DRAFT DOCUMENT

International Medical Device Regulators Forum

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: October 1, 2019

Table of Contents

1.0 Introduction ... 5
2.0 Scope ... 5
3.0 Definitions ... 6
4.0 General Principles ... 9
4.1 Total Product Life Cycle ... 9
4.2 Shared Responsibility ... 11
4.3 Information Sharing ... 11
4.4 Ability to Identify, Protect, Detect, Respond, Recover ... 11
4.5 Global Harmonization ... 11
5.0 Pre-Market Considerations for Medical Device Manufacturers ... 12
5.1 Security Requirements and Architecture Design ... 12
5.2 Risk Management ... 14
5.3 Security Testing ... 15
5.4 Post-market Management Strategy ... 15
5.5 Labeling or Customer Security Documentation ... 16
5.6 Regulatory Submission Requirements ... 17
5.6.1 Design Documentation ... 17
5.6.2 Risk Management Documentation ... 17
5.6.3 Security Testing Documentation ... 17
5.6.4 Post-market Management Plan ... 18
5.6.5 Labelling or Customer Security Documentation ... 18
6.0 Post-Market Considerations for Medical Device Cybersecurity ... 18
6.1 Operating Devices in the Intended Use Environment ... 18
6.1.1 Healthcare Providers and Patients ... 18
6.1.2 Medical Device Manufacturers ... 19
6.2 Information Sharing ... 19
6.2.1 Key Stakeholders ... 20
6.2.2 Types of Information ... 22
6.2.3 Trusted Communication ... 22
6.3 Coordinated Vulnerability Disclosure ... 22
6.3.1 Medical Device Manufacturers ... 23
6.3.2 Regulators ... 24

6.3.3 Vulnerability Reporters (includes security researchers and others) 24
6.4 Vulnerability Remediation 25
6.4.1 Medical Device Manufacturers 25
6.4.2 Healthcare Providers and Patients 27
6.4.3 Regulators 30
6.5 Incident Response 32
6.5.1 Medical Device Manufacturers 32
6.5.2 Healthcare Providers 33
6.5.3 Medical Device Regulators 34
6.6 Legacy Medical Devices 34
6.6.1 Medical Device Manufacturers 34
6.6.2 Healthcare Providers 35
7.0 References 35
7.1 IMDRF Documents 35
7.2 International Standards 35
7.3 Regulatory Guidance 36
7.4 Other References 37
8.0 Appendices 39
8.1 Appendix A: Incident Response Roles (from ISO/IEC 27035) 40
8.2 Appendix B: Background on Legacy Devices 42
8.3 Appendix C: Jurisdictional resources for Coordinated Vulnerability Disclosure 44

Preface

The document herein was produced by the International Medical Device Regulators Forum (IMDRF), a voluntary group of medical device regulators from around the world. The document has been subject to consultation throughout its development.

There are no restrictions on the reproduction, distribution or use of this document; however, incorporation of this document, in part or in whole, into any other document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

1.0 Introduction

The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet, and network-connected devices. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities. Such incidents may lead to patient harm because of delays in diagnoses and/or treatment, errors in diagnoses and/or treatment, etc.

Stakeholders within the healthcare sector have a shared responsibility regarding medical device cybersecurity. This guidance assists all these stakeholders in gaining a better understanding of their role in support of proactive cybersecurity that helps protect and secure medical devices in anticipation of future attacks, problems, or events.

Convergence of global healthcare cybersecurity principles and practices is necessary to ensure that patient safety and medical device performance is maintained. To date, however, current disparate regulations across governments lack the global alignment needed to ensure medical device cybersecurity.

The purpose of this IMDRF guidance document is to provide fundamental concepts and considerations on the general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity. The document is structured as follows: the scope of the document is defined in Section 2 followed by defined terms in Section 3. Section 4 provides an overview of the general principles of medical device cybersecurity, while Sections 5 and 6 provide a number of recommendations for stakeholders regarding best practices in the pre-market (focus is on medical device manufacturers) and post-market (includes numerous stakeholders) management of medical device cybersecurity.

While this is the first IMDRF guidance document to focus exclusively on medical device cybersecurity, there are other relevant IMDRF documents which should be noted in terms of global security considerations. IMDRF/GRRP WG/N47 FINAL: 2018 provides harmonized Essential Principles that should be fulfilled in the design and manufacturing of medical devices and IVD medical devices[1]. Those should be considered along with this guidance document throughout the total product life cycle of a medical device. IMDRF/SaMD WG/N12 FINAL: 2014 is also worth noting. It describes the importance of information security with respect to safety considerations in Section 9.3 and illustrates some particular factors which affect the information security of software as a medical device (SaMD).

2.0 Scope

This document is designed to provide concrete recommendations to all responsible stakeholders on the general principles and best practices for medical device cybersecurity (including in vitro

[1] Section 5.8 describes important requirements on information security and cybersecurity such as the protection against unauthorized access. They should be considered along with this guidance document throughout the total product life cycle of the medical device.

diagnostic (IVD) medical devices). In general, it outlines recommendations for medical device manufacturers, healthcare providers, regulators, and users to: employ a risk-based approach to the design and development of medical devices with appropriate cybersecurity protections; minimize risks that could arise from use of the device for its intended purposes; and to ensure maintenance and continuity of critical device safety and effectiveness.

This document considers cybersecurity in the context of medical devices that: 1) contain software, including firmware and programmable logic controllers (e.g. pacemakers, infusion pumps); and 2) exist as software only (e.g. Software as a Medical device (SaMD)). It is important to note that the scope of this medical device cybersecurity guidance is limited to consideration of the potential for patient harm. While other types of harms such as those associated with breaches of data privacy are important, they are not considered within the scope of this document.

This document is intended to:

- Recognize that cybersecurity is a shared responsibility among all stakeholders, including but not limited to medical device manufacturers, healthcare providers, users, regulators, and vulnerability reporters;
- Provide recommendations to aid in minimizing cybersecurity risks across the total product life cycle to those stakeholders;
- Define terms consistently and describe the current best practices on achieving medical device cybersecurity;
- Provide advice to medical device manufacturers on how to achieve the cybersecurity recommendations described in this document; and,
- Promote broad information sharing policies for cybersecurity incidents, threats, and vulnerabilities to increase transparency and to strengthen response.

It is important to note that differences across regulatory jurisdictions, along with consideration of the affected medical device, may give rise to specific circumstances where additional requirements exist.

3.0 Definitions

For the purposes of this document, the terms and definitions given in IMDRF/GRRP WG/N47 FINAL:2018 and the following apply.

3.1 *Asset:* physical or digital entity that has value to an individual, an organization or a government (ISO/IEC JTC 1/SC 41 N0317, 2017-11-12)

3.2 *Attack:* attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (ISO/IEC 27000:2018)

3.3 *Authentication:* provision of assurance that a claimed characteristic of an entity is correct (ISO/IEC 27000:2018)

3.4 *Authenticity:* property that an entity is what it claims to be (ISO/IEC 27000:2018)

3.5 *Authorization:* granting of privileges, which includes the granting of privileges to access data and functions (ISO 27789:2013)

NOTE: Derived from ISO 7498-2: the granting of rights, which includes the granting of access based on access rights.

3.6 *Availability:* property of being accessible and usable on demand by an authorized entity (ISO/IEC 27000:2018)

3.7 *Common Vulnerability Scoring System (CVSS):* system that provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score

NOTE: Derived from the CVSS v3.0 Specification.

3.8 *Compensating Risk Control Measure (syn. Compensating Control):* specific type of risk control measure deployed in lieu of, or in the absence of, risk control measures implemented as part of the device's design (AAMI TIR97:201x)

NOTE: A compensating risk control measure could be permanent or temporary (e.g., until the manufacturer can provide an update that incorporates additional risk control measures).

3.9 *Confidentiality:* property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 27000:2018)

3.10 *Coordinated Vulnerability Disclosure (CVD):* process through which researchers and other interested parties work cooperatively with a manufacturer in finding solutions that reduce the risks associated with disclosure of vulnerabilities (AAMI TIR97:201x)

NOTE: This process encompasses actions such as reporting, coordinating, and publishing information about a vulnerability and its resolution.

3.11 *Cybersecurity:* preservation of confidentiality, integrity and availability of information in the Cyberspace (ISO/IEC 27032:2012)

NOTE 1: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2: Adapted from the definition for information security in ISO/IEC 27000:2009.

3.12 *End of Life (EOL):* point at which a product or component is taken out of use (ISO 8887-1:2017)

3.13 *End of Support (EOS):* point at which the manufacturer terminates all service support activities (AAMI TIR97:201x)

NOTE: Service support does not extend beyond this point.

3.14 *Exploit:* defined way to breach the security of information systems through vulnerability (ISO/IEC 27039)

3.15 *Integrity:* property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored (ISO/IEC 29167-19:2016)

3.16 *Legacy Medical Device (syn. Legacy Device):* medical devices that cannot be reasonably protected against current cybersecurity threats

3.17 *Non-Repudiation:* ability to prove the occurrence of a claimed event or action and its originating entities (\ISO/IEC 27000:2018)

3.18 *Patch:* modification made directly to an object program without reassembling or recompiling from the source program (ISO/IEC/IEEE 24765:2017)

3.19 *Patient Harm:* physical injury or damage to the health of patients (Modified from ISO/IEC Guide 51:2014)

3.20 *Privacy:* freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual (ISO/TS 27799:2009)

3.21 *Security:* condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences (ISO/IEC Guide 120)

NOTE: Hostile acts or influences could be intentional or unintentional.

3.22 *Threat:* potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm (ISO/IEC Guide 120)

3.23 *Threat Modeling:* systematic exploration technique to expose any circumstance or event having the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service (IEEE 24765-2017)

3.24 *Update:* corrective, preventative, adaptive, or perfective modifications made to software of a medical device

NOTE 1: Derived from the software maintenance activities described in ISO/IEC 14764:2006.

NOTE 2: Adaptive and perfective modifications are enhancements to software. These modifications are those that were not in the design specifications for the medical device.

3.25 *Validation:* confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled (IEC 62366:2007)

NOTE 1: The term “validated” is used to designate the corresponding status.

NOTE 2: The use conditions for validation can be real or simulated.

3.26 *Verification:* confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (ISO/IEC Guide 63)

NOTE 1: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

NOTE 2: The activities carried out for verification are sometimes called a qualification process.

NOTE 3: The word “verified” is used to designate the corresponding status.

3.27 *Vulnerability:* weakness of an asset or control that can be exploited by one or more threats (ISO/IEC 27000:2018)

4.0 General Principles

This section provides general principles for the relevant stakeholders to ensure safety and effectiveness of medical device cybersecurity based on the risk management and quality management system, articulated respectively in ISO 14971 and ISO 13485.

4.1 Total Product Life Cycle

Risks associated with cybersecurity threats and vulnerabilities should be considered throughout all phases in the life of a medical device, from initial conception to end of support (EOS). To effectively manage the dynamic nature of cybersecurity risk, risk management should be applied throughout the total product life cycle (TPLC) where cybersecurity risk is evaluated and mitigated in the design, manufacturing, testing, and post-market monitoring activities.

A cybersecurity risk that impacts device safety and essential performance, negatively affects clinical operations, or results in diagnostic or therapeutic errors should also be considered in the medical device’s risk management process. This consideration is reflected in AAMI TIR57:2016 Principles for medical device security - Risk management which suggests that the risks associated with the cybersecurity of a device include harms to patient safety (as described in ISO 14971) and can be associated with indirect patient harm via cybersecurity security risks. As part of their risk management process a manufacturer should:

- Identify any cybersecurity vulnerability
- Estimate and evaluate the associated risks
- Control those risks to an acceptable level, and
- Monitor the effectiveness of the risk controls

Figure 1 below shows the security risk management process[2].

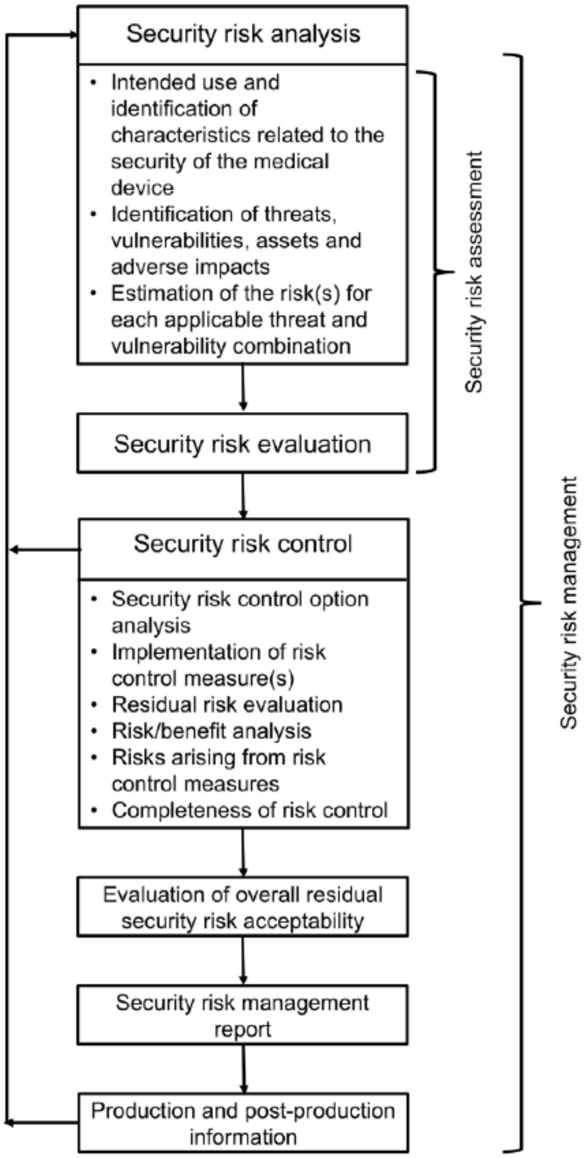
Security risk analysis
• Intended use and identification of characteristics related to the security of the medical device
• Identification of threats, vulnerabilities, assets and adverse impacts
• Estimation of the risk(s) for each applicable threat and vulnerability combination
Security risk evaluation
Security risk control
• Security risk control option analysis
• Implementation of risk control measure(s)
• Residual risk evaluation
• Risk/benefit analysis
• Risks arising from risk control measures
• Completeness of risk control
Evaluation of overall residual security risk acceptability
Security risk management report
Production and post-production information
Security risk assessment
Security risk management

Figure 1: Schematic representation of the security risk management process (with permission from AAMI TIR 57:2016.)

Medical device manufacturers should employ a risk-based approach to ensure the design and development of medical devices with appropriate cybersecurity protections. Doing so necessitates that manufacturers take a holistic approach to device cybersecurity by assessing risks and mitigations throughout the product's life cycle. However, it is recognized that there is a need to

[2] Figure 1 shows the security risk management process. This can be thought as a part of risk management process described in ISO 14971. Also, this can be a separate process for the rest of risk management process. For further guidance on risks related to security, see ISO/TR 24971:20XX, Annex F.

balance safety and security. When incorporating cybersecurity controls and mitigations, it is critical that medical device manufacturers ensure maintenance and continuity of critical device safety andessential performance (i.e. design choices that maximize device cybersecurity while not unduly affecting other safety-related aspects of the medical device (e.g. usability)).

4.2 Shared Responsibility

Medical device cybersecurity is a shared responsibility between stakeholders including the manufacturer, healthcare provider, users, regulator, and vulnerability finder. All stakeholders are responsible for continuously monitoring, assessing, mitigating, and communicating potential cybersecurity risks and threats throughout the life cycle of the medical device.

4.3 Information Sharing

Cybersecurity information sharing is a foundational principle in the TPLC approach to safe and secure medical devices. All stakeholders are encouraged to adopt a proactive pre- and post-market cybersecurity approach. The availability of timely information provides all responsible parties with enhanced capability to identify threats, assess associated risks, and respond accordingly. All responsible stakeholders are therefore encouraged to actively participate in Information Sharing Analysis Organizations (ISAOs) to foster collaboration and communication of cybersecurity incidents, threats, and vulnerabilities that may affect the safety, effectiveness, integrity, and security of the medical devices and the connected healthcare infrastructure. These efforts promote transparency. Furthermore, the ecosystem would benefit from additional development of information sharing policies that would extend beyond manufacturers to include healthcare providers as well as users of medical devices. Regulators are also encouraged to share information with other regulators to help protect and maintain patient safety globally.

4.4 Ability to Identify, Protect, Detect, Respond, Recover

The National Institute of Standard and Technology (NIST) has developed a “Framework for Improving Critical Infrastructure Cybersecurity,” which is a general framework applicable across critical infrastructure. The NIST framework includes best practices that align with the concepts described in this document. The five core functions of the framework readily adapt to strengthen medical device cybersecurity and include: identify, protect, detect, respond, and recover. Responsible stakeholders should consider:

- **Identifying** cybersecurity risks in the device’s design and operating environment;
- **Protecting** the device to reduce risk through various risk mitigations;
- **Detecting** if a device has been compromised due to a cybersecurity event;
- **Responding** using a previously-defined process to respond to a cybersecurity event; and
- **Recovering** using a previously-defined process to restore the device to normal operation following a cybersecurity event.

4.5 Global Harmonization

Medical device cybersecurity is an issue of global concern. Security incidents can threaten the safety of patients in healthcare systems across the world by causing diagnostic or therapeutic errors, by compromising the safe performance of a device, by affecting clinical operations, or by denying patient access to critical care. Convergence of global healthcare cybersecurity efforts is necessary to ensure that patient safety is maintained while encouraging innovation and allowing timely patient access to safe and effective medical devices. All stakeholders are encouraged to harmonize their approaches to cybersecurity across the entire life cycle of the medical device. This includes harmonization across product design, risk management activities throughout the life cycle of the device, device labelling, regulatory submission requirements, information sharing, and post-market activities.

5.0 Pre-Market Considerations for Medical Device Manufacturers

Although medical device cybersecurity should be considered over the total product life cycle, there are important elements that a manufacturer should address during the design and development of a medical device prior to market entry. These pre-market elements include: designing security features into the product; the application of accepted risk management strategies; security testing; provision of useful information for users to operate the device securely; and the consideration of having a plan in place for post-market activities. The following sections are intended to introduce these concepts and provide recommendations to manufacturers in the pre-market phase of the product's life cycle.

5.1 Security Requirements and Architecture Design

Proactively addressing cybersecurity threats at the design stage can better mitigate patient harm than engaging in reactive, post-market activities alone. These design inputs can come from various phases across the product's life cycle, such as from requirements capture, design verification testing, or risk management activities in the pre- and post-market.

The life cycle requirements for medical device software is defined in IEC 62304. The general requirements for programmable electrical medical systems (PEMS) included in IEC 60601-1 also requires to apply part of IEC 62304. Specifically, Figure H-2 of IEC 60601-1 (Ed. 3.1) is titled "A PEMS DEVELOPMENT LIFE-CYCLE model" and includes process elements for requirements capture and architecture design. Security requirements should also be identified during the requirements capture stage of the life cycle design process. Sources of security requirements and security risk control measures include AAMI TIR57:2016, IEC TR 80001-2-2, IEC TR 80001-2-8, the ISO 27000 family, and resources published by NIST (e.g. NIST's Secure Software Development Framework (SSDF), OWASP (e.g. Security by Design principles), ENISA, and the US Healthcare and Public Health Sector Coordinating Council (HPH SCC) Joint Cyber Security Working Group (JCWG).

In order to provide concrete examples of security design considerations, the following Table 1 outlines some design principles that medical device manufacturers should consider in designing their product. This table is not meant to be an exhaustive list:

Design Principle	Description

Secure Communications	The manufacturer should consider how the device would interface with other devices or networks. Interfaces may include hardwired connections and/or wireless communications. Examples of interface methods include Wi-Fi, Ethernet, Bluetooth and USB.
	The manufacturer should consider how data transfer to and from the device is secured to prevent unauthorized access or modification. For example, manufacturers should determine: how the communications between devices/systems will authenticate each other; if encryption is required; and if terminating communication sessions after a pre-defined time is appropriate.
Data Confidentiality	The manufacturer should consider if data that is stored on – or transferred to or from – the device requires some level of protection such as encryption.
	The manufacturer should consider if confidentiality risk control measures are required to protect message control/sequencing fields in communication protocols or to prevent the compromise of cryptographic keying materials.
Data Integrity	The manufacturer should consider design controls that take into account a device that communicates with a system and/or device that is less secure (e.g., a device connected to a home network or a legacy device).
	The manufacturer should evaluate the system-level architecture to determine if design controls are necessary to ensure data non-repudiation (e.g., supporting an audit logging function).
User Access	The manufacturer should consider user access controls that validate who can use the device or allows granting of privileges to different classes of users or allow users access in an emergency. Examples of authentication or access authorization include passwords, hardware keys or biometrics.
Software Maintenance	The manufacturer should consider how the device will be updated to secure it against newly discovered cybersecurity threats. For example, consideration could be given to whether updates will require user intervention or be initiated by the device.
	The manufacturer should consider what connections will be required to conduct updates and the authenticity of the connection, update, or patch.
	The manufacturer should consider how often a device will need to be updated via regular and/or routine updates.
	The manufacturer should consider how operating system software, third-party software, or open source software will be updated or controlled.
Hardware or Physical Design	The manufacturer should consider controls to prevent an unauthorized person from accessing the device. For example, controls could include physical locks or disabling a USB port used only in service mode.

Reliability and Availability	The manufacturer should consider design controls that will allow the device to detect, resist, respond and recover from cybersecurity attacks.

Table 1: Select design principles for consideration in medical device design

Secure software development principles are integral to secure device design. Many current software development life cycle models or standards do not incorporate these principles by default. It is important for device manufacturers that develop medical device software to recognize this deficiency and to incorporate these security principles into the development of their software.

5.2 Risk Management

Sound risk management principles, as described in ISO 14971:2007 Medical devices - Application of risk management (ISO 14971), should be incorporated throughout the life cycle of a medical device and the manufacturer should take steps to identify, estimate, and control risks in the production and post-production phase of the device as per Figure 1 in Section 4.1 above.

With respect to cybersecurity, risk analyses should focus on assessing the risk of patient harm by considering: 1) the exploitability of the cybersecurity vulnerability; and 2) the severity of patient harm if the vulnerability were to be exploited. These analyses should also incorporate consideration of compensating controls and risk mitigations.

Risk assessments tie design to threat models, clinical hazards, mitigations, and testing. It is important to establish a secure design architecture such that risk can be adequately managed. There are numerous tools and approaches that may be leveraged in this assessment including but not limited to security risk assessment, threat modeling, and vulnerability scoring.

- **Security Risk Assessment**: Manufacturers should consider cybersecurity risks, threats and controls throughout the product life cycle. Where applicable, cybersecurity requirements should be cross-referenced to specific device cybersecurity threats and vulnerabilities if the requirements are mitigations to identified hazards. Creating a traceability matrix that links the cybersecurity controls to the cybersecurity risks and threats that were considered in the security risk analysis is of value in this assessment.

- **Threat Model**: A threat model is a way to systematically assess risk against threats in the device and system. Specifically, a system level threat model includes consideration of system level risks, including but not limited to risks related to the supply chain (e.g., to ensure the device remains free of malware), design, production, and deployment (e.g., into a connected/networked environment). Furthermore, creating sufficiently detailed system diagrams aids in the understanding of how cybersecurity device design elements are incorporated into a system-level which further aids in the generation of the threat model. As an initial step in generating a threat model, device manufacturers should consider the device functionality, its interfaces, and dependencies.

- **Vulnerability scoring**: Vulnerability scoring provides a way to characterize and assess the severity of a cybersecurity vulnerability. Known common vulnerabilities and exposures

(CVEs) identified in design and development are analyzed and evaluated using a consistent vulnerability scoring methodology such as the Common Vulnerability Scoring System (CVSS). Cybersecurity risk and information coming out of vulnerability scoring may be used to inform other risk assessment tools not specific to cybersecurity (e.g. failure mode and effects analysis (FMEA), etc.).

5.3 Security Testing

The validation of the design phase of a medical device requires security testing. Testing should take into consideration the context of use of the device and its deployment environment. Application of software verification techniques are recommended to minimize the risk of anomalies and ensure that the software complies with the specifications. It is also important to ensure that the medical device is tested for known vulnerabilities that could be exploited. To do this, the medical device should undergo a security assessment process or acceptance check (e.g. software testing, attack simulation, etc.). Security testing is a component of secure development framework and additional granularity regarding testing considerations may be found in the standards and resources provided in Section 5.1. Below are some high-level considerations for medical device manufacturers:

- Perform target searches on software components/modules for known vulnerabilities or software weakness. For example, security testing can include: static code analysis, dynamic analysis, robustness testing, vulnerability scanning, software composition analysis.
- Conduct technical security analyses (e.g. penetration testing). These include: efforts to identify unknown vulnerabilities and checks for unknown vulnerabilities, e.g. through fuzz testing; or checks for alternative entry points, e.g. by reading hidden files, configuration, data streams or hardware registers.
- Complete a vulnerability assessment. This, includes an impact analysis of the vulnerability on other in-house products (i.e. variant analysis);, the identification of countermeasures; and the remediation or mitigation of vulnerability.

5.4 Post-market Management Strategy

As cybersecurity threats will continuously evolve, manufacturers should proactively monitor, identify, and address vulnerabilities and exploits as part of their post-market management strategy. A plan should be developed prior to market entry for ongoing monitoring of and response to emerging cybersecurity threats. This plan should apply throughout the device’s life cycle. Items to consider as part of this plan, developed prior to market entrance, should include:

- **Post-market Vigilance**: A plan to proactively monitor and identify newly discovered cybersecurity vulnerabilities, assess their threat, and respond.
- **Vulnerability Disclosure**: A formalized process for gathering information from vulnerability finders, developing mitigation and remediation strategies, and disclosing the existence of vulnerabilities and mitigation or remediation approaches to stakeholders.
- **Patching and Updates**: A plan outlining how software will be updated to maintain ongoing safety and performance of the device either regularly or in response to an identified vulnerability.

- **Recovery**: A recovery plan for either the manufacturer, user, or both to restore the device to its normal operating condition following a cybersecurity incident.
- **Information sharing**: Participation in Information Sharing Analysis Organizations (ISAOs) or Information Sharing and Analysis Centers (ISACs) that promote the communication and sharing of updated information about security threats and vulnerabilities.

5.5 Labeling or Customer Security Documentation

In addition to the instructions for use, the technical documentation written by the manufacturer for installation, configuration of the device, as well as the technical requirements for their operating environments are particularly important for a safe and secure use by the user. This also includes providing the Software Bill of Material (SBOM) to ensure appropriate level of transparency. Importantly, administrators can use the SBOM as part of their asset management to examine applications and code from suppliers to obtain an accurate view of potential vulnerabilities and weaknesses, as well as identify required software patches in a timely manner in order to better protect their systems. The SBOM also helps inform purchasing decisions by providing prospective buyers with visibility into the components used in applications and determining potential security risk and licensing problems. This labeling is also referred as Customer Security Documentation. It is recommended that the following be included in the labeling to communicate to end-users relevant security information, taking into account the relative presumed cybersecurity risk. Care should be taken on providing such information which could potentially increase cybersecurity risks if inappropriately disclosed.

- Device instructions and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-virus software, use of a firewall).
- A description of backup and restore features and procedures to regain configurations.
- Specific guidance to users regarding supporting infrastructure requirements so that the device can operate as intended.
- A description of how the device is or can be hardened using secure configuration. Secure configurations may include end point protections such as anti-malware, firewall/firewall rules, whitelisting, security event parameters, logging parameters, physical security detection.
- A list of network ports and other interfaces that are expected to receive and/or send data, and a description of port functionality and whether the ports are incoming or outgoing (note that unused ports should be disabled).
- Sufficiently detailed system diagrams for end-users.
- Where appropriate, technical instructions to permit secure network (connected) deployment and servicing, and instructions for users on how to respond upon detection of a cybersecurity vulnerability or incident.
- A description of how the device or supporting systems will notify the user when anomalous conditions are detected (i.e., security events) where feasible. Security event types could be configuration changes, network anomalies, login attempts, anomalous traffic (e.g., send requests to unknown entities).
- A description of the methods for retention and recovery of device configuration by an authenticated privileged user.
- Where appropriate, risks of using the medical device outside of the intended use environment.
- A description of systematic procedures for authorized users to download and install updates from the manufacturer.

- Information, if known, concerning device cybersecurity end of support (see Section 6.4, Legacy Medical Devices).
- A SBOM including but not limited to a list of commercial, open source, and off-the-shelf software components including the version and build of the components, to enable device users (including patients and healthcare providers) to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the device (and the connected system) and to deploy countermeasures to maintain the device's safety and performance. Manufacturers should leverage industry standards in the deployment of the SBOM

5.6 Regulatory Submission Requirements

In addition to the activities outlined in the preceding sections, medical device manufacturers are encouraged to clearly document and summarize their activities related to cybersecurity. Depending on the risk class of the device, the regulator may require this type of documentation to assess the medical device prior to market entry or may request it during the post-market phase of the product's life cycle. Should the regulator require cybersecurity documentation for pre-market authorization, the manufacturer is encouraged to submit clear documentation describing, in relation to cybersecurity, the device's design features, risk management activities, testing, labelling, and evidence of a post-market plan to monitor and respond to emerging threats. The following paragraphs provide further clarity on each of the above items:

5.6.1 Design Documentation

Documentation that describes the device including any interfaces or communication pathways, and all design features that were included to mitigate cybersecurity risks and threats such as those previously outlined in Section 5.1 above (e.g. access control, encryption, secure updates, logging, physical security, etc.).

5.6.2 Risk Management Documentation

Documentation that clearly describes cybersecurity threats and vulnerabilities, an estimation of the associated risks, descriptions of the controls in place to mitigate those risks and evidence to demonstrate that those controls have been adequately tested. Manufacturers should consider risk controls that maximize device cybersecurity while not unduly affecting other safety controls. Specifically, the risk management documents related to cybersecurity that are submitted to the regulator should be clear, follow the requirements of ISO 14971and AAMI TIR57, and include:

- Comprehensive risk management documentation, such as a risk management report or security risk management report which should include any threat modelling, and identifiable cybersecurity threats.
- Discussion on any impact of security risk mitigations on the management of other risks;
- A summary of the manufacturer's plan to maintain the device's cybersecurity resiliency throughout its entire product life cycle.

5.6.3 Security Testing Documentation

Test reports that summarize all tests performed to verify the security of the device and the effectiveness of any mitigating controls. Details of specific testing, such as cross-referencing software components or subsystems with known vulnerability databases, for example, can be found in Section 5.3 above, however all testing documents should contain:

- Descriptions of test methods, results, and conclusions
- A traceability matrix between security risks, security controls, and testing to verify those controls; and
- References to any standards used.

5.6.4 Post-market Management Plan

A summary of the device's maintenance plan describing the post-market processes by which the manufacturer intends to ensure the continued safety and performance of the device throughout its life cycle. As described in Section 5.4 above, these planned processes may include: post-market vigilance, planned updates, patching, vulnerability disclosure policies, and information sharing.

5.6.5 Labelling or Customer Security Documentation

All additional user documentation that includes relevant information, as outlined in Section 5.5 above, to allow the user to effectively manage risk in the device's intended environment.

6.0 Post-Market Considerations for Medical Device Cybersecurity

As vulnerabilities change over time, pre-market controls designed and implemented may be inadequate to maintain an acceptable risk profile; therefore, a post-market approach is necessary in which multiple stakeholders play a role. This post-market approach includes various elements and include: the operation of the device in the intended environment, information sharing, coordinated vulnerability disclosure, vulnerability remediation, incident response, and legacy devices. The following sections are intended to introduce these concepts and provide recommendations to all key stakeholders in the post-market phase of the product's life cycle.

6.1 Operating Devices in the Intended Use Environment

6.1.1 Healthcare Providers and Patients

a. Cybersecurity best practices to be adopted by healthcare providers

With regard to medical device cybersecurity, it is important to recognize that it is a shared responsibility and requires participation of all stakeholders, including healthcare providers. Healthcare providers should consider adopting a risk management process to address the safety, effectiveness and cybersecurity aspects of medical devices that are connected to their IT infrastructure. The process should be applied at the (i) initial development of the IT infrastructure; (ii) integration of a new medical device into existing IT network; and (iii) changing of operating systems or IT network or to the medical device itself (software and firmware) with updates or modifications. In order to carry out the above-mentioned risk management process, healthcare providers may refer to relevant standards such as: IEC 80001-1, ISO 31000, and the ISO 27000 series in particular ISO 27799 for adoption.

In addition to adopting a risk management system, healthcare providers should also adhere to the following general cybersecurity best practices to maintain the healthcare provider's overall security posture:

- Good physical security to prevent unauthorized physical access to medical device or network access points;
- Access control measures (e.g. role based) to ensure only authorized personnel are allowed access to network elements, stored information, services and applications;
- Network access control to limit medical device communication;
- Patch management practices that ensure timely security patch updates;
- Malware protection to prevent attacks;
- Session timeout to prevent unauthorized access to devices left unattended for extended period.

The implementation of these best practices should be placed in context with the clinical use of the device. For example, adherence to these best practices may not be feasible in a medical emergency.

b. Training/education for all users

Finally, healthcare providers should take a holistic approach to prevent cybersecurity incidents from occurring in their institutions. As such, they are encouraged to provide the following cybersecurity training:

- Basic training to create security awareness and introduce cyber hygiene practices among all users (e.g. doctors, nurses, biomedical engineers, technicians, etc.);
- Training should also be extended to patients if the connected medical devices (e.g. home use devices such as a continuous glucose monitor or portable insulin pump) are intended to be operated by the patients themselves. The training is expected to consist of the following:
  - Operating the medical device in a secure manner (e.g. only connect their devices to secured network);
  - Ability to spot any anomalous device behavior and report to their healthcare provider/doctor immediately.

6.1.2 Medical Device Manufacturers

In addition to the information contained in the product labelling, manufacturers are encouraged to partner with health delivery organizations, redistributors and consumers of their products when possible to ensure optimal deployment and configuration of their devices.

6.2 Information Sharing

Information sharing is a vital tool for managing cybersecurity threats and vulnerabilities across multiple sectors of the global economy. Standards and best practices for intelligence and threat sharing have been developed and implemented in sectors outside of healthcare; and medical devices stakeholders are encouraged to adapt proven tools from other sectors to strengthen the security of the medical device ecosystem.

Because of the varied access to resources, different methods, and range of maturity levels across stakeholders, there is also a spectrum of valid approaches to information sharing. In addition, cybersecurity best practices continue to evolve and are informed by several factors, including device type, connected infrastructure, organizational size and maturity, and threat level. Therefore, this document does not favour one specific approach over another. Instead, it articulates the principles that should be followed with regard to information sharing. Examples are not intended to specify requirements, but rather to serve as illustrations.

Manufacturers, healthcare organizations, medical device users and other stakeholders should also consider cybersecurity requirements from other interacting sectors. Because cybersecurity is a whole-of-economy concern, businesses will often be operating in an environment with multiple sources of guidance, standards and regulation. It is the intention of this document to provide guidance specific to the cybersecurity of medical devices, but it should be considered against other requirements and best-practices.

6.2.1 Key Stakeholders

The medical device sector is regulated and global. Consequently, local or jurisdictional recommendations for information sharing may not be sufficient for a manufacturer who is supplying devices to multiple markets. Strategies for sharing information relating to the security of medical devices need to be global. Stakeholders may therefore need to be involved in multiple networks, recognizing that some networks may be international.

Information relating to the security of medical devices should be shared with anyone who needs that information to ensure that the medical device in question can be used safely. This may include users, patients, other manufacturers, distributors, healthcare organisations, security researchers, and the public. However, it is important to balance the type of information that is meaningful and actionable for different stakeholders. One useful approach could be ‘need to know’, i.e., does the stakeholder need to know this information to ensure patient safety? For example, information about a more secure chipset could be important across manufacturers, but the information may provide no benefit to end-users of the device. In contrast, knowing how to protect devices from a high-risk vulnerability while a patch is still in development and prior to deployment is likely important for all stakeholders.

a. Regulators

Medical device regulators, generally mandated with the protection and promotion of public health, play a fundamental role in information sharing. Regulators are a key receiver of information that relates to the security of medical devices, and are also often involved in its dissemination. Furthermore, they have an industry wide view and usually interact with other agencies within and external to the health sector. Many jurisdictions have statutory requirements for what information must be shared with regulators. However, stakeholders are encouraged to share any information that will help the regulator manage expectations and facilitate regulatory requirements. Importantly, many medical devices are distributed in multiple markets and therefore multiple regulatory jurisdictions. To ensure globally consistent information and, if appropriate, a globally aligned response, manufacturers should aim to synchronize notification of all the regulators where the affected product is distributed. Similarly, regulators should share information amongst each other to facilitate a globally coordinated response.

b. Healthcare Organisations

As primary consumers of information related to medical device security, health care organisations will often be responsible for taking action or facilitating action. They therefore should have access to any information needed to implement a recommendation, and to ensure the protection of their patients.

Healthcare organisations are also key generators of information because they work with medical devices in the field. They are also key sources of verification. Furthermore, because many actions taken to remediate a vulnerability or threat would likely happen in their facilities, healthcare organisations are key advisors in designing a response to a vulnerability.

c. Users

End users of medical devices include clinicians, patients, caregivers, and consumers. These individuals are often the ones making the final choice on whether a patch or other correction is actioned. Therefore, they need clear and meaningful information so that they can make an informed decision. Technical jargon will generally not be appropriate for this audience. This may need to include information about the clinical benefits and risks associated with deploying a patch, or compensating controls required until the patch is available. Providing education to the clinical community on how to have these risk-benefit discussions with patients is of value.

Cybersecurity is an emerging challenge in medical devices, and so it is often not part of a clinician's education. Therefore, increasing awareness and educating clinician communities is important for empowering them to discuss risks and benefits with their patients, and to make clinical decisions that are impacted by cybersecurity considerations.

d. Other stakeholders, including governments and information sharing entities

Key stakeholders from outside the healthcare sector also have important roles. Law enforcement, security, and other government agencies are important stakeholders in the cybersecurity of medical devices. Healthcare facilities are considered critical infrastructure and so it is important for governments to have critical and timely information regarding potential threats. Each jurisdiction will be different, but manufacturers (and regulators) should consider if they need to share information about the security of their products with wider government. In some jurisdictions there are multiple requirements for reporting security vulnerabilities, or incidents (e.g. data breaches).

Entities that collect or share information, or provide security advice or expertise can also be important sources of security information as well as support resources. These may be government or private organizations. Examples include information sharing networks (e.g. ISAOs, ISACS), dissemination agencies (e.g. CERTs), and others. These stakeholders are likely to differ between jurisdictions and markets.

6.2.2 Types of Information

Cybersecurity vulnerabilities can pose threats to multiple product components, including software and hardware, and first-party or third-party components. For example, a vulnerability in a shared library, operating system or chip will affect any product using that same component. Furthermore, the nature of vulnerabilities is that they are continually discovered during the product's lifetime. The goal of information sharing in the context of medical devices, is to protect patients from harm. Therefore, any information that, if shared, would reduce the risk of patient harm or ensure continuity in healthcare delivery should be shared. This might include, but is not limited to, sharing:

- Information about the vulnerabilities of the products
- Information about vulnerabilities of components that are used in other products
- Information about IT equipment that may impact the security of medical devices
- Information about attacks, potential and exploit development
- Confirmation of incidents (e.g. "Are you seeing this too?")
- Availability of patches or more secure alternatives

An important principle is that information sharing should not be limited to vulnerabilities and threats, but also practices and methods that may mitigate threats, for example, how IT equipment can be configured to mitigate a vulnerability that impacts a medical device, or methods for responding to known exploits.

6.2.3 Trusted Communication

Information about security vulnerabilities and threats can be sensitive, but also vital to managing patient safety. Therefore, it is important that information is shared freely and in good faith, with the aim of improving patient safety. Commercial interests need to be set aside in this case. Information sharing networks should be set up with the understanding, a written agreement if necessary, that information is shared to improve security and patient safety, and shared information is not to be used to gain a commercial advantage.

It also needs to be recognised that regulators are a key collaborator in this ecosystem, but may be bound by legislation to take action in particular cases. That said, regulators should aim to build processes that encourage timely disclosure of information relating to the cybersecurity of medical devices.

6.3 Coordinated Vulnerability Disclosure

Transparency is an essential building block in cybersecurity because it is difficult to secure what is not known. One mechanism that enhances transparency is coordinated vulnerability disclosure (CVD). CVD establishes formalized processes for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing mitigations and compensating controls, and disclosing this information to various stakeholders—including customers, peer companies, government regulators, cybersecurity information sharing organizations, and the public.

Adopting CVD policies and procedures is a proactive approach that enables end users of impacted technologies to make more informed decisions regarding actions that they can take to better protect their medical devices, Health IT infrastructure, and patients.

Engaging in CVD is a responsible course of action for raising awareness to security issues and should be viewed as a sign of a manufacturer's maturity related to continuous quality improvement and risk management, as is noted in other industry sectors. As stated in the US Energy and Commerce Committee report titled The Criticality of Coordinated Vulnerability Disclosure in Cybersecurity: "*The Committee's work has shown that the complexity of modern information systems and networks makes coordinated disclosure an essential, rather than optional, part of an organization's overall cybersecurity strategy. This fact is demonstrated by the increasing number and frequency of significant coordinated disclosures, highlighted most recently by the Spectre and Meltdown disclosures that impacted nearly every modern technology that relies on computer chips. As the Committee's investigation into that disclosure showed, not only is coordinated disclosure critically important, its criticality necessitates that society move past a debate of whether coordinated disclosure is "good" or "bad" and instead focus on how disclosure processes may be meaningfully improved."*

Though a forward-leaning stance with respect to CVD is a sign of proactive and responsible corporate behavior, there have been several unfortunate instances of medical device manufacturers facing negative publicity as a consequence of adopting this best practice.

6.3.1 Medical Device Manufacturers

As the medical device ecosystem continues to mature, the benefits of behaving in a transparent manner will be more fully recognized. Disclosure of this type is of extreme importance by pre-emptively protecting the public from potential harm across multiple marketed products that may be impacted by the same vulnerability. Manufacturers also benefit directly from transparent behavior as it enables improved security design for new products. Healthcare providers and patients should be made aware that CVDs from manufacturers and through computer response teams such as CERTs and Computer Security Incident Response Team (CSIRT) or government regulators are the only authoritative source of information regarding vulnerabilities. No medical device is completely free of vulnerabilities and as such, engaging in CVD should be a part of routine practice. It is not the number of vulnerabilities that serves as an indicator of a manufacturer's cybersecurity posture, but rather the consistency and timeliness with which it responds.

Manufacturers are expected to develop and distribute information through customer bulletins, notifications, or other means in a timely manner after the matter has been assessed. Manufacturers should be aware of specific jurisdictional requirements regarding timely communications.

CVD should be part of manufacturers' proactive approach to medical device cybersecurity because it aids in improving patient health and safety. As it relates to a proactive CVD, manufacturers should:

- Monitor cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk

- Adopt a coordinated vulnerability disclosure policy and practice (ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure). This includes acknowledging receipt of the initial vulnerability report to the vulnerability submitter within a specified time frame
- Establish and communicate processes for vulnerability intake and handling (ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes). These processes are clear, consistent, and reproducible irrespective of the originating source of the vulnerability (e.g. security researcher or healthcare provider, etc.)
- Assess reported vulnerabilities according to established security (e.g. CVSS) and clinical (e.g. ISO 14971) risk assessment methodologies
- Develop a remediation if possible. If not possible, develop appropriate vulnerability mitigation and/or compensating controls with established means of reporting deployment failures and rolling back changes.
- Engage with regulators so that they have awareness of forthcoming vulnerability disclosures
- Communicate a description to stakeholders of the vulnerability including scope, impact, risk assessment based on the manufacturer's current understanding and describe the vulnerability mitigations and/or compensating controls. Stakeholders should also be updated as the situation changes.
- Deploy a remediation if available. If not, deploy mitigations and/or compensating controls with established means of reporting deployment failures and rolling back changes.

In addition to its own customer communications, manufacturers are encouraged to coordinate disclosure of their vulnerabilities globally. Computer Emergency Response Teams (CERTs) and equivalent organizations often work collaboratively with the vulnerability finder and the manufacturer throughout the CVD process. In particular, CERTs often play a role in public disclosure via global and regional CERT advisories translated into local languages. For more information regarding CVD, please see the CERT® Guide to Coordinated Vulnerability Disclosure

6.3.2 Regulators

Regulators can help support coordination of vulnerability assessment/evaluation, impact analysis, and mitigation/remediation process between the manufacturer and the vulnerability finder, which ultimately can then drive towards more timely communication to the public in order to mitigate risk of exploit. This communication includes concurrent global communications as appropriate as CVD is recognized as a best practice.

6.3.3 Vulnerability Reporters (includes security researchers and other vulnerability finders)

Vulnerabilities, when discovered, should be reported either directly to the relevant manufacturer or to a coordinating third party, such as an appropriate government entity. The manufacturer then coordinates and communicates with the reporter of the vulnerability throughout its assessment and remediation. Finally, the vulnerability reporter and manufacturer should coordinate in disclosing the vulnerability publicly. As adopted from the National Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group (December 2016), as long as the manufacturer is responsive to the reporter and there is no evidence of an attack using the vulnerability in the wild, coordinated disclosure means that the reporter of the vulnerability does not disclose it until a fix or other mitigation has been developed. If the reporter discloses the vulnerability ahead of a fix, then the reporter and manufacturer should at least coordinate in describing a full range of possible mitigations, putting users, including healthcare providers and/or patients, in the most empowered position to operate their devices safely and securely.

6.4 Vulnerability Remediation

Actions associated with vulnerability remediation are essential to reducing the risk of patient harm. Remediations may include a wide-range of actions including patient notifications. As such, several stakeholder groups play critical roles in this process and these roles are described in greater detail below.

6.4.1 Medical Device Manufacturers

a. Risk Management

The first part of any response to a cybersecurity vulnerability in a medical device is risk assessment. Risk management is a well-established and mature practice in the medical device sector. This practice should be applied to evaluating the patient safety impact of cybersecurity vulnerabilities by manufacturers and regulators alike. A remediation strategy that is well- grounded in the context of patient safety can then be developed and agreed upon. To drive the effectiveness of this approach, information should be shared between regulators and manufacturers, especially with regard to perceived risk and justification of action. Since the outcome of risk assessment informs prioritization and timing of remediation, manufacturers and regulators are unlikely to agree on an appropriate remediation strategy if their respective perception of risk differ significantly.

Manufacturers and regulators also need to take into account the risk perceived by other stakeholders who may be less familiar with risk management, quality management and regulation. This can lead to different expectations about how the manufacturer should respond to a security vulnerability and within what timeframe. Similarly, some stakeholders may not understand risk reduction mechanisms, such as compensating controls, that can be deployed to sufficiently protect a vulnerable device, hence mitigating risk of patient harm to an acceptable level. Inaccurate information that overplays the risk to patients can create a crisis of confidence in healthcare technologies.

All stakeholders need to recognise that, like other risk related to medical devices, cybersecurity vulnerabilities are managed with regard to the risk they represent to patients and users.

b. Third Party Components

Third party components are a key part of the medical device supply chain, whether they are software or hardware. These components can create risk of their own, which is managed by the manufacturer through risk management, quality management, and design choice. Manufacturers should manage the cybersecurity implications of the components - software and hardware - that

are part of their devices. Similarly, post-market issues with a third party component may also affect the security of the medical device, and manufacturers need to manage this risk.
Users expect the manufacturer to understand how a security vulnerability in an underlying component such as an operating system or processor affects the medical device. Regulators will require it.

The response of manufacturers to a vulnerability in a third party component should be the same as for first party vulnerabilities, namely, ongoing risk management and sharing of information with customers and users. While manufacturers are unlikely to have control over the timing of resolution for a third party vulnerability (e.g., availability of a patch or update), they are still expected to take measures to reduce risk to patients and users.

c. Communication

As discussed in other sections of this document, communication with those who need information to manage risk to patients is vital. Communication should include the following key information: timeline for vulnerability resolution (e.g., when will a fix be available); mechanism for resolution (e.g., how will patch deployment occur); and interim risk mitigating measures (e.g., what actions should be taken, including use of compensating controls, while awaiting the more permanent resolution).

d. Remediation Action

Stakeholders' actions will depend upon multiple factors including the type of device, the regulatory jurisdiction, the risk to users, and the intended purpose. Therefore, this document does not elaborate upon specific action that is expected for all devices. There are, however, principles that should underlie all vulnerability remediation actions:

- Compliance with local regulatory requirements
- Adherence to the essential principles of safety and performance
- Information sharing with stakeholders to reduce the risk to patients and users
- Cooperation of stakeholders to achieve the agreed remediation
- Timely remediation, relative to the risk

When the device lacks sufficient fundamental or inherent protective measures, and updates are not feasible (e.g. certain legacy devices), risk-mitigating alternatives should be applied as compensating controls. Examples may include - installing a firewall appliance between device and medical IT-network, or removing the device from the medical IT-network. These compensating controls are generally implemented by the healthcare provider based on the information provided by the manufacturer.

Regulators operate under their jurisdiction's legislation, which means that they may impose particular requirements before remediation can be applied to medical devices in their market. Manufacturers need to consider this when planning vulnerability remediation actions. Regulators should be informed early on so as not to impede or delay the manufacturer's remediation activities from proceeding. Early notification to regulators allows ample time to initiate any regulatory processes or required actions while concurrently supporting expedient remediation and assisting in managing stakeholders and their expectations (e.g. users, media, public).

Information about security vulnerabilities travels rapidly in a global economy and exploits of security vulnerabilities can reach around the globe in seconds. Consequently, a global and coordinated strategy to remediate vulnerabilities is needed. If a vulnerability is corrected and disclosed in one jurisdiction, but remains unaddressed in another, it can give an adversary an advantage and leaves patients, as well as the healthcare sector at large, exposed to attack.

Manufacturers who supply to multiple markets are expected to coordinate the release of information and remediation to minimize timing gaps. The manufacturer's coordination should extend to proactive communication with all of the regulators where affected product is in distribution.

All stakeholders need to recognise that immediate patching may not be possible, or desirable, and that interim measures may be critical to ensuring patient safety. This is particularly important where those measures must be implemented by stakeholders outside of the direct control of the manufacturer or the regulator. For example, some actions can only be taken by a hospital IT department. Successful execution of remediation strategies is often dependent upon effective information sharing and stakeholder management (including users and media). It is important to note that remediation, though ideal, may not always be possible and in that instance appropriate risk mitigations and compensating controls should be applied.

6.4.2 Healthcare Providers and Patients

a. Patching

Patients receive medical care in professional healthcare facilities and in the home healthcare environment, and each use environment is associated with unique considerations for patching.[3] In the home healthcare environment, for example, the user can be the patient, caregiver, trusted neighbor, or a family member. This section provides general guidance for patching and subsequent sections describe specific considerations for each use environment.

In the context of cybersecurity, the installation of corrective and preventive changes is commonly referred to as "patching" although adaptive and perfective changes are also possible. Subclause 6.2.5 of IEC 62304:2006 +AMD1:2015, Medical device software — Software life cycle processes, requires manufacturers to inform users and regulators about any problem in released medical software and how to obtain and install changes. Specific users of a medical device, as identified by the manufacturer and approved by the local regulatory authority, are expected to implement patches provided by a manufacturer in accordance with associated installation instructions. These users should follow manufacturer guidance to access service bulletins and other information typically provided on a web page.

[3] IEC 60601-1-11:2015, *Medical electrical equipment — Part 1-11: General requirements for basic safety and essential performance – Collateral Standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment*, defines the "home healthcare environment" as "dwelling place in which a patient lives or other places where patients are present, excluding professional healthcare facility environments ..." and includes examples of "In a car, bus, train, boat or plane, in a wheelchair or walking outdoors."

When a patch cannot be applied within a reasonable time frame, the manufacturer may recommend compensating controls (e.g., segmentation of a medical IT-network) or changes to user-programmable settings of the medical device. To reduce the risk of patient harm for certain types of vulnerabilities, the local regulatory authority may direct the manufacturer to disable specific functionality of the medical device, accessories, or the supporting ecosystem (e.g., software update servers). In either case, users should follow manufacturer guidance and, as appropriate, assess risks associated with their use environment.[4]

Table 2 is adapted from patching methods documented in the Joint Security Plan.[5] The rightmost column of the table describes the primary responsibility of the user identified to implement a manufacturer-validated patch.

Patching method	Summary description	User responsibility
Remote update	Patches applied via secure authorized remote service and support platforms provided by the manufacturer.	Ensure remote connectivity in accordance with instructions provided by the manufacturer.
User administered	Validated patches are available for customer retrieval and installation from a designated source including direct download from the third-party that provides the product or component.	Retrieve and install the patch in accordance with instructions provided by the manufacturer.
Service visit	Local service facility administers cybersecurity patches (includes on-site servicing). Note, this method is applicable in cases where faulty patching has foreseeable and serious harm and local service personnel may be required for resolution.	Provide the medical device to a service facility, support an on-site service visit, or travel to a professional healthcare facility.

Table 2: Patching methods and user responsibility for implementation

Note, for service visits, the user is responsible for interacting with a qualified professional for patch installation.

b. Considerations for the professional healthcare facility environment

In professional healthcare facilities, patients are provided care by qualified healthcare professionals (e.g., nurses, physicians) who may be licensed or unlicensed as a function of local regulatory requirements. Patients are expected to follow instructions provided by these

[4] In general, patients who are also users do not have sufficient training to assess risk.

[5] *Medical Device and Health IT Joint Security Plan*, Healthcare and Public Health Sector Coordinating Council (HSCC), January 2019. Note, the first two columns incorporate minor changes to improve clarity and the "ad hoc" patching method is removed (only validated patches are considered).

professionals, including those pertaining to security, to ensure safe and effective operation of their medical device.

Subclause 3.2 of IEC 80001-1:2010, Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities, describes risk management responsibilities of the "responsible organization" including maintenance of medical devices deployed in a medical IT-network. The responsible organization can be different than the patient's immediate healthcare provider. Patching is one type of risk control measure and subclause 4.4.4.3 provides specific guidance:

"Risk control measures within the medical device should only be implemented by the medical device manufacturer or by the responsible organization following the instructions for use or with the documented permission of the medical device manufacturer. … Any changes to a medical device undertaken by the responsible organization without documented consent of the medical device manufacturer are not recommended."

These recommendations were developed to ensure efficient and safe management of medical IT-networks. Lay persons should not be permitted to install patches in medical devices that are connected to medical-IT network.

As highlighted in IEC 80001-1, responsibility agreements are one option to ensure that all parties understand the shared responsibility of managing devices in a medical IT-network. If a manufacturer is directed to disable certain functions of the medical device, then healthcare providers should evaluate their clinical workflow to ensure patient safety is maintained.

c. Considerations for the home healthcare environment

The home healthcare environment accommodates a diverse set of potential users as noted in FDA's related guidance, Design Considerations for Devices Intended for Home Use:

"The users of home use devices are different from the health care professionals who typically operate medical devices in a professional health care facility. Home users can have a large range of physical, sensory, and cognitive capabilities and disabilities, and emotional differences that should be considered in your home use device design."

The applicability of patching methods for the home healthcare environment is a function of many factors including medical device classification, resource requirements (e.g., high-speed internet connection), and usability. Due to the wide range of user capabilities, many home use devices require the "service visit" patching method listed in Table 1. Patch installation for an implanted medical device may require in-person interaction with the patient's healthcare provider.

Some home use devices, especially those categorized as SaMDs, accommodate the remote update or user administered patching methods. Remote updates require the least amount of user interaction but often necessitate patient consent in accordance with processes established by the healthcare provider. With either patching method, patients should follow instructions provided by their healthcare provider and, as applicable, the medical device manufacturer.

If a patient intends to travel internationally, then they should speak with their healthcare provider to understand software maintenance options for their device.

6.4.3 Regulators

a. Post-market patching

Threat actors are constantly adapting and advancing exploitation techniques. As a result, frequent software maintenance activities are often required to enhance a device's cybersecurity resilience ("cyber hygiene"), remediate vulnerabilities, or mitigate risk for vulnerabilities that cannot be remediated. If each change made "solely to strengthen cybersecurity" were subjected to the highest level of regulatory review, then the resulting review burden would soon overload most regulatory authorities.

In the context of cybersecurity, the regulatory authority should establish two fundamental questions to determine if a software change requires approval prior to release:

1. Is the change proposed to solely strengthen cybersecurity and has been determined to not have any other impact on the software or device?

The manufacturer should evaluate their system to ensure that such changes do not impact the safety or effectiveness of the device by performing necessary analysis, verification, and/or validation. If a manufacturer becomes aware of any incidental or unintended impacts of the change on other aspects of the software or device, then the regulatory authority may determine that review of the proposed modification, pre-deployment, is appropriate.

2. Is the change proposed to remediate or reduce the risk of a vulnerability associated with unacceptable residual risk related to patient harm?

Post-market vulnerability risk assessments should be based on an evaluation of exploitability and the severity of potential patient harm. Note, the definition of "patient harm" is a subset of "harm" as defined in ISO 14971:2007, Medical devices — Application of risk management to medical devices.[6] The narrow definition of patient harm has the net effect of prioritizing regulatory review of those changes necessary to protect public health.

Table 3 is applicable to changes made solely to strengthen cybersecurity that do have any other impact on the software or device (i.e., an affirmative response to the first question posed in this section). Otherwise, regulatory processes for non-cybersecurity software changes are applicable.

Purpose/(categorization) of software maintenance	**Level of regulatory requirements**	**Examples**
Enhances security ("cyber hygiene")	Low	A Software as a Medical Device (SaMD) application ("app") manufacturer is informed of a host operating system update

[6] ISO 14971:2007 defines "harm" as "physical injury or damage to the health of people, or damage to property or the environment" whereas "patient harm" only includes the first phrase of this definition.

			that adds security controls to support a defense-in-depth strategy. The SaMD app requires modification to be compatible with low-level interface changes in the host operating system. The associated SaMD app modifications are not related to any known vulnerability.
Vulnerability remediation or risk reduction	(Acceptable residual risk of patient harm)	Medium	A device manufacturer receives a user complaint that a blood gas analyzer has been infected with malware and there was concern that the malware may alter the data on the device. The outcome of a manufacturer investigation and impact assessment confirms the presence of malware and finds that the malware does not result in the manipulation of unencrypted data stored and flowing through the device. The device's safety and essential performance is not impacted by the malware and the manufacturer's risk assessment determines that the risk of patient harm due to the vulnerability is acceptable. [7]
	(Unacceptable residual risk of patient harm)	High	A manufacturer is made aware of open, unused communication ports. The manufacturer acknowledges receipt of the vulnerability report to the submitter/identifier and subsequent analysis determines that the device's designed-in features do not prevent a threat from downloading unauthorized firmware onto the device, which could be used to compromise the device's safety and essential performance. Although there are no reported serious adverse events or deaths associated with the vulnerability, the risk assessment concludes the risk of patient harm is unacceptable. [8]

Table 3: Software maintenance and recommended level of regulatory oversight

If the proposed software change affects multiple vulnerabilities, or alternatively improves "cyber hygiene" and affects at least one vulnerability, then the manufacturer should consider the highest

[7] Adapted from examples provided in *Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices*. Dec. 2016.

[8] Ibid.

applicable level indexed in Table 3 to inform subsequent actions. For example, a single software change could enhance system security, reduce risk for Vulnerability A (acceptable residual risk of patient harm), and remediate Vulnerability B (unacceptable residual risk of patient harm). In this case, the “high” level of regulatory requirements associated with Vulnerability B would apply.

For any level, the regulatory authority may, at their discretion, request evidence that the manufacturer is following established life cycle processes and other regulatory requirements for software maintenance including those identified in IEC 62304, Medical device software — Software life cycle processes.

6.5 Incident Response

6.5.1 Medical Device Manufacturers

Medical device manufacturers should prepare for response to cybersecurity incidents and events which may impact their products and customers including patients. As such, manufacturers should establish an incident response management policy and build an incident response team based on its product portfolio. The aim of incident response team is to provide appropriate capacity for assessing, responding to and learning from cybersecurity incident, and providing the necessary coordination, management, feedback and communication, for timely and pertinent action during the next incident.

Preparedness includes establishing an incident management policy, developing detailed incident response plans, building an incident response team, routinely testing and exercising incident response, and continuously improving this capability through lessons learned.

Incident management as defined in ISO/IEC 27035 includes the following at a high-level (see roles and responsibilities section for additional detail): plan and prepare, detection and reporting, assessment and decision, responses and lessons learned (see appendix for items description)

a. Roles and Responsibilities

The incident response team could be divided into different groups: manager, planning group, monitoring group, responding group, implementation group, analyzing group, and sometimes including external experts. Each group have different roles and responsibilities. The team should assign members to these groups based on their skills and knowledge and some of the positions may be filled by more than one team members. The members assigned to the relevant groups should be responsible for the same or similar work. More detailed information on the roles of manager, planning group, monitoring group, responding group, implementation group, analysing group are provided in Appendix A.

b. Communication Expectations

Customers should be provided contact information of a medical device manufacturer to report cybersecurity incidents and events, or otherwise submit through regular customer support channels. The aim of incident response team is to provide appropriate capacity for assessing, responding to and learning from cybersecurity incident, and providing the necessary coordination, management, feedback and communication, for timely and pertinent action during the next incident. The incident response team will establish a routine cadence for providing updates to all stakeholders impacted by an incident and work towards delivering customer-targeted communications as soon as possible after an initial discovery (manufacturers should be aware of specific jurisdictional requirements regarding timely communications). Achieving the aforementioned timing for bulletins or notifications by the vendor during incidents may be dependent on timely and accurate communication with customers.

Medical device cybersecurity incidents which impact patient safety and privacy must be reported to applicable regulatory agencies as required by regulation. When criminal activity has been identified through the course of investigation, local and applicable law enforcement agencies should be notified. Cyber Emergency Response Team (CERT) and Information Sharing and Analysis Organization (ISAO) should be contacted for further coordination on global cybersecurity attacks and events.

6.5.2 Healthcare Providers

Healthcare providers should establish policies for handling security incidents and mechanisms to mitigate or resolve a security incident and to disclose the related information to internal and external stakeholders. To that purpose, healthcare providers should consider building into the device purchase and/or maintenance fees the cost for mitigating device vulnerabilities. This could include ensuring that spare or extra devices will be available, as needed, during an incident.

a. Policy and Roles

Vulnerability or security incident handing policy and roles should be in place in a healthcare provider organisation. Those policies should establish the way healthcare providers will receive and disseminate information from manufacturer disclosure documents (e.g. MDS2, SBOM, vulnerability/patch information), information sharing institution or participating Information Sharing Analysis Organizations (ISAOs). To that end, a list of point of contacts must be maintained and verified periodically to inform and be informed. Similarly, service level agreements (SLAs), established before installation and periodically reviewed, provide the substance and terms which manufacturers and other vendors are obligated to fulfill, during or in response to an incident. Healthcare providers should establish their own Security Incident Response Team or similar organization.

b. Training by Roles

Requirements for training each relevant role should be established and periodically reviewed to determine if they need to be updated. Security experts who evaluate evidence of security incidents should have training in security forensic analysis in addition to practical experience. Those who participate in the incident response process should be trained in that process and the theory of incident response, in addition to practical experience. Training processes should be evaluated periodically and an incident response exercise may be played to perform that evaluation.

c. Analysis and Response

Healthcare providers should identify and verify a vulnerability or an incident from reports or communications between internal or external stakeholders. Healthcare providers should evaluate the impact and cooperate with stakeholders by providing information describing the result of the investigation. When any actions for the resolution are needed, the status of the investigation and its timetable should be included in the result. Healthcare providers should keep patients informed with safety related information including best practices and mitigation measures. When the resolution includes remediation, validation and non-regression must be performed before applying the remediation to the entire facility. Those tests should provide assurance that the remediation does not disrupt existing system functionality. Healthcare providers should update remediation and mitigation information as necessary.

6.5.3 Medical Device Regulators

Regulators are also engaged in medical device cybersecurity incident and response. As noted in the manufacturers' response section above, regulators should be notified of cybersecurity incidents so that they are aware, can request additional information for regulatory decision making, and can take additional actions as needed. As appropriate, additional actions may include but are not limited to the assessment of patient safety impact, assessment of the benefit/risk of a manufacturer's proposed mitigation, communication to stakeholders (including non-traditional stakeholders, e.g. cybersecurity researchers), and engagement with other governmental agencies and regulators.

6.6 Legacy Medical Devices

6.6.1 Medical Device Manufacturers

Legacy devices, or those medical devices that cannot be reasonably protected against current cybersecurity threats, are a challenge for healthcare stakeholders as the cybersecurity of these devices may not have been considered in the device design and maintenance. This challenge is further exacerbated by the fact that the clinical utility of a device often outlasts their security supportability. Legacy devices cannot be protected by making changes to the device's design, but compensating controls may be able to provide some level of protection. As appropriate, regulators encourage medical device manufacturers to leverage compensating controls to address legacy device challenges. Device design, vulnerability management, and customer communications all play an important role in addressing legacy device cybersecurity challenges. Recommendations for manufacturers include the following:

- Design and develop devices under a secure development framework such that devices, at a minimum, meet a security baseline and include mechanisms for updates and patches (i.e. maintained over its clinically useful life).
- Monitor legacy devices for critical vulnerabilities and provide a best-effort response and maintain ongoing risk documentation aligned to the total product life cycle of the device as a part of risk management.
- Clearly communicate the end of life (EOL) and end of support (EOS) dates of the devices as part of the procurement and installation process including a communication of customer responsibilities at these time points. This helps healthcare organizations understand their responsibilities and device risk.

6.6.2 Healthcare Providers

Many healthcare providers plan for a clinical useful life much longer than the communicated life of the device given by the manufacturer. However, as the threat landscape changes over time and new threats emerge, the risk and costs of using outdated technology increases and must be accounted for through a shared responsibility between the medical device manufacturer and the healthcare provider. The following recommendations are expected to help address healthcare providers' legacy challenges:

- Improved communication between medical device manufacturers and healthcare providers is necessary to ensure proper life cycle planning, understanding, and transparency.
- Complex medical devices often include many hardware and software components, including workstations, servers, operating systems and other 3rd party software that is engineered to work together to give clinicians the information necessary to diagnosis and treat patients. Within that software Bill of Materials (SBOM), those components with the shortest support life cycle will ultimately affect the supportability and security of those devices. To ensure transparency, medical device manufacturers should provide software BOMs to customers so they can better understand those components affecting the device life cycle. This BOM can include information for additional hardware for risk control measures such as compensating controls.
- Medical device manufacturers should clearly communicate key life cycle milestones, including End of Support dates that include software, for all products. Medical Device life cycle management, including support milestones and device update and upgrade options are the responsibility of the medical device manufacturer.
- Healthcare providers are responsible for ensuring proper support and maintenance of their medical devices while in use, either through the medical device manufacturer, 3rd party service agents or through internal resources and controls.
- Healthcare providers should continue to understand the risks within their environment and make every effort to control risks through proper mitigations, including but not limited to network segmentation, user access roles, risk assessment, security testing, network monitoring, etc.

7.0 References

7.1 IMDRF Documents

1. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations IMDRF/SaMD WG/N12:2014 (September 2014)

2. Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices IMDRF/GRRP WG/N47 FINAL:2018 (November 2018)

7.2 International Standards

3. IEC 60601-1:2005+AMD1:2012, Medical electrical equipment - Part 1: General requirements for basic safety and essential performance

4. IEC 62304:2006/Amd 1:2015, Medical device software – Software life cycle processes

5. IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices

6. IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities

7. IEC/TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

8. IEC/TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

9. ISO 13485:2016, Medical devices – Quality management systems – Requirements for regulatory purposes

10. ISO 14971:2007, Medical devices – Application of risk management to medical devices

11. ISO TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

12. ISO/IEC 27000 family - Information security management systems

13. ISO/IEC 27035-1:2016, Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management

14. ISO/IEC 27035-2:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response

15. ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure

16. ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes

17. ISO/TR 24971:20XX, Medical devices – Guidance on the application of ISO 14971 (under development)

7.3 Regulatory Guidance

18. ANSM (Draft) : Cybersecurity of medical devices integrating software during their life cycle (July 2019)

19. China: Medical Device Network Security Registration on Technical Review Guidance Principle (January 2017)

20. European Commission: REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (May 2017)

21. European Commission: REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (May 2017)

22. FDA (Draft): Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (October 2018)

23. FDA: Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software (January 2005)

24. FDA: Design Considerations for Devices Intended for Home Use (November 2014)

25. FDA: Postmarket Management of Cybersecurity in Medical Devices (December 2016)

26. Germany: Cyber Security Requirements for Network-Connected Medical Devices (November 2018)

27. Health Canada: Pre-market Requirements for Medical Device Cybersecurity (June 2019)

28. Japan: Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1 (April 2015)

29. Japan: Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1 (July 2018)

30. Singapore Standards Council Technical Reference 67: Medical device cybersecurity (2018)

31. TGA: Medical device cybersecurity - Consumer information (July 2019)

32. TGA: Medical device cybersecurity guidance for industry (July 2019)

33. TGA: Medical device cybersecurity information for users (July 2019)

7.4 Other References

34. CERT® Guide to Coordinated Vulnerability Disclosure
https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

35. The NIST Cybersecurity Framework
https://www.nist.gov/cyberframework

36. NIST's Secure Software Development Framework (SSDF)
37. https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

38. Medical Device and Health IT Joint Security Plan (January 2019)
https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

39. MITRE medical device cybersecurity playbook (October 2018)
https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

40. Open Web Application Security Project (OWASP)
https://www.owasp.org/index.php/Main_Page

41. ECRI approach to applying the NIST framework to MD
https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical-Devices.aspx

42. National Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group
https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

43. https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf

44. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

8.0 Appendices

8.1 Appendix A: Incident Response Roles (from ISO/IEC 27035)

Incident management – ISO/IEC 27035	
Plan and prepare	Establish an information security incident management policy, form an Incident Response Team etc.
Detection and reporting	Someone has to spot and report “events” that might be or turn into incidents.
Assessment and decision	Someone must assess the situation to determine whether it is in fact an incident.
Responses	Contain, eradicate, recover from and forensically analyze the incident, where appropriate
Lessons learned	Make systematic improvements to the organization’s management of information risks as a consequence of incidents experienced.

Incident response team		
Roles	**Responsibilities**	**Main actions**
Manager	Leads and makes decisions on major issues concerning cybersecurity incident response	a) commitment and support to incident response, including the provision of necessary resources (manpower, financial and material); b) review and approval of incident response policies and plans, and supervision of the implementation; c) review and revision of incident response plans; d) internal and external coordination of the team.
Planning Group	Operates the incident response	a) establishing and planning security policies; b) implementing security processes; c) adjusting the risk priorities; d) communicating with higher-level organizations and other third-party organizations; e) supporting administration; f) discussing/registering/approving vulnerability reports on the target organizations; g) performing other activities directed by the manager.
Monitoring group	Performs the real-time security monitoring activities	a) daily monitoring and operation; b) intrusion detection, registering incidents, and first responses; c) performing the security patches and upgrades; d) implementation of the security policy and backup management; e) help desk; f) facility management; g) performing other activities directed by the manager.
Responding group	Provides services such as real-time responses, technical support	a) propagating and reporting incidents; b) correlation analysis between monitoring systems; c) incident investigation and recovery supports; d) vulnerability analysis on the target incident; e) performing other activities directed by the manager.

Implementation group	Performs the total action of the incident response	a) analyzing incident response requirements; b) determining incident response policies and levels; c) implementation of incident response policies and plans; d) projecting incident response plans; e) summarizing the incident response work and report; f) deployment and use of incident response resources; g) performing other activities directed by the manager.
Analysing group	Performs incident analysis	a) planning vulnerability analysis for the team and manufacture; b) improving the security analysis tools and checklist; c) improving the monitoring rules; d) publication of newsletter; e) performing other activities directed by the manager.

8.2 Appendix B: Background on Legacy Devices

Legacy devices, or those medical devices that cannot be reasonably protected against current cybersecurity threats, are a challenge for healthcare stakeholders as the cybersecurity of these devices may not have been considered in the device design and maintenance. This challenge is further exacerbated by the fact that the clinical utility of a device often outlasts their security supportability. Device design, vulnerability management, and customer communications all play an important role in addressing legacy device cybersecurity challenges.

Medical device manufacturers must take into consideration the support life cycle of hardware and software components that comprise the medical device. In order to provide comprehensive support of a medical device, the manufacturer should be able to obtain support from the corresponding hardware and software vendors, by means of software/firmware updates and patches that address quality, performance and security concerns. A legacy medical device is determined by the manufacturer's published End of Life date (EOL). The manufacturer's EOL date signifies the diminished capacity to provide comprehensive support of the medical device for the aforementioned reasons. Medical device support is not guaranteed beyond the end of life EOL date. Manufacturers may offer limited support or best effort support beyond EOL, depending upon the medical device until the published end of support (EOS) date. The published EOS date designates the time where all service support activities by the medical device manufacturer will be terminated. Service support contracts should not extend beyond this point. No support should be expected for any medical device past the established EOS date.

The shift to digital technology within medical devices offered expanded functionality that could never be realized within older analog devices. Analog clinical devices can be operated for decades as long as the components performed as intended. The expectation within many HDOs is that newer digital technology should be comparable to the older analog model. Today's digital technology (workstations, servers, processors, etc.) are considered commodity items based on their relatively low cost and short life cycle. The advancements and innovations in digital technology have enabled clinicians to better serve their patients and improve treatment outcomes. These advancements, while beneficial to clinicians in diagnosing and treating patients, also introduced many new challenges for medical device manufacturers. With this shift to digital technology came significant costs associated with technologically advanced commodity computer components and a significantly reduced software support life cycle. Digital technology brought about several challenges, including but not limited to

- Reliance on third party software components,
- Reliance on vendor specific hardware components,
- Security related vulnerabilities potentially threatening these components and the operation of the medical device,
- Performance decrease over time as software and hardware components age, which can also increase the likelihood of costly device downtimes.

This combination of software, hardware, and network connectivity puts new demands on the device lifetime, which often consists of capital equipment (scanner hardware) and as well as commodity components (servers, workstations, databases and operating systems). The lifecycle expectations between capital and expense items are particularly problematic for medical device manufacturers since these products are designed and engineered to operate closely together as a validated medical device.

Purchasing IT-based medical devices requires a substantial capital investment for HDOs. In many cases, purchasing the device is only part of the total costs which may require the construction of new space or the redesign and restructuring of an existing space, as well as the associated installation costs. To control cost, HDOs may choose to operate the medical device well past the products support life cycle. A longer lifespan means a lower annual cost, which increases the perceived value for the HDO. As healthcare providers faces multiple challenges and must take into account the requirements associated with life cycle management and the lifespan of devices. It is important to note that, as equipment ages, the number of identified hardware and software vulnerabilities could potentially increase the inherit risks associated with these devices.

Many HDOs plan for a clinical useful life much longer than the communicated life of the device given by the manufacturer thus leading to HDOs having to consider the lost opportunity costs associated with postponing equipment upgrades and older devices tend to break down more often as components wear out and often require frequent service. For these reasons, among others, in establishing the Estimated Useful Lives of Depreciable Hospital Assets, the American Hospital Association (AHA) recommends a useful life for Magnetic Resonance Imaging (MRI) equipment of five years - CT scanners and X-ray units are the same. As software became more prevalent on IT-based medical devices, the relatively short lifespan of that software has also become a point often overlooked. Non-supported and obsolete software increases cybersecurity risks and threats, adding risks and unknown costs on HDOs as equipment ages.

As the threat landscape changes over time and new threats emerge, the risk and costs of using outdated technology increases and must be accounted for through a shared responsibility between the medical device manufacturer and HDO. However, all technology has an expiration date. Devices using outdated and unsupported components become vulnerable to new exploits.

8.3 Appendix C: Jurisdictional resources for Coordinated Vulnerability Disclosure

Australia
CERT Australia
https://www.cert.gov.au/

AusCERT
https://www.auscert.org.au/

Brazil
All Certs in Brazil
https://www.cert.br/csirts/brazil/

Canada
Canadian Centre for Cyber Security
https://www.cyber.gc.ca/

Europe
CERT European Union
https://cert.europa.eu

France
ANSM
https://ansm.sante.fr/

https://www.ansm.sante.fr/Declarer-un-effet-indesirable/Votre-declaration-concerne-un-dispositif-medical/Votre-declaration-concerne-un-dispositif-medical/(offset)/0

French Ministry of Health and Solidarity
https://solidarites-sante.gouv.fr/soins-et-maladies/signalement-sante-gouv-fr/

Shared Health Information Systems Agency
https://www.cyberveille-sante.gouv.fr/

ANSSI - National Agency for Information Systems Security
https://www.ssi.gouv.fr/en/

Germany
CERT Germany
https://www.cert-bund.de/

Japan
Japan Computer Emergency Response Team (JPCERT)
https://www.jpcert.or.jp/vh/top.html or https://www.jpcert.or.jp/english/

Singapore
SingCERT

https://www.csa.gov.sg/singcert/news/advisories-alerts

United States

Industrial Control Systems CERT (ICS-CERT)
https://www.us-cert.gov/ics

US CERT
https://www.us-cert.gov/