IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: 18 March 2020

Dr Choong May Ling, Mimi, IMDRF Chair

Table of Contents

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.

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 through delays and/or errors in diagnoses and/or treatment interventions, etc.

Stakeholders within the healthcare sector have a shared responsibility regarding medical device cybersecurity. This guidance intends to assist all 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 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 and post-market management of medical device cybersecurity. While the pre-market section primarily addresses medical device manufacturers, the post-market section includes recommendations for all stakeholders.

This is the first IMDRF guidance document to focus exclusively on medical device cybersecurity. However, there are other relevant IMDRF documents which should be noted in terms of general 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 essential principles should be considered along with this guidance document throughout the total product life cycle of a medical device. IMDRF/SaMD WG/N12 FINAL:2014 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 diagnostic (IVD) medical devices). It outlines recommendations for medical device

[1] Section 5.8 of N47 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.

manufacturers, healthcare providers, regulators, and users to: minimize cybersecurity risks that could arise from use of the device for its intended purposes; and to ensure maintenance and continuity of device safety and performance. For the purpose of this guidance, healthcare providers include healthcare delivery organizations.

This document considers cybersecurity in the context of medical devices that either contain software, including firmware and programmable logic controllers (e.g. pacemakers, infusion pumps) or exist as software only (e.g. Software as a Medical device (SaMD)). It is important to note that due to most regulators' authority over medical device safety and performance, the scope of this medical device cybersecurity guidance is limited to consideration of the potential for patient harm. For example, cybersecurity risks that impact performance, negatively affect clinical operations or result in diagnostic or therapeutic errors are considered in scope of this document. While other types of harm such as those associated with breaches of data privacy are important, they are not considered within the scope of this document. Furthermore, this document acknowledges the importance of cybersecurity for the manufacturer's enterprise, however, enterprise cybersecurity is not within the scope of this document. For additional best practices related to security of the manufacturer's enterprise, the NIST Cybersecurity Framework serves as an important resource.

This document is intended to:

- Employ a risk-based approach to the design and development of medical devices with appropriate cybersecurity protections;
- Ensure the safety, performance, and security of medical devices and the connected healthcare infrastructure;
- Recognize that cybersecurity is a shared responsibility among all stakeholders, including but not limited to medical device manufacturers, healthcare providers, users, regulators, and vulnerability finders;
- Provide recommendations to those stakeholders to aid in minimizing the risk of patient harm across the total product life cycle;
- Define terms consistently and describe the current best practices for achieving medical device cybersecurity;
- 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 medical device types and regulatory jurisdictions, may give rise to specific circumstances where additional considerations are required.

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 *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 TIR97:2019)

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).

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

3.9 *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 TIR97:2019)

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

3.10 *Cybersecurity:* a state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle. (ISO 81001-1)

3.11 *End of Life (EOL):* Life cycle stage of a product starting when the manufacturer no longer sells the product beyond their useful life as defined by the manufacturer and the product has gone through a formal EOL process including notification to users.

3.12 *End of Support (EOS):* Life cycle stage of a product starting when the manufacturer terminates all service support activities and service support does not extend beyond this point.

3.13 *Essential Performance*: performance of a clinical function, other than that related to basic safety, where loss or degradation beyond the limits specified by the manufacturer results in an unacceptable risk (IEC 60601-1:2005+AMD1:2012)

3.14 *Exploit:* defined way to breach the security of information systems through vulnerability (ISO/IEC 27039:2015)

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

3.19 *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)

3.20 *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)

3.21 *Threat Modeling:* exploratory process 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 (Adapted from ISO/IEC/IEEE 24765-2017)

3.22 *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: Updates may include patches and configuration changes

NOTE 3: Adaptive and perfective modifications are enhancements to software. These modifications are those that were not in the design specifications for the medical device.

3.23 *Validation:* confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled (ISO 9000:2015)

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

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

3.24 *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.

3.25 *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 guiding principles for medical device cybersecurity, relevant for all stakeholders to consider when developing, regulating, using, and monitoring medical devices. These themes, found throughout this guidance document, are critical to the global improvement of medical device cybersecurity and when followed, are expected to have a positive impact on patient safety.

4.1 Global Harmonization

Medical device cybersecurity is an issue of global concern. Security incidents have the potential to 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.

4.2 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 various phases of the TPLC including but not limited to design, manufacturing, testing, and post-market monitoring activities.

It is recognized that there is a need to balance safety and security. When incorporating

cybersecurity controls and mitigations, it is critical that medical device manufacturers ensure that device safety and essential performance are maintained.

4.3 Shared Responsibility

Medical device cybersecurity is a shared responsibility between stakeholders including the manufacturer, healthcare provider, users, regulator, and vulnerability finder. All stakeholders must understand their responsibilities and work closely with other stakeholders to continuously monitor, assess, mitigate, communicate, and respond to potential cybersecurity risks and threats throughout the life cycle of the medical device.

4.4 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 approach to cybersecurity information sharing. 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, performance, integrity, and security of the medical devices and the connected healthcare infrastructure. These efforts promote transparency. Coordinated vulnerability disclosure is another information sharing mechanism that is encouraged as a best practice. 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.

5.0 Pre-Market Considerations for Medical Device Cybersecurity

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 having a plan in place for post-market activities. For the aforementioned pre-market elements, manufacturers should consider the intended use environment as well as reasonably foreseeable misuse scenarios. 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. Note that the life cycle activities for medical device software are specified in IEC 62304:2006/AMD 1:2015.

5.1 Security Requirements and Architecture Design

Proactively addressing cybersecurity threats at the design stage (e.g. through efforts such as threat modeling) can better mitigate the potential for 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.

Security requirements should also be identified during the requirements capture stage of the life cycle design process. Some security requirements and security risk control measures can be found in 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), and the US Healthcare and Public Health Sector Coordinating Council (HPH SCC) Joint Cyber Security Working Group (JCWG) (e.g. the Joint Security Plan).

While the following Table 1 is not meant to be an exhaustive list, it outlines some design principles that medical device manufacturers should consider in designing their product.

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, USB, etc.
	The manufacturer should consider design features that validate all inputs (not just external) and take into account communication with devices and environments that only support less secure communication (e.g., a device connected to a home network or a legacy device).
	The manufacturer should consider how data transfer to and from the device is secured to prevent unauthorized access, modification, or replay. For example, manufacturers should determine: how the communications between devices/systems will authenticate each other; if encryption is required; how unauthorized replay of previously transmitted commands or data will be prevented; and if terminating communication sessions after a pre-defined time is appropriate.
Data Protection	The manufacturer should consider if safety-related data that is stored on or transferred to/from the device requires some level of protection such as encryption. For example, passwords should be stored as cryptographically secure hashes.
	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.
Device Integrity	The manufacturer should evaluate the system-level architecture to determine if design features are necessary to ensure data non-repudiation (e.g., supporting an audit logging function).
	The manufacturer should consider risks to the integrity of the device such as unauthorized modifications to the device software.

	The manufacturer should consider controls such as anti-malware to prevent viruses, spyware, ransomware, and other forms of malicious code of being executed on the device.
User Authentication	The manufacturer should consider user access controls that validate who can use the device or allows granting of privileges to different user roles or allow users access in an emergency. Additionally, the same credentials should not be shared across devices and customers. Examples of authentication or access authorization include passwords, hardware keys, or biometrics, or a signal of intent that cannot be produced by another device.
Software Maintenance	The manufacturer should establish and communicate a process for implementation and deployment of regular updates.
	The manufacturer should consider how operating system software, third-party software, or open source software will be updated or controlled. The manufacturer should also plan how to respond to software updates or outdated operating environments outside of their control (e.g. medical device software running on an unsecure operating system version).
	The manufacturer should consider how the device will be updated to secure it against newly discovered cybersecurity vulnerabilities. For example, consideration could be given to whether updates will require user intervention or be initiated by the device and how the update can be validated to ensure it has no adverse effect on the safety and performance of the device.
	The manufacturer should consider what connections will be required to conduct updates and the authenticity of the connection or update through the use of code signing or other similar methods.
Physical Access	The manufacturer should consider controls to prevent an unauthorized person from accessing the device. For example, controls could include physical locks or physically restricting access to ports, or not allowing access with a physical cable without requiring authentication.
Reliability and Availability	The manufacturer should consider design features that will allow the device to detect, resist, respond and recover from cybersecurity attacks in order to maintain its essential performance.

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

Secure 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 incorporate these security principles into the development of their software. Doing so necessitates that manufacturers take a holistic approach to device cybersecurity by assessing risks and mitigations throughout the product's life cycle.

5.2 Risk Management Principles for the TPLC

Sound risk management principles addressing the security and safety domains should be incorporated throughout the life cycle of a medical device. 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. Risk management as described in ISO 14971:2019, and cybersecurity risk management (for example, as described in AAMI TIR57:2016; AAMI TIR97:2019) should be used by the manufacturer to take the following steps as part of their risk management process:

- Identify any cybersecurity vulnerability;
- Estimate and evaluate the associated risks;
- Control those risks to an acceptable level;
- Assess and monitor the effectiveness of the risk controls; and
- Communicate risks via coordinated disclosure to key stakeholders.

Figure 1 below shows the security risk management process from AAMI TIR57:2016. This can be a specialized risk management process performed as part of overall risk management, or can be an integral part of the ISO 14971:2019 risk management process with appropriate mapping of vulnerability, threat and other security related terms. See ISO/TR 24971:2020 Annex F for possible mapping.

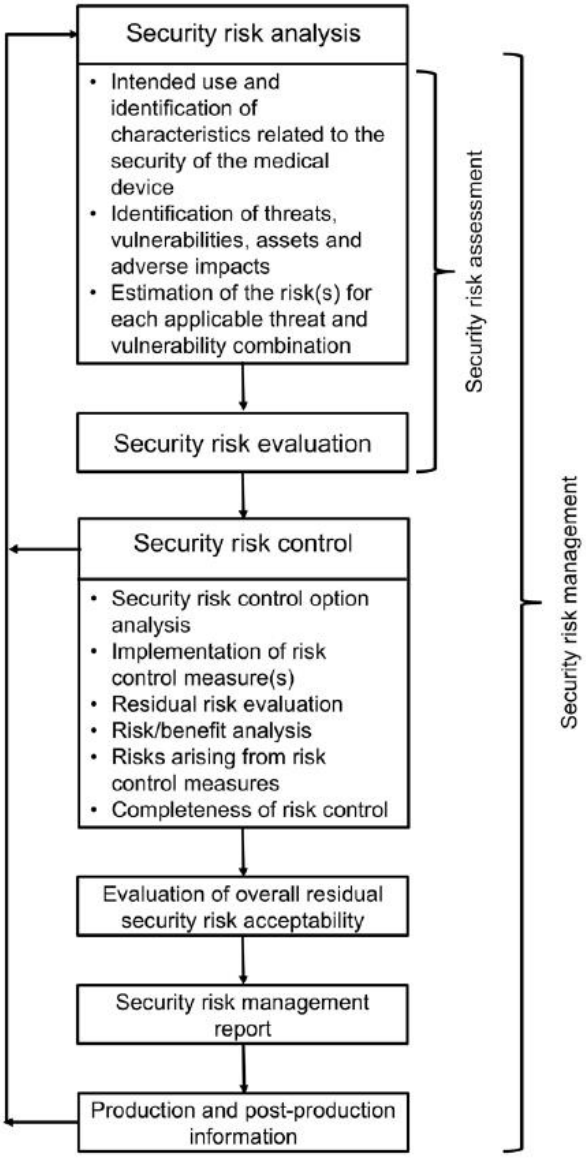

Figure 1: Schematic representation of the security risk management process (with permission from AAMI TIR57:2016.)

With respect to cybersecurity in medical device regulation, 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 link design to threat modeling, patient harm, mitigations, and testing. It is therefore 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.

- **Threat Modeling**: Threat modeling is a process for identifying, enumerating and mitigating risks from potential threats in the device and system. Specifically, threat modeling includes consideration of risks, including but not limited to risks related to the supply chain (e.g., system components), design, production, deployment (e.g., into a hospital environment) and maintenance. Furthermore, creating sufficiently detailed system diagrams aid in the understanding of how cybersecurity design elements are incorporated into a device which further aids in threat modeling. In generating a threat model and per guidance from OWASP, device manufacturers should consider answering four basic questions as it pertains to cybersecurity:

    1. What are we building?
    2. What can go wrong? (e.g. how could it be attacked)
    3. What are we going to do about that?
    4. Did we do a good enough job?

    These questions can be asked in the context of application architecture, operational data flow, or broader system-level threat modeling as appropriate. When determining what can go wrong during threat modeling, manufacturers should consider unintended or malicious misconfiguration of software and hardware (e.g. connecting a device to the Internet that was not designed to do so).

- **Vulnerability scoring**: Vulnerability scoring provides a way to characterize and assess the exploitability and severity of a cybersecurity vulnerability. Known common vulnerabilities and exposures (CVEs) identified in design and development should be analyzed and evaluated using a consistent vulnerability scoring methodology such as the Common Vulnerability Scoring System (CVSS) or any future widely adopted vulnerability scoring system. Cybersecurity risk, vulnerability scoring, and control measures may be used to inform threat modeling and security risk assessments for new products and other risk assessment tools not specific to cybersecurity (e.g. failure mode and effects analysis (FMEA)).

In integrating a security risk management process into an existing ISO 14971:2019 risk management process, activities that address security such as threat modeling and vulnerability scoring should be taken into account.

5.3 Security Testing

At the verification and validation stage in the design and development process, the manufacturer should employ various types of security testing to provide assurance that the code is free of significant known vulnerabilities and that security controls have been effectively implemented. Testing should take into consideration the context of use of the device and its deployment environment. Application of software verification techniques are recommended to ensure that the

software complies with the specifications and anomalies are minimized. 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 also during development. For example, periodic security testing can include: static code analysis, dynamic analysis, robustness testing, vulnerability scanning, or software composition analysis.
- Conduct technical security analyses (e.g. penetration testing). These include efforts to identify unknown vulnerabilities through fuzz testing, for example; 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 TPLC Cybersecurity Management Plan

As cybersecurity threats will continuously evolve, manufacturers should proactively monitor, identify, and address vulnerabilities and exploits as part of their cybersecurity management plan across the total product life cycle. A plan should be in place in the pre-market stage of product development and ideally maintained throughout the manufacturer's organization. This plan should address:

- **TPLC Vigilance**: The proactive monitoring and identification of newly discovered cybersecurity vulnerabilities, assessment of their threat, and appropriate responses.
- **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.
- **Updates and Remediation**: A plan outlining how software will be updated or how other remediation actions would be applied 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 and Customer Security Documentation

5.5.1 Labeling

Labeling communicates to end-users relevant security information, taking into account the relative cybersecurity risk. It should include the following elements:

- Device instructions and product specifications related to recommended cybersecurity controls appropriate for the intended use environment (e.g., anti-malware software, network connectivity configuration, use of a firewall).
- A description of backup and restore features and procedures to regain configurations.
- 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.

5.5.2 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 safe and secure use by the user. It should include the following elements:

- Specific guidance to users regarding the supporting infrastructure requirements so that the device can operate as intended.
- A description of how the device is - or can be hardened - using a 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, etc.
- 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, security risks and consequences of changes to the security configuration, or to the 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 6.6, Legacy Medical Devices).
- A Software Bill of Materials (SBOM) to inform and support operators regarding the cybersecurity of commercial, open source, or off-the-shelf software components which are included in the medical device. An SBOM creates the necessary transparency via a list identifying each software component by its name, origin, version and build. SBOMs enable device operators (including patients and healthcare providers) to effectively manage their assets and related risks, 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 essential performance. Device operators can use the SBOM to facilitate work with the device manufacturer in identifying software that may have vulnerabilities, update requirements, and performing appropriate security risk management. The SBOM also helps inform purchasing decisions by providing prospective buyers with visibility into the components used in applications and determining potential security risk. Manufacturers

should leverage industry best practices for the format, syntax and markup used for deployment of the SBOM. Since the SBOM reveals sensitive information about the medical device, its distribution is encouraged through trusted communication channels. It is recognized that manufacturers will determine trusted ways for communicating SBOMs to the operator.

5.6 Documentation for Regulatory Submission

In addition to the activities outlined in the preceding sections, medical device manufacturers should 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. If required for premarket authorization, clear documentation describing the device's design features, risk management activities, testing, labeling and evidence of a plan to monitor and respond to emerging threats throughout the product's life cycle in relation to cybersecurity, should be submitted by the manufacturer. The following paragraphs provide further details on each of the above items.

5.6.1 Design Documentation

Documentation that describes the device including any interfaces or communication pathways or components (hardware and software), and all design features that were included to mitigate cybersecurity risks relating to patient harm such as those previously outlined in Section 5.1 above (in particular the rationale and assumptions leading to the selection of the measures for 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 and use a cybersecurity risk management standard (e.g. AAMI TIR57:2016, AAMI TIR97:2019) for guidance. The outcomes should be aligned with the overall requirements of ISO 14971:2019, to ensure that output can be used as input for the overall risk management. Risk management documents related to cybersecurity can include:

- Comprehensive risk management documentation, such as a risk management report or security risk management report which should include any threat modeling, and identified cybersecurity threats.
- Discussion on any impact of security risk mitigations on the management of other risks.

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 security 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 and internal SOPs/documentation used.

5.6.4 TPLC Cybersecurity Management Planning Documentation

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: TPLC vigilance, planned or corrective updates, coordinated vulnerability disclosure policies, and information sharing.

5.6.5 Labelling and Customer Security Documentation

All 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 covers various elements and includes: 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

Medical device cybersecurity 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, performance, and cybersecurity aspects of medical devices that are connected to their IT infrastructure. The process should be applied at the:

- Initial development of the IT infrastructure;
- Integration of a new medical device into existing IT network; and
- 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. The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients documents may also serve as another resource.

In addition to adopting a risk management system, healthcare providers should also adhere to the following general cybersecurity best practices (which are not meant to be an exhaustive list) 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;
- Employ configuration management to identify all current assets and track future configuration changes;
- Apply the configuration and protection measures as recommended by the manufacturer;
- Network access control to limit medical device communication;
- Update management practices that ensure timely security updates;
- Malware protection to prevent attacks; and
- 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 some of these best practices may not be feasible in a medical emergency. Many of the practices above are described in the NIST Cybersecurity Framework.

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 basic cybersecurity training to create security awareness and introduce cyber hygiene practices among all users (e.g. doctors, nurses, biomedical engineers, technicians, etc.). This will include training on operating the medical devices in a secure manner (e.g. only connect their devices to secured network) and how to spot and report any anomalous device behavior (e.g. random shutdowns/ restarts, security software disabled). Such 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.

6.1.2 Medical Device Manufacturers

In addition to the information contained in the product labeling and customer security documentation, manufacturers are encouraged to partner with healthcare providers, distributors, 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 adopt proven tools from other sectors to strengthen the security of the medical device ecosystem globally.

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 principles that should be followed regarding information sharing. Examples are not intended to specify requirements, but rather to serve as illustrations.

6.2.1 Key Principles

- 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 (e.g. users, patients, other manufacturers, distributors, healthcare providers, security researchers, and the public).
- The information shared should be balanced such that it is meaningful, consumable and actionable for different stakeholders (e.g. information about a more secure chipset could be important across manufacturers, but the information may provide no benefit to end-users of the device).
- Information should be shared freely and in good faith as appropriate, with the aim of improving patient safety irrespective of commercial interests.
- Ensure as much as possible, globally consistent information that is shared synchronously across jurisdictions (as appropriate) to enable stakeholders in various jurisdictions to respond accordingly.

6.2.2 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.

a. Regulators

- Are key receivers of information related to the security of medical devices, and are often involved in information dissemination.
- Should aim to build processes that encourage timely disclosure of information relating to the cybersecurity of medical devices. This includes sharing information amongst regulators to facilitate a globally coordinated response.

b. Medical Device Manufacturers

- Should identify, assess, and share vulnerability information irrespective of where this information comes from. Manufacturers are encouraged to share any information that will help the regulator manage expectations and facilitate regulatory requirements.

- Should aim to synchronize notification of all the regulators where the affected product is distributed to ensure globally consistent information and, if appropriate, a globally aligned response.
- Should use plain language, at an appropriate reading level for the intended user, to communicate actionable information regarding medical device cybersecurity vulnerabilities and threats. This may need to include information about the clinical benefits and risks associated with deploying an update, or compensating controls required until the update is available.

c. Healthcare Providers

- Are often 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.
- Are also key generators of information because they work with medical devices in the field and can provide feedback regarding which devices have been affected as well as ease/efficacy of implementing the remediation or mitigation in a real-world setting.

d. Users (e.g. clinicians, patients, caregivers, and consumers)

- Are often the ones making the final choice on whether an update or other correction is actioned. Therefore, they need clear and meaningful information so that they can make an informed decision.

e. Other stakeholders, including governments and information sharing entities

- Law enforcement, national security, and other government agencies may need to share medical device cybersecurity threat and vulnerability information across various parts of government to protect healthcare and other critical infrastructure.
- 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. Computer Emergency Response Teams (CERTs)), and others. These stakeholders likely differ between jurisdictions and markets.

6.2.3 Types of Information

Cybersecurity vulnerabilities can pose threats to multiple product components, including software and hardware, and first-party or third-party components. In order to protect patients from harm, information shared might include, but is not limited to:

- Information about products that are affected by a vulnerability and how they are affected;
- 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 attacks, and availability of exploit code;
- Confirmation of incidents (e.g., “Are you seeing this too?”);

- Availability of patches and other security mitigations such as compensating controls; and
- Additional instructions on the use and integration of medical devices as an interim measure

Information sharing should also include 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.

6.2.4 Trusted Communication

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. One way to encourage information sharing is to offer anonymized sharing.

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.

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. As a best practice, CVD should be undertaken as a norm rather than as an exception and medical device stakeholders are encouraged to ask manufacturers about their CVD policies to further catalyze adoption.

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 Teams (CSIRT) or government regulators are authoritative sources of information regarding vulnerabilities. There may be jurisdictional differences regarding if, how, and when the regulator communicates as a part of

CVD. However, 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.

No software-enabled 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. Therefore, 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 finder 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 14971:2019) 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 when required 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.

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 since CVD is recognized as a best practice.

6.3.3 Vulnerability Finders (includes security researchers and others)

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 finder of the vulnerability throughout its assessment and remediation. Finally, the vulnerability finder 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 finder and there is no evidence of an attack using the vulnerability in the wild, coordinated disclosure means that the finder of the vulnerability does not disclose it until a fix or other mitigation is available. If the finder discloses the vulnerability ahead of a fix, then the finder 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 outlined in ISO 14971:2019 is a well-established and mature practice in the medical device sector. This practice should be applied to evaluating the cybersecurity risk of a vulnerability, and then to determine patient safety impact by manufacturers and regulators alike by establishing a cybersecurity risk management process linked to risk management. 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 as is appropriate. 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 commensurate with 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 their software and hardware components. 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.

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 an 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, clear and concise communication to those that need information to manage risk is vital. Moreover, there should be some awareness of the level of technical expertise of those managing risk. 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); vulnerability score such as a CVSS score; exploitability index (e.g., low skill level) and method (e.g., remote) 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/patient safety, 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 principles of safety and essential performance;
- Information sharing with stakeholders to reduce the risk to patients and users;
- Cooperation of stakeholders to achieve the agreed remediation; and
- Timely remediation, relative to the risk.

When the device lacks sufficient fundamental or inherent protective measures, and updates are not feasible, risk-mitigating alternatives should be applied as compensating controls. Examples may include installing a firewall 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 updating 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. Updates

Patients receive medical care in professional healthcare facilities and in the home healthcare environment, and each use environment is associated with unique considerations for updating.[2] In the home healthcare environment, for example, the user can be the patient, caregiver, trusted

[2] 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."

neighbor, or a family member. This section provides general guidance for updating and subsequent sections describe specific considerations for each use environment.

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 updates 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.

When an update 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.[3]

Table 2 is adapted from patching methods documented in the Joint Security Plan.[4] The rightmost column of the table describes the primary responsibility of the user identified to implement a medical device manufacturer-approved update.

Update method	Summary description	User responsibility
Remote update	Updates 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	Approved updates 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 update in accordance with instructions provided by the manufacturer.
Service visit	Local service facility administers cybersecurity updates (includes on-site servicing). Note, this method is applicable in cases where faulty updating 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: Update methods and user responsibility for implementation

[3] It is acknowledged that in certain situations, the user cannot appropriately assess risks.
[4] *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).

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

b. Considerations for the healthcare facility environment

In 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 healthcare providers, 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. Updating 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 updates for medical devices that are connected to medical-IT networks.

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 updating methods for the home healthcare environment is a function of many factors including medical device risk 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" update method listed in Table 1. Update 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 update 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 or the medical device manufacturer to understand software maintenance options for their device.

6.4.3 Regulators

Post-market Updates

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 intended 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 performance 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 intended 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 and is used to determine whether residual risk is acceptable or unacceptable. Note, the definition of "patient harm" is a subset of "harm" as defined in ISO 14971:2019, Medical devices — Application of risk management to medical devices.[5] The narrow definition of patient harm has the net effect of prioritizing regulatory review of those changes necessary to protect public health.

[5] ISO 14971:2019 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.

Table 3 presents a recommended framework for regulators to consider when considering the regulatory oversight required for the various types of software maintenance activities. It is acknowledged that the levels presented in this table are not prescriptive, but provide a guide to the recommended relative levels of regulatory oversight.

Purpose of Update		**Proposed 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 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 strategy for vulnerabilities that cannot be remediated	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. [6]
	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 vulnerability finder 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

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

			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. [7]

Table 3: Software updates 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 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 62304:2006/AMD 1:2015.

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 which can be scalable and build an incident response team based on its product portfolio. The aim of an incident response team is to provide appropriate capacity for assessing, responding to and learning from cybersecurity incidents, 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 A for item description).

a. Roles and Responsibilities

The incident response team can be divided into the following groups: manager, planning, monitoring, responding, implementation, analysing, and sometimes external experts. Each group has different roles and responsibilities. The team should assign members to these groups based on

[7] Ibid.

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 those groups is provided in Appendix A.

b. Communication Expectations

Customers should be provided contact information of the medical device manufacturer to report cybersecurity incidents and events, or otherwise submit through regular customer support channels. The incident response team should 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 manufacturer 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. CERTs and ISAOs 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 the planning and the resource management 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 handling 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. Manufacturer Disclosure Statement for Medical Device Security (MDS2), SBOM, vulnerability/update information), and information sharing institutions or participating 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 fulfil, during or in response to an incident. Healthcare providers are encouraged to establish their own Security Incident Response Team.

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 evaluate the impact of any incidents or reported vulnerabilities and cooperate with stakeholders including the medical device manufacturer by providing information describing the result of any 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 including regression testing 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 should also be engaged in medical device cybersecurity incident 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

For purposes of this IMDRF guidance, medical devices that cannot be reasonably protected (via updates, and/or compensating controls) against current cybersecurity threats are considered legacy devices. The legacy condition represents an especially complex challenge for the present state of the healthcare ecosystem globally since device cybersecurity may not have been considered in the initial device design and maintenance for many devices in use today. Today's challenge is further exacerbated by the fact that the clinical utility of a device often outlasts its security supportability as the shift to digital technology within medical devices has offered expanded functionality that could never be realized within older analog devices. While beneficial to patient care, the combination of software, hardware, and network connectivity in these technologies puts new demands on the device lifetime, which often consists of capital equipment (e.g. scanner hardware) as well as commodity components (e.g. servers, workstations, databases and operating systems). It is important to note, however, that device age is not a sole determinant of legacy status. In other words, a device that cannot be reasonably protected against current cybersecurity threats may be less than five years old; irrespective of its age, this device would still be considered legacy. On the other hand, a device may be 15 years old, but if it maintains the capability of being reasonably protected against current cybersecurity threats, it would not be considered legacy.

As efforts to address the TPLC of medical device cybersecurity starting from the earliest device design and development stage continue to advance, availability of devices that maintain the capability of reasonable protection against cybersecurity threats through its use lifetime will

become more and more the norm, and the imbalance observed with respect to the multitude of legacy devices in current clinical use - - posing a security threat to healthcare providers and their networks - - will lessen. The following subsections of this IMDRF guidance articulate a conceptual framework driving towards an optimal future state of medical device cybersecurity where legacy devices (those that cannot be reasonably protected against current cybersecurity threats) are decommissioned/phased out of use, with appropriate advanced notification to healthcare providers to enable business continuity planning. (See Figure 2).

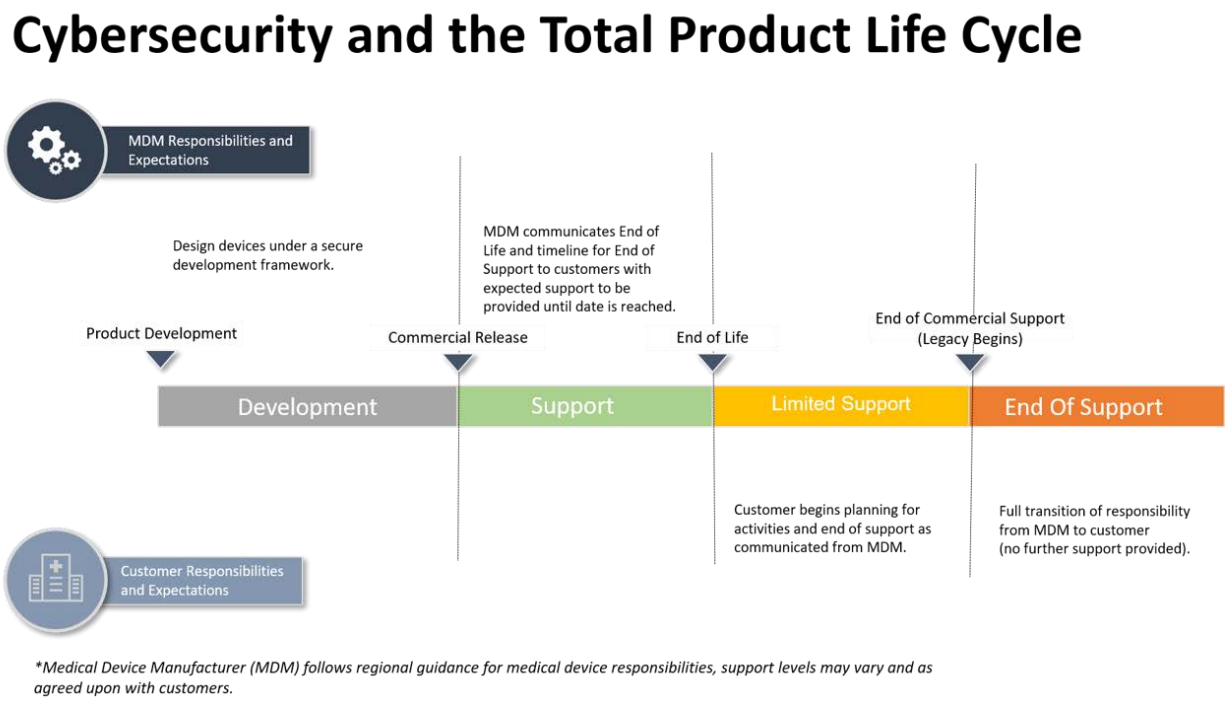

Figure 2: Legacy device conceptual framework as a function of product life cycle for cybersecurity

6.6.1 Medical Device Manufacturers

Attention to medical device cybersecurity begins during device design and development, well before commercial release, as depicted in Figure 2. Aligning with the TPLC framework, full support of medical devices to ensure reasonable protection against current cybersecurity threats should continue through the manufacturer's published cybersecurity End of Life date (EOL). The manufacturer's cybersecurity EOL date signifies the diminished capacity to provide comprehensive cybersecurity support of the medical device. Upon approaching the cybersecurity EOL, the manufacturer should release a communication to its customers notifying them of the limited support that remains available beyond the EOL, with clear communication of the device's cybersecurity End of Support (EOS) date. No support should be expected for any medical device past the established cybersecurity EOS date.

Per this conceptual framework, when a medical device reaches its cybersecurity EOS date, it is considered a legacy medical device that cannot be reasonably protected against current cybersecurity threats and should be decommissioned. The responsibility for maintaining device

security and assumption of risk for its ongoing use beyond the EOS date would transfer at this point to the customer, e.g., the healthcare provider.

It is important to note that while design changes to some devices may not be feasible (e.g. an obsolete operating system that is no longer supported and cannot be patched for security purposes), compensating controls may be able to provide some level of protection. In the presence of available and successfully deployed compensating controls, the medical device would not be considered legacy per this framework. As appropriate, regulators may encourage medical device manufacturers to leverage compensating controls to address present day device security challenges after EOL date, to enable ample time for healthcare providers to conduct business continuity planning for EOS when no further security support is available from the manufacturer. Device design, vulnerability management, and customer communications all play an important role in addressing device cybersecurity challenges. Recommendations for manufacturers as a function of device life cycle stage include the following:

- Development:

    a. 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 that address quality, performance and security concerns. A manufacturer should anticipate the need to support safety and efficacy of a product throughout its use. The manufacturer should consider that the third-party vendor support for a component may end within the healthcare provider's projected use life of the device, and this may adversely impact the manufacturer's ability to support secure operation of the device.
    b. Design and develop devices under a secure development framework to minimize the number of legacy devices in the future. These devices, at a minimum, should meet a security baseline and include mechanisms for updates and patches.

- Support:

    a. Monitor medical devices for vulnerabilities with unacceptable risk 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.
    b. Clearly communicate key life cycle milestones, including cybersecurity EOL dates of devices as part of procurement and installation processes - customer responsibilities should be integrated into communications at these time points.
    c. Notify customers proactively of third-party vendor end of support for device components.
    d. Release a customer notification that signals ongoing but limited support through the cybersecurity EOS date, beyond which the device would be considered unsupportable and in a legacy state. The timing of this customer communication should occur upon approaching the EOL date and will enable advanced notice for device decommissioning/phase out and business continuity planning for healthcare providers. Clearly communicating helps healthcare organizations understand their responsibilities as well as device risk so that they can plan device retirement and replacement and budget accordingly.

- Limited Support (EOL begins here):
  a. Continue to communicate timelines for cybersecurity EOS dates to allow ample time for customers to prepare for EOS and the associated customer responsibilities.
  b. Continue actions "a" and "c" from the Support life cycle phase above.

- End of Support (Legacy begins here):
  a. Full transfer of responsibility from manufacturer to customer. Following formal cybersecurity EOS for the device, users of devices should not expect any level of support.

6.6.2 Healthcare Providers

Many healthcare providers plan for device use much longer than the communicated life of the device given by the manufacturer in its published cybersecurity EOL. 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, as a function of device life cycle stage, are expected to help address healthcare providers' challenges with medical devices, to plan in advance for a defined cybersecurity EOS date:

- Support:

  a. Request clear points of contact and communication processes with device manufacturers to ensure product life cycle planning, understanding, and transparency.
  b. Request an SBOM, as software components with the shortest support life cycle will ultimately affect the supportability and security of those devices. Obtaining an SBOM helps customers better understand those components affecting the device life cycle and can include information for additional hardware for risk control measures such as compensating controls.
  c. Ensure 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. This includes proper support of network security, asset security, identity and access management, and security operations.
  d. Evaluate new and evolving 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.
  e. Plan ahead for the manufacturer's cybersecurity EOS date, so that an unsupported legacy device (potentially jeopardizing patient safety and healthcare network security), can be appropriately phased out and replaced with a securable and supported medical device.

- Limited Support:

  a. Continue actions "c", "d", and "e" under the Support device life cycle phase above

- End of Support:

a. Accept responsibility for management of device security and assumption of security risk for its ongoing use beyond the cybersecurity EOS date if unable to decommission the device without impacting continuity of care.

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 Standards

3. AAMI TIR57:2016 Principles for medical device security—Risk management

4. AAMI TIR 97:2019, Principles for medical device security—Postmarket risk management for device manufacturers

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

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

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

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

9. 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

10. 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

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

12. ISO 14971:2019, Medical devices – Application of risk management to medical devices

13. 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

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

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

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

17. ISO/IEC 29147:2018, Information Technology – Security Techniques – Vulnerability Disclosure

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

19. ISO/TR 24971:2020, Medical devices – Guidance on the application of ISO 14971

20. UL 2900-1:2017, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements

21. UL 2900-2-1:2017, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems

7.3 Regulatory Guidance

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

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

24. 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)

25. 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)

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

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

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

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

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

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

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

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

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

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

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

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

7.4 Other Resources and References

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

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

40. NIST's Secure Software Development Framework (SSDF)
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

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

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

43. MITRE CVSS Healthcare Rubric

https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

44. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

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

46. Manufacturer Disclosure Statement for Medical Device Security (MDS^2) https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

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

48. 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

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

50. 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 updates; 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: 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/

Italy
https://www.csirt-ita.it/

Japan
Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC)
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/