user, device, and network credentials.

Software as a Medical Device (SaMD) (IMDRF, 2013) or 3rd party service providers such as manufacturers collecting and hosting medical device data may need additional protections. Examples may include considerations regarding device ownership (e.g., SaMD running on a smartphone or tablet) or data residency (e.g., in a third party hosted cloud service). These technologies or services are beyond the scope of this paper. Decommissioning activities for SaMD or hosted services may require (in addition to data purge on the device) third party action, license and software support termination, or contractual mitigation (e.g., a Business Associate Agreement, BAA).

There are significant cybersecurity implications for EOL medical devices that contain patient medical records. To avoid a privacy breach of medical records stored in decommissioned devices, the following security tasks are recommended:

1. Scrubbing of all medical records contained on the device.
2. Adopt NIST SP 800-88 guidelines for Media Sanitization (NIST, 2014).
3. Address licensing issue, if device is resold/reassigned to a different site.
4. Remove all network configurations from the device including host names, IP address, firewall configurations, Wi-Fi credentials, etc.
5. Remove all user accounts and passwords.
6. Manage changes to service contracts, licenses, and software support contracts.

Another aspect that requires consideration is when an MDM drops support and maintenance for a device (i.e., the MDM EOL/EOS of a product line or type). In this case the HDO assumes the liability of continuing use of the device. The HDO may need to update its risk assessment and implement additional security mitigation (e.g., network segmentation, firewalls) as the device will no longer receive MDM security updates and patches, thus becoming increasingly vulnerable over time. Refer to your local IT Security exception handling process to record and manage this risk.

6.7 Special considerations

Some circumstances may require special considerations:

Legacy devices: Based on information that may be available (e.g., SBOM, MDS2), perform security risk assessments on legacy medical devices to identify threats and vulnerabilities. Complete a risk analysis to assess impacts on patient safety, care delivery, operations, and other business risks. Assess availability of compensating controls, e.g., network segmentation.

Leased / loaned devices: In general, the security processes applied to leased or loaned devices are not different than what has been outlined before. However, device ownership may impact security responsibility and security management. The following are some recommended steps for securing a loaned / leased device in cooperation with the device owner:

- Scan the device for malware prior to acceptance.

- Assure the received device is of the latest version and does not contain any confidential data (e.g., credentials or PHI).
- When possible, create a system image (clone) of the device prior to use.
- Apply secure configurations, implement access controls, enable log monitoring, install security controls as indicated by manufacturer instructions, configuration documentation or organizational practice.
- Before returning the device to the owner, assure purge of confidential data (e.g., credentials, PHI, PII). If possible, restore device image.

Vulnerable devices: HDOs should identify and document specific security weakness with potential patient impacts. If the device cannot be brought to a level that meets the HDO's security policies (temporarily or permanently), a risk/benefits analysis may be performed and external or procedural security controls may need to be established. Further, high-vulnerability devices should receive priority consideration in replacement planning (see section 6.2)

IDE devices: Align security of Investigational Device Exemption (IDE) devices to FDA regulations of §812.40.

7 Summary and Conclusion

This document provides an overview of a lifecycle-based approach to managing medical device cybersecurity from the perspective of Medical Device Manufacturers and Healthcare Delivery Organizations. It provides a high-level overview of the four main lifecycle phases and the relationship between them. Further, it provides references to key regulations and standards as well as other leading practices provided in the literature.

In light of the importance of medical device cybersecurity, and in consideration of the growing complexity of our medical device ecosystem on one hand and the increase in the number and sophistication of cyber threats, following a programmatic and repeatable set of security processes is a requirement for any medical device manufacturer and healthcare delivery organization. We hope that this whitepaper lies the foundation for a better understanding of such approach.

8 References

AAMI. (2016). *TIR57: Principles for medical devices security - risk management.* Arlington, VA: Association for the Advancement of Medical Instrumentation.

AAMI. (2019). *TIR97: Principles for medical device security - Postmarket risk management for device manufacturers.* Association for the Advancement of Medical Instrumentation.

FDA. (2016). *Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance,and Enforcement Decisions.* U.S. Food and Drug Administration.

FDA. (2016). *Postmarket management of cybersecurity in medical devices. Guidance for industry and food and drug administration staff.* U.S. Food & Drug Administration.

FDA. (2019, 12 16). *How to Determine if Your Product is a Medical Device*. From U.S. Food and Drug Administration: https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device

Health Canada. (2019). *Premarket Requirements for Medical Device Cybersecurity .* Health Canada.

HSCC. (2019). *Health Industry Cybersecurity Supply Chain Risk Management Guide.* Healthcare and Public Health Sector Coordinating Councils.

HSCC. (2019). *Medical Device and Health IT Joint Security Plan.* Healthcare and Public Health Sector Coordinating Councils.

HSCC. (2020). *Health Industry Cybersecurity Information Sharing Best Practices.* Healthcare and Public Health Sector Coordinating Councils.

IEC. (2006). *IEC 62304 Medical device software - Software life cycle processes.* International Electrotechnical Commission.

IMDRF. (2013). *Software as a Medical Device (SaMD): Key Definitions.* International Medical Device Regulators Forum, SaMD Working Group.

IMDRF. (2020). *Principles and Practices for Medical Device Cybersecurity.* International Medical Device Regulators Forum.

ISO. (2019). *ISO 14971 Medical devices — Application of risk management to medical devices.* International Organization for Standardization.

ISO/IEC . (2010). ISO/IEC-80001-1:2010 — Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities. International Electrotechnical Commission.

MITRE. (2019, 09). *Rubric for Applying CVSS to Medical Devices*. From MITRE Technical Papers: https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

NIST. (2012, August). SP 800-61 Rev. 2 Computer Security Incident Handling Guide.

NIST. (2014, December). SP 800-88 Rev. 1 Guidelines for Media Sanitization.

NIST. (2015, April). Best Practices in Cyber Supply Chain Risk Management. Gaithersburg, MD: NIST. From National Institute for Standards and Technology: https://csrc.nist.gov/publications/detail/sp/800-161/final

NTIA Framing Working Group. (2019). *Framing Software Component Transparency.* National Telecommunications and Information Administration.

Schneier, B. (2020, 07 28). *Survey of Supply Chain Attacks*. From Schneier on Security: https://www.schneier.com/blog/archives/2020/07/survey_of_suppl.html

Shostack, A. (2014). *Threat Modeling.* Indianapolis, IN: John Wiley & Sons.

Therapeutic Goods Administration. (2019). *Medical device cyber security guidance for industry.* Australian Government, Department of Health.

Wirth, A., Gates, C., & Smith, J. (2020). *Medical Device Cybersecurity: A Guide for Engineers and Manufacturers.* Boston, London: Artech House.

Feedback and suggestions on this document are encouraged and welcome.

Please email contact@h-isac.org