IMDRF International Medical Device Regulators Forum

Final Document

IMDRF/CYBER WG/N70FINAL:2023

Principles and Practices for the Cybersecurity of Legacy Medical Devices

AUTHORING GROUP

Medical Device Cybersecurity Working Group

Preface

© Copyright 2023 by the International Medical Device Regulators Forum.

This work is copyright. Subject to these Terms and Conditions, you may download, display, print, translate, modify and reproduce the whole or part of this work for your own personal use, for research, for educational purposes or, if you are part of an organisation, for internal use within your organisation, but only if you or your organisation do not use the reproduction for any commercial purpose and retain all disclaimer notices as part of that reproduction. If you use any part of this work, you must include the following acknowledgement (delete inapplicable):

"[Translated or adapted] from [insert name of publication], [year of publication], International Medical Device Regulators Forum, used with the permission of the International Medical Device Regulators Forum. The International Medical Device Regulators Forum is not responsible for the content or accuracy of this [adaption/translation]."

All other rights are reserved, and you are not allowed to reproduce the whole or any part of this work in any way (electronic or otherwise) without first being given specific written permission from IMDRF to do so. Requests and inquiries concerning reproduction and rights are to be sent to the IMDRF Secretariat.

Incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the IMDRF.

Andrzej Rys, IMDRF Chair

Contents

1. Introduction

Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60 FINAL:2020, hereinafter also referred to as “IMDRF N60 guidance”) set forth foundational security principles and best practices that span the total product life cycle (TPLC) of medical devices. Global adoption of the guidance is predicated on successful and consistent implementation of the recommendations contained within it. Focused attention on some specific challenges in the guidance is important for such implementation and is a natural progression towards further advancing the resilience of medical device cybersecurity throughout the TPLC.

While modern medical device designs benefit from improved cybersecurity considerations, there are many devices in use today—some even beyond the time point of a manufacturers’ intended useful life of the device — that were not designed with these same considerations. Those devices may present risks to the patients that cannot be sufficiently mitigated (e.g., patched or otherwise updated) to address cybersecurity threats, as current best practices recommend. They may contain insufficient or no security controls, or they may have contained state-of-the-art security controls at the time they were deployed, but—because of the long lifetimes of healthcare technologies—are now faced with unanticipated threats against which they cannot defend. Such devices, often termed “legacy medical devices”, often require different means to maintain cybersecurity throughout the TPLC. It is important to note, however, that device age is not a sole determinant of whether a device is legacy. In other words, a newer device that cannot be reasonably protected against current cybersecurity threats, irrespective of its age, would still be considered legacy in the context of cybersecurity. In organizations lacking the staff and resources to adequately execute TPLC plans, which is not uncommon, these legacy devices and their associated risks can persist indefinitely.

Because legacy medical devices are still used to provide healthcare today, they could create significant threats to patient safety. In this context, the intention of this guidance document is to operationalize the legacy device conceptual framework articulated in the IMDRF N60 guidance, including the detailed recommendations provided to stakeholders such as medical device manufacturers (MDMs) and healthcare providers (HCPs). For the purpose of this guidance, HCPs include healthcare delivery organizations.

This guidance document is intended to provide stakeholders with clear ways of identifying potential legacy devices and practical, feasible approaches to maintain cybersecurity of legacy medical devices. It is intended to provide stakeholders with a variety of options to implement without distorting each jurisdiction’s regulatory systems and this work is intended to be complementary to the IMDRF N60 guidance.

For additional recommendations related to legacy cybersecurity risk management, see the US Health Sector Coordinating Council (HSCC) Health Industry Cybersecurity – Managing Legacy Technology Security (HIC-MaLTS).

2. Scope

This document is designed to provide concrete recommendations on how to apply the TPLC to legacy devices to aid in the implementation of the framework put forward in the preceding IMDRF N60 guidance. This document is complementary to the IMDRF N60 guidance, and the scope of relevant medical devices (including in vitro diagnostic (IVD) medical devices), as well as the focus on potential for patient harm remain unchanged.

It considers cybersecurity in the context of legacy 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 guidance is limited to consideration of the potential for patient harm. For example, threats that could 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.

Legacy devices were previously defined in IMDRF N60 guidance as medical devices that cannot be reasonably protected against current cybersecurity threats. This document therefore only addresses legacy devices within the context of cybersecurity, and not all other situations in which a device may be considered "legacy" (e.g., an older model of a medical device).

Given the above definition of legacy, many devices currently in use would be considered legacy devices. To transition from this current state into a more ideal future state, the IMDRF N60 guidance proposed a TPLC Framework for legacy devices, which is further elaborated in this document. A key characteristic of this framework is effective communication between MDMs and HCPs to allow for timely and planned introduction and decommission of devices to minimize the number of legacy devices remaining in use. While beyond the scope of this guidance, MDMs and HCPs should communicate life cycle stage information to patients where relevant. Resellers (e.g., re-labellers) are also outside the scope of this guidance as they often do not have the same regulatory obligations as MDMs.

Specifically, this document is intended to:

- Explain legacy medical device cybersecurity within the context of the TPLC Framework (Development, Support, Limited Support, and End of Support) with clearly defined responsibilities for MDMs and HCPs at each stage;
- Provide recommendations for MDMs and HCPs in communication (including vulnerability management), risk management, and transfer of responsibility to the HCP;
- Provide recommendations regarding compensating controls after End of Support;
- Provide implementation considerations for MDMs and HCPs in addressing existing legacy devices that were developed prior to the TPLC Framework for medical device cybersecurity and are still in use.

As was emphasized in the preceding IMDRF N60 guidance, this document continues to recognize that cybersecurity is a shared responsibility among all stakeholders, including, but not limited to, MDMs and distributors, HCPs, users, regulators, and software vendors.

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. Definitions

For the purposes of this document, the terms and definitions given in IMDRF/GRRP WG/N47 FINAL:2018, as well as IMDRF/CYBER WG/N60FINAL:2020, and the following apply.

3.1 *Application software*: 1. software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself 2. software or a program that is specific to the solution of an application problem *[ISO/IEC 2382:2015).*

3.2 *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).

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

3.4 *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).

3.5 *Component:* collection of system resources that (a) forms a physical or logical part of the system, (b) has specified functions and interfaces, and (c) is treated (e.g., by policies or specifications) as existing independently of other parts of the system. (ISO 81001-1:2021).

NOTE: In the medical device context, components include any raw material, substance, piece, part, software, firmware, labelling, or assembly that is intended to be included as part of the finished, packaged, and labelled device.

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

3.7 *Configuration*: manner in which the hardware and software of an information processing system are organized and interconnected (ISO/IEC 2382:2015).

3.8 *Configuration management*: coordinated activities to direct and control the configuration (ISO/IEC TR 18018:2010).

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 *Decommission:* to remove from active service (ASTM E3173-18).

3.12 *Deployment*: phase of a project in which a system is put into operation and cutover issues are resolved (ISO/IEC/IEEE 24765:2010).

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

NOTE: End of Life time point triggers Limited Support stage of the TPLC.

3.14 *End of Support (EOS):* Point in time in the life cycle of a product starting when the manufacturer terminates all service support activities and service support does not extend beyond this point.

NOTE: End of Support time point triggers End of Support stage of the TPLC.

3.15 *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).

NOTE: Maintenance, repairs, or upgrades (e.g., safety or cybersecurity modifications) can be necessary to maintain the essential performance.

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

3.17 *Firmware*: ordered set of instructions and associated data stored in a way that is functionally independent of main storage, usually in a read only memory (ROM) (ISO/IEC 2382:2015).

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

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

3.20 *Life cycle:* series of all phases in the life of a product or system, from the initial conception to final decommissioning and disposal. (ISO 81001-1:2021).

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

3.22 *Patient Safety*: freedom from unacceptable risk to the health of patients (Modified from ISO/IEC Guide 51:2014).

3.23 *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).

3.24 *Product:* output of an organization that can be produced without any transaction taking place between the organization and the customer. (ISO 81001-1:2021).

3.25 *Resilience*: ability of a functional unit to continue to perform a required function in the presence of faults or errors (ISO/IEC 2382:2015).

3.26 *Risk management:* systematic application of management policies, procedures and practices to the tasks of analysing, evaluating, controlling and monitoring risk. (ISO/IEC Guide 63:2019).

3.27 *Risk transfer*: transferring responsibility for managing a risk factor to another organization or functional entity better able to mitigate the risk factor (ISO/IEC/IEEE 24765:2017).

3.28 *Security policy*: 1. rules for need-to-know and access-to-information at each project organization level 2. set of rules that constrains one or more sets of activities of one or more sets of objects (ISO/IEC 10746-3:2009).

3.29 *Security testing*: type of testing conducted to evaluate the degree to which a test item, and associated data and information, are protected so that unauthorized persons or systems cannot use, read, or modify them, and authorized persons or systems are not denied access to them (ISO/IEC/IEEE 29119-1:2013).

3.30 *Software Bill of Materials (SBOM)*: list of one or more identified components, their relationships, and other associated information.

NOTE: The SBOM for a single component with no dependencies is just the list of that one component. “Software” can be interpreted as “software system,” thus hardware (true hardware, not firmware) and very low-level software (like CPU microcode) can be included. (NTIA Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) 2021-10-21).

3.31 *Software component*: general term used to refer to a software system or an element, such as module, unit, data, or document. (IEEE 1061)

NOTE: A software component may have multiple units or have multiple lower-level software components.

3.32 *Third-party software*: software provided by a person or body that is recognized as being independent of the parties involved. (Modified from ISO/IEC 25051:2014)

NOTE: Parties involved are usually supplier ("first-party") and purchaser ("second-party") interests.

3.33 *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).

3.34 *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).

3.35 *Total Product Life Cycle (TPLC)*: Development, Support, Limited Support, and End of Support Stages in the life of a medical device.

NOTE: Some jurisdictions may refer to the stages with different terms.

3.36 *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.

3.37 *Upgrade*: replacement of device or device components with a newer or better version, or with additional features.

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

3.39 *Vulnerability management*: cyclical practice of identifying, classifying, prioritizing, remediating, and mitigating software vulnerabilities.

4. General Principles

This section provides general principles for legacy devices for all stakeholders to consider when developing, regulating, using, and monitoring medical devices. These general principles, found throughout this guidance document, are foundational to the improvement of the cybersecurity posture of health systems around the world that include legacy devices.

4.1. Total Product Life Cycle Framework

Risks associated with cybersecurity threats and vulnerabilities should be considered throughout all stages in the life of a medical device, from Development to EOS. It is known that, in practice, clinical life may extend beyond EOS, where decommissioning could occur sometime after EOS if an HCP decides to continue using the device beyond EOS. It is known that in many cases, the clinical utility of a device exceeds its supportability. It should be acknowledged by all stakeholders that, a medical device should have a planned life cycle for cybersecurity that includes the TPLC stages of Development, Support, Limited Support, and End of Support (EOS).

Limited support is a transitional period for the MDM and HCP to coordinate and prepare for eventual transition to End of Support or product upgrade/replacement. EOS is considered the time point where the responsibility for cybersecurity of a medical device is primarily transferred to the HCP. After EOS, the MDM may still be responsible for certain post-market activities dependent upon jurisdictional regulations (see Section 7.2.1.3 for additional details). There will be numerous activities related to communications, risk management and transfer of responsibility that occur over time in lead up to the medical device EOS to ensure that MDMs and HCPs can adequately prepare for each life cycle stage.

4.2. Communication

Effective protection against threats requires open and transparent communication between stakeholders. MDMs are expected to plan for EOL and EOS. MDMs should strive to communicate when to expect EOL and EOS as soon as possible, even as a part of device procurement and installation. Early awareness enables users to appropriately plan for EOL and EOS dates by obtaining information from the MDM to inform next steps regarding device maintenance. Using this information, the HCP would either decommission the device or assume additional responsibility for maintaining its security.

Throughout this document, recommendations related to communications either from the MDM or the HCP should be understood to involve active outreach and/or engagement between these parties or other stakeholders. Information that is provided or communicated should be proactively sent to the other party, or the other party should be actively made aware that such information is available for retrieval. Communication policies and procedures that make information passively available, without active notification, are not recommended and should be avoided where possible.

4.3. Shared Risk Management

Medical device cybersecurity is a shared responsibility between stakeholders, notably between MDMs and HCPs. This shared responsibility is particularly important when it comes to legacy devices.

To appropriately manage risk for legacy devices, MDMs should design their devices in a way that optimizes cybersecurity in the Support Stage and minimizes security risk after EOS in the future. MDMs should support devices as described by this document in sections 7, 8, and 9. HCPs should actively engage with MDMs to obtain an SBOM, ensure that the device operates with appropriate cybersecurity safeguards as recommended by the MDM (including associated IT infrastructure), ensure that those cybersecurity safeguards are maintained, and plan for the device's EOS date. Devices that no longer have any support by the MDM are likely to become vulnerable to current and future threats, and HCPs should consider upgrading those devices with models supported by the MDM. For additional information regarding the SBOM, see IMDRF/CYBER WG/N73.

5. Overview of IMDRF TPLC Framework for Medical Device Cybersecurity

To effectively manage the dynamic nature of cybersecurity risk, risk management should be applied throughout the TPLC where cybersecurity risk is evaluated and mitigated in various parts 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 MDMs ensure that device safety and essential performance are maintained.

The IMDRF N60 guidance explains legacy medical device cybersecurity with the context of four (4) TPLC stages: Development, Support, Limited Support, and EOS (Figure 1). Some jurisdictions may refer to the stages with different terms. However, the concepts described in each stage should be generally applicable. Also, please note that the TPLC stages may occur for different time durations (e.g., the Support Stage may be longer than the Limited Support Stage).

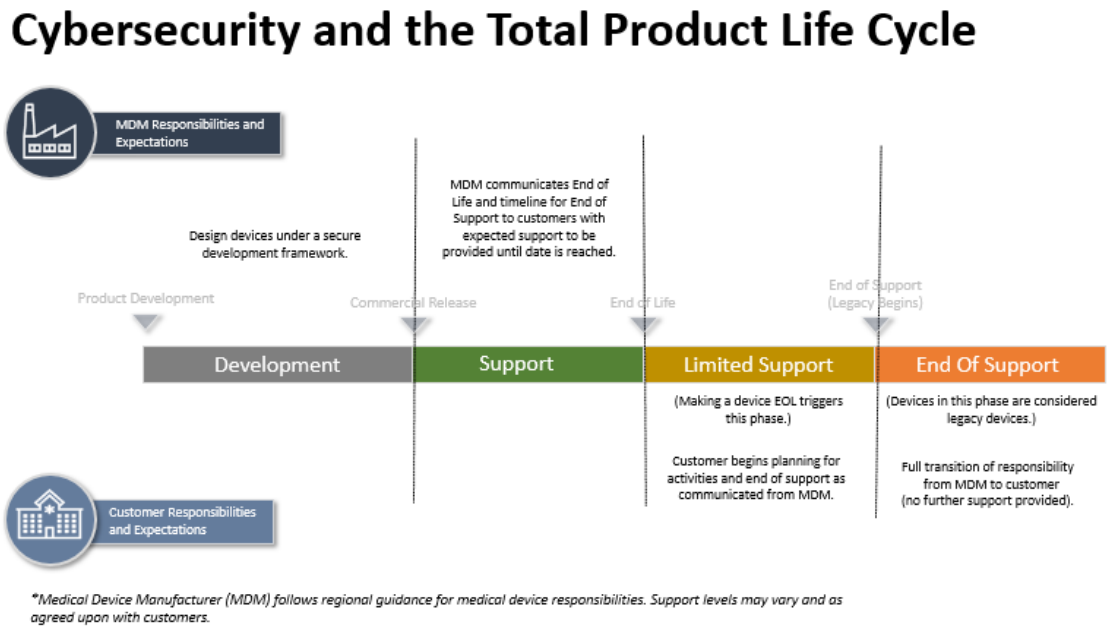

Figure 1: High-level legacy device conceptual framework as a function of total product life cycle for cybersecurity

Note on Figure 1: In addition, the term “customer” should be understood to mean “HCP” in the context of this paper.

5.1. Development (Stage 1)

The Development Stage (stage 1) is a pre-market stage where MDMs are expected to incorporate security by design. MDMs should perform risk assessments, identify threats, execute security testing, and mitigate risks to ensure devices can operate safely and effectively throughout their life cycle. Another outcome of the Development Stage is a set of product-related security documentation that supports users in securely operating devices. Product development best practices are outside the scope of this document. References to established standards include, but may not be limited to:

- (IEC 62443-4-1 (Product Life Cycle)
- IEC 62443-3-2 (Security Risk Assessment)
- NIST 800-12
- NIST Secure Software Development Framework
- IEC 81001-5-1: 2021
- IEC TR 60601-4-5: 2021
- IEC TR 80001-2-8:2016
- IEC 62443-4-2:2019

For additional standards, see also IMDRF/CYBER WG/N60 guidance.

5.2. Support (Stage 2)

Devices in the Support stage (stage 2) are defined as medical devices that:

1. Are used for providing patient care, and
2. Are available on the market, and
3. Contain major software, firmware, or programmable hardware components (e.g., CPU) which are all supported by their suppliers[1].

Stage 2 devices should receive full cybersecurity support such as software patches, software and hardware updates, and support as deemed appropriate.

While devices in this category may be considered by the market as “new” or “state of the art”, they can exhibit a wide range of security capabilities within their design. The extent of security best practice integration into product design will determine the ease with which the MDM can adhere to the support practices outlined in this document.

One key practice established in this stage is vulnerability identification and notifications through a Coordinated Vulnerability Disclosure process (CVD). Depending upon support agreements, MDMs may also support security by providing additional services (e.g., security monitoring, backup/recovery, etc.).

Not all Stage 2 support practices will carry over into later stages of the legacy progression.

5.3. Limited Support (Stage 3)

Devices within the Limited Support Stage (stage 3) are defined as medical devices that:

1. Are used for providing patient care, and
2. Have been declared EOL by the MDM and are not currently marketed or sold by their respective MDM, or
3. Contain software, firmware, or programmable hardware components (e.g., CPU) which a) are not supported by their developers and b) whose risks to device safety and effectiveness are

[1] If a software component is unexpectedly declared EOL/EOS during Stage 2, the MDM should update the device to a supported version or alternative supported component to prevent premature stage transitions. See Section 5.5 for more information regarding this aspect of life cycle management

mitigated resulting in a device that can be reasonably protected against current cybersecurity threats.

In stage 3, device MDMs should continue to provide cybersecurity support when possible. For example, it may not be feasible for the MDM to develop updates or patches to their software, but they would continue to apply third-party component or software patches where possible.

Devices in this category may exhibit a wide range of security capabilities within their design. The extent of security best practice integration into product design will determine the ease with which the MDM can adhere to the support practices outlined in the Support Stage.

MDMs should communicate to users the devices and services affected by the limitations, threats that may appear to be unmitigated, and elements of security protection that need to be implemented by the HCP.

Devices in stage 3 often require additional compensating controls, such as network controls, as compared to devices in Stage 2. In Stage 3, MDMs and providers should continue to follow any stage 2 practices that can be reasonably achieved.

5.4. EOS (Stage 4)

Devices within the EOS Stage (stage 4) are defined as medical devices that:

1. Are in use for providing patient care, and
2. Have been declared EOS by the MDM and are not currently marketed or sold by their respective MDM, or
3. Contain software, firmware, or programmable hardware components (e.g., CPU) which a) are not supported by their developers and b) whose risks to device safety and effectiveness are not mitigated resulting in a device that cannot be reasonably protected against current cybersecurity threats.

MDMs should communicate to users they can no longer assure support for devices before the device enters stage 4. Those communications should identify potential risks that users might inherit, as well as mitigation strategies, and upgrade opportunities.

All medical devices will eventually reach an EOS. Preparing for that eventuality is a shared responsibility between MDMs and their customers, since the secure use of a device beyond its cybersecurity EOS depends heavily upon the security capabilities of its deployment environment.

5.5. Framework for Assessing Risk to Trigger Transition to Different Life Cycle Stages

Medical devices and their software and other digital components out of which they are built will reach EOL/EOS over time. Often, these EOL/EOS dates will not be synchronized: a third-party software component may knowingly have a shorter supported lifetime when the device is sold or may be suddenly declared unsupported years before the MDM's announced EOS date. When the support of a third-party software component is known in advance, the MDM should have appropriate plans in place to address the risk from the component's stage transition in the device design. To manage the risks that may arise from sudden, unsynchronized EOL/EOS declarations and statuses of components, MDM's may leverage the following framework for assessing risks that may trigger transition to different life cycle stage:

1. If a single component within a device becomes EOL/EOS, then this serves as a trigger for an MDM to perform a risk assessment to determine if patient safety risks arise, and if so, what kind.
    a. If there are no patient safety impacts, then the device remains in the current life cycle stage (i.e., Support or Limited Support) and the user is made aware the component has reached EOL/EOS.

2. If there are patient safety impacts and the device is in the Support Stage, MDMs should attempt to mitigate the risk of the unsupported component via an update or other design change. When in the Support Stage, the goal of an update or design change would be to replace functionality of the unsupported component with either a supported alternative component or other design change such that the device can safely maintain its intended use until the device reaches its planned EOS. The MDM's risk assessment, along with any relevant threat information from the broader sector, should inform the decision of whether a stage transition is appropriate at this time.
    a. If the risk is mitigated without the use of unsupported components such that the device may be reasonably protected, then the device may remain in the Support Stage.
    b. If the risk is mitigated such that the device may be reasonably protected but the mitigation includes unsupported components, MDMs should transition the device to the Limited Support stage. Use of a mitigation that leverages unsupported components is not considered best practice and should be a last resort. MDMs are expected to publicly communicate this transition and provide the more detailed security documentation needed to facilitate the transition (see section 8.1.1.5 for additional specifics regarding this communication).
3. If there are patient safety impacts and the device is in the Limited Support Stage, MDMs should attempt to mitigate the risk of the unsupported component (e.g., via a design change or compensating control). The MDM's risk assessment, along with any relevant threat information from the broader healthcare sector, should inform whether a TPLC stage transition is appropriate at this time.
    a. If the risk is mitigated such that the device may be reasonably protected, the device may remain in the Limited Support Stage and the user is made aware the component has reached EOL/EOS.
    b. If the risk cannot be reasonably protected against, then the device should transition to EOS and MDMs are expected to publicly communicate this transition (see section 9.1.1.2 for additional specifics regarding this communication).

The framework above is intended for sudden third-party component EOL/EOS declarations. Generally, the software level of support provided for device maintenance is articulated in the device maintenance plan. The software component's EOS date may also be included in the SBOM as it aids in medical device risk management across the TPLC.

For additional information regarding how to balance risks for continuing to operate devices after EOL/EOS, see the Responsibility Transfer Framework of the HSCC HIC-MaLTS.

6. Development Life Cycle Stage: Responsibilities/Expectations

This section of the document details stakeholder responsibilities in the Development Life Cycle Stage as it relates to communications, risk management, and transfer of responsibility.

6.1. Communications

One of the most significant and acknowledged challenges with respect to legacy devices is a lack of information. This lack of information can be associated with a device's technical features, such as its security controls, software supply-chain, or support status. It can also be associated with organizational challenges, such as which parties within an organization—both on the MDM and HCP side—are responsible for its continued maintenance, as well as when, how and to whom information on its security status will be communicated. As a result, communications between MDMs, HCPs, and other relevant parties with respect to legacy devices is critical. To address this need, organizations should establish and enforce legacy communications strategies at multiple stages of a device's TPLC.

6.1.1. MDM Recommendations

Feedback from HCPs in various life cycle stages may inform the MDM's design of future devices and device upgrades. Additional communication sections tied to subsequent TPLC stages provide recommendations that address considerations after medical devices have been procured and deployed by the HCP.

6.1.2. Healthcare Provider Recommendations

HCPs may provide feedback in this TPLC stage regarding their clinical and cybersecurity needs and expectations which inform the MDMs device development.

6.2. Risk Management

6.2.1. MDM Recommendations

1. **Baseline Security Controls:** MDMs should design their products in such a way that security is incorporated and maintainable throughout the life cycle of devices. This may be accomplished through using a secure development framework. Appropriate areas of controls, and specific recommendations, may include:

    a. Security design and controls based on the intended use of the medical device, as well as:
        i. Security risk assessments
        ii. Threat modelling
        iii. Security testing
        iv. Customer facing product security documentation and communication
    b. Post-market monitoring of cybersecurity vulnerabilities capabilities, such as:
        i. Identification of vulnerabilities
        ii. Vulnerability risk identification based on the device security design, controls, and mitigations

c. Ensuring availability of security patches and mitigations based on device risk, such as through:
    i. Coordinated and clear communication to all affected users in regard to the vulnerability and its corresponding mitigations
    ii. Identification of other mitigation options when a security patch is unavailable

2. **Third-Party Component Consideration:** The MDM should consider that the third-party vendor support for a component may end within the HCP's projected use life of the device, and this may adversely impact the MDM's ability to support secure operation of the device.

6.2.2. Healthcare Provider Recommendations

Risk management recommendations for HCPs are not applicable yet because they have not begun the procurement process.

6.3. Transfer of Responsibility

There is no transfer of responsibility recommendations at this stage because the MDM has not provided a device to the HCP. The transfer of knowledge and support begins during procurement discussions.

7. Support Life Cycle Stage: Responsibilities/Expectations

This section of the document details stakeholder responsibilities in the support life cycle stage as it relates to communications, risk management, and transfer of responsibility.

7.1. Communications

This section provides recommendations on the various types of communications that should be exchanged by HCPs and MDMs during the Support Stage of a device's life cycle to ensure ongoing secure operations. Specifically, it is critically important that communications during the Support stage are comprehensive. When entering this stage, organizations should identify what documentation and other information they require, and at what times they may need it. These requirements should then be communicated to the other party and agreed upon. While specific documentation needs may vary from organization to organization, the following sections provide general recommendations. One possible communication strategy about the existing or missing security capabilities of the medical device is described in IEC TR 60601-4-5.

7.1.1. MDM Recommendations

1. **Provide Product Security Documentation**: MDMs should provide product security documentation at the beginning and throughout this life cycle stage to enable HCP risk management during procurement and deployment of medical devices. Appropriate documentation may include:

    a. Manufacturer Disclosure Statement for Medical Device Security (MDS2);
    b. Software Bill of Materials (SBOM) (See IMDRF N73 for additional details about SBOM best practices);
    c. Security test report summaries, third-party security certifications, or similar;
    d. Customer Security documentation (e.g., technical instructions to ensure secure deployment, operation & servicing including information on the interfaces, communication protocols, and networking, Cloud, or communication dependencies for the system).

2. **Provide Product Life Cycle Documentation:** MDMs should communicate clearly on the key life cycle milestones, including cybersecurity EOL and EOS dates (if available) of devices as part of procurement and installation processes. The MDM should provide this information as far in advance as possible. Current practice suggests information to be provided at least 2 years in advance to best support the HCP. MDMs can support HCPs and users by clearly communicating the following information:

    a. affected device
    b. the device's operating system(s)
    c. the version of device deployed
    d. identification of software components
    e. expected date of service changes
    f. the extent of any available maintenance after those changes
    g. additional compensating controls

3. **Provide Relevant Updated Product Security and Life Cycle Documentation:** As a device continues throughout its life cycle, it is possible that its supporting product security or life cycle documentation (as discussed in Section 6.1.1 regarding Communications during the Development Stage) may change. In such cases, MDMs should provide relevant updated documentation, which may be in electronic form, to HCPs to enable them to adjust their risk management strategies as needed to respond to new or changed risks.

4. **Provide Vulnerability and Patching Information:** If a vulnerability is discovered, the MDM should provide relevant vulnerability information, including appropriate mitigations (e.g., software patches). It is expected that high priority should be placed on high-risk vulnerabilities where timely communication is required to prevent patient harm or device disruption. In addition, the mitigation method (e.g., over-air update, deployment of service personnel to install) and implementation instructions should be provided to the device operators.

5. **Provide Proactive Communications for Third-Party Components:** It is possible that the software and other digital components within a medical device will reach EOL/EOS before the device itself does. In such cases, the lack of support for such components may introduce risks to the device. To help compensate for these risks, MDMs should:

    a. Track the support status of the third-party components used within their device.
    b. Assess the risks that may exist if and when those third-party components become unsupported.
    c. Communicate new risks and any available mitigations to HCPs.

6. **Provide Patient Communications:** While beyond the scope of this document, both MDMs and HCPs should communicate EOL/EOS dates and information to patients where relevant.

7.1.2. Healthcare Provider Recommendations

1. **Identify Information Needs:** For all devices—legacy and otherwise—HCPs should identify the types of information that they believe they need to appropriately maintain and protect a device (discussed in more detail below), when, how, and from where they should receive that information, and to whom that information should be provided.

    a. For example, an HCP may decide that for a specific legacy device, they need to understand if the device will receive updates, for how long, and when those updates may be expected. In turn, the HCP may decide that information should be provided to the HCP's security and clinical engineering teams so that those teams can make appropriate operational and maintenance decisions.
    b. One particular area that HCPs should consider as they develop operational strategies is transfer of responsibility. In some cases, HCPs continue to use devices past a MDM's declared EOL or EOS date. To ensure that devices remain safe and effective for use, HCPs should proactively ask the MDM when responsibility for the risk of using unsupported device transfers from one party to the other.

2. **Pre-Procurement Communications:** To prepare an HCP to manage the security of the device during its lifetime at the facility, prior to purchase and installation of a device, information should be shared between the MDM and the HCP to aid in proper onboarding and management. HCPs may want to request the following:

    a. EOL date (if known)
    b. EOS date (if known)
    c. Upgrade strategy for device software components (e.g., operating system, third-party software, application software)
    d. Ports and services necessary for the device to function appropriately
    e. Firewall rules that can be leveraged to isolate the device and maintain function

f. Anti-malware capabilities and appropriate definitions (what can be scanned)
g. Security scanning capabilities and appropriate scanning definitions (how to scan)
h. Security logging capabilities
i. Device backup and restore procedures
j. Notification method to receive vulnerability notifications
k. Administrative accounts and the ability to manage through a privilege access management tool

3. **Ongoing Communications:** Once a device is installed and in use, communication between the MDM and HCP is needed to ensure proper operational and risk management throughout the device's life cycle. HCP should be prepared to receive the following communications throughout the device lifecycle:

a. Vulnerability disclosures that describe the assessed risk, with updates through a push mechanism as appropriate
b. Mitigation recommendations to control risk of known vulnerabilities
c. Indicators of compromise that may appear on the device or that may be revealed as a result of network monitoring
d. Updated SBOM throughout the device's life cycle in machine readable format
e. Options to address outdated software components (i.e., operating system, third-party software) as soon as possible prior to reaching end of support

7.2. Risk Management

7.2.1. MDM Recommendations

1. **Third-Party Risk Management:** While a medical device might be in any of these life cycle stages, there could be embedded components that are already end of life, or even end of support. Risk assessment should determine the overall impact on safety, essential performance and cybersecurity.

Even when an unsupported component has exploitable vulnerabilities, there can be other compensating controls within or external to the medical device that could significantly reduce the likelihood of exploitation. For example, a network firewall could block or provide controlled limited access to a network port on a medical device which exposes a network vulnerability. While a firewall is an option, the MDM should avoid solely relying upon the use of firewalls or segmentation to address vulnerabilities and control risk as doing so may impact patient care.

2. **Communication Expectations**: When the medical device approaches the EOL date, the MDM should provide clear communication to HCPs and regulators on the EOL and EOS dates and provide adequate information to the HCP to plan for the EOS life cycle stage. In addition to the information indicated in Section 7.1.1, this life cycle information might include upgrade options.

These additional pieces of information can be used to support the required risk management activities of the HCP for the continued use of the medical device.

3. **Post-market Expectations:** There are certain activities that MDMs are expected to complete in the post-market for devices and these expectations apply to the TPLC for medical device cybersecurity. Specifically, these expectations are:

a. Collecting, documenting, and responding to customer complaints (including servicing)

b. Reporting adverse events/incidents as required by regulators (e.g., events caused by a device problem that led to death, serious injury, or may lead to death or serious injury if the event were to recur)

c. Performing field safety corrective actions if necessary (e.g., recall, modification, change IFU, etc.).

   i. In some cases (e.g., depending on the life cycle stage) pursuant to the regulatory requirements, the MDM may not take a formal action, they might just communicate the existence of a cybersecurity vulnerability and any known mitigations.

   ii. For devices in which the medical device is connected directly to the patient (e.g., continuous glucose monitors), MDMs are expected to communicate recall and removal information per jurisdiction requirements

d. Engaging in proactive risk management including vulnerability management (e.g., using tools, resources, and personnel to monitor, address, and communicate security issues that impact device security and safety risks on an ongoing basis)

e. Engaging in reactive risk management including vulnerability management (e.g., using tools, resources, and personnel pulled together to address and communicate significant security and safety risks as needed)

4. **Continued Monitoring:** Until EOS, the MDM should continue to monitor for changes in the risk profile of the medical device and inform HCPs and regulators of such changes as this might impact safety, timeline, budget, activities or even the continued use of the medical device. Whether or not the HCP still receives software updates during the Limited Support Stage for components that might still be supported might depend on specific agreements between the MDM and the HCP and the ability of the MDM to extend the EOL date.

7.2.2. Healthcare Provider Recommendations

As a device continues through the TPLC, it is important to consider the evolving needs around risk and vulnerability management and how the HCP can implement best practices to mitigate these risks. With an evolving threat landscape, actions and practices may need to change and evolve as well. Without careful planning, the risk that legacy devices pose, and the potential consequences will increase over time. While cybersecurity of medical devices is a shared responsibility, as a device continues through its life cycle through to its communicated EOL and EOS dates, the HCP may need to take increased of responsibility for implementing security measures around devices.

1. **Baseline Security Considerations:** Baseline security recommendations become critically relevant during the Support stage. Baseline security recommendations for HCPs may include:

   a. Applying network security controls to devices by assessing the importance and criticality of devices through a risk assessment process
   b. Performing a risk assessment to identify critical devices, which may also require additional network and physical controls and regular monitoring
   c. Maintaining active communication with MDMs for support and patching recommendations
   d. Employing configuration management to identify all current assets, data flows, and track future configuration changes
   e. Maintaining IT security monitoring and patching processes that support cyber hygiene and vulnerability remediation.
   f. Protection from unauthorized access through logical and physical security controls
   g. Cybersecurity training and awareness programs.
   h. Vulnerability Management

2. **Operating Environment Considerations:** Appropriate device risk and vulnerability management will depend on the specific device and its operating environment. Considerations for access controls and monitoring are described in the paragraphs below.

3. **Access Controls**: It is important that devices have access and connections only to parts of a HCP's network that they require to perform their function. Implementing access controls for devices may restrict the flow of information and commands to/from the device more than what is necessary. While these controls may evolve depending on the type of device, other network functions, and the device's position in the TPLC, existing tools such as Next Generation Firewalls allow for dynamic network segmentation and system policy enforcement based on a set of defined rules.

4. **Network Segmentation:** Networks may also be segmented based on security requirements and business needs. However, segmenting a network may limit the ability of any lateral movement across a network should any part of it become compromised. If implementing network segmentation, consideration should be given to how the segmentation (including use of firewalls) impact device function.

   Note: Many devices have been and are designed and built to integrate with clinical applications and the electronic health record. Controlling vulnerabilities in a legacy device through segmentation or a firewall creates administrative burden, presents possibility of negative patient care impacts, and depreciates intended integration benefits. As a result, an MDM should avoid solely relying upon the use of segmentation or firewalls to address vulnerabilities and control risk.

5. **Multifactor Authentication:** Implementation of multifactor authentication allows for the enforcement of roles-based access to network or device functionality. However, the modes and speed of authentication must be considered in the context of the healthcare environment.

6. **Monitoring:** Monitoring the activity of devices on a network can be used to help HCPs prevent compromise, as well as aid in response should it occur. Throughout a device's life cycle, the HCP should implement some kind of activity monitoring system that is able to track activity of networked devices, and in some cases provide information around potentially errant behaviour.

   Note: This may take the form of an Intrusion Detection System, Intrusion Prevention System, system logging, or firewall logging system. For HCPs with a more mature cybersecurity posture, these could be incorporated into Security Information and Event Management system. HCPs should work with the MDM as appropriate regarding the use of such systems since they may impact the intended use of the device. Given the nature of legacy devices, installation, and addition of monitoring software to the device itself may not be feasible, especially for devices that use real time operating systems. However, there are tools available that allow for monitoring of information flow to and from external devices which may allow for the collection of appropriate device behavioural information.

7. **Inventory Considerations:** Proactive planning for EOS begins during procurement discussions before the device is installed, whether EOS dates are known or not. Use of a strong inventory management system can help. An easy to use, accurate, and real-time inventory will allow the HCP organization sufficient time to proactively plan for any upcoming EOS dates. For each asset in inventory, it would be of benefit to include information such as:

a. Current life cycle stage

b. Expected EOS date

c. SBOM (See IMDRF N73 for additional details about SBOM best practices)

d. Vulnerability status & software patch status

e. Operational environment (network diagram)

f. Maintenance schedules

Automating certain tasks, where possible, may also allow clinical staff to focus on healthcare delivery. This robust inventory management system is also essential should the healthcare delivery organization decide to continue the clinical use of the device past its EOS date. During planning for and after EOS, the HCP should understand and accept the risk to continue using the device. The HCP should consider performing regular clinical benefit/risk analyses comparing the use of the legacy device past its EOS date by employing risk compensation measures versus purchasing a new or upgraded device.

8. **Vulnerability Management Considerations:** As stated in the IMDRF N60 guidance, HCPs should consider adopting a risk-based approach to the management of medical device cybersecurity. This process should be applied to:

a. Development, upkeep and upgrading of IT infrastructure
    i. Consideration of the network that devices connect to is important, and any network design and architecture should take into account the variety of potential devices (including legacy devices) that may exist on the network. This may include implementing Zero Trust Architecture protocols that increase device security, without inhibiting healthcare practitioners from delivering timely aid when required.

b. Acquisition and use of SBOMs
    i. The nature of medical device architecture and design means that it may contain both software and hardware from multiple different sources and suppliers (including but not limited to embedded systems, data logging, and hardware componentry). It is important that the HCP request an SBOM for any devices that are integrated into their network infrastructure. If available, the SBOM will enable a customer to better understand how the device may progress through its TPLC, and how to apply risk control measures and mitigation strategies more effectively.
    ii. It is not uncommon for some types of software or sub-systems to have vulnerabilities that affect all systems that include them as components. An SBOM would allow the HCP to check if a device may be affected by a disclosed vulnerability that relates to a component of the device, rather than the device itself.
    iii. As a device approaches EOL and EOS dates, it is important that the HCP have a system in place to monitor disclosed vulnerabilities and how they may affect devices that are in use.

c. Integration and installation of any new device on the network
    i. New devices may undergo risk assessment prior to integration into an existing network. This may include the decision to have the device exist on network segments, application of access controls, and integration of network monitoring for device activity.

d. Updates/changes to any networked equipment (including but not limited to medical devices and connected equipment, such as laptops and servers).

The IMDRF N60 guidance lays out several recommended standards that HCPs may choose to refer to in applying a risk management process.

The HSCC HIC-MaLTS "Challenges and Recommendations" section includes specific recommendations for addressing many of these challenges, including inventory management and SBOM.

9. **Decommissioning Considerations:** Section 6.6.2 of the IMDRF N60 guidance sets out a number of security recommendations over the TPLC of a medical device. As a device approaches its EOS, it is important that the HCP investigate decommissioning the device or assume the cybersecurity risk for its ongoing use.

7.3. Transfer of Responsibility

As products age and move through the TPLC, it is important to identify the transition from shared MDM/HCP security responsibility in Support and Limited Support, to transfer of cybersecurity support responsibilities to the HCP in EOS. Except when a device component is unexpectedly declared unsupported, the EOL declaration triggers the Limited Support Stage which serves as a transitional period for MDM/HCP coordination. For additional information on transitioning to different life cycle stages, see Section 5.5). Section 7.3 provides recommendations for both MDMs and HCPs in implementing this life cycle transfer of responsibility.

7.3.1. MDM Recommendations

1. **Timeline Considerations:** As a best practice, the transfer process to move cybersecurity responsibilities to the HCPs begins approximately 2-3 years before the EOS. MDMs providing HCPs 2-3 years of notice helps enable the HCP to evaluate, plan and budget for equipment replacements.

2. **Pathway to transition to new/upgraded supported device**: Before the Support Stage ends, the MDM and HCP should coordinate and prepare for eventual transition to EOS and/or product upgrade/replacement. Transitioning to a supported device maintains the shared security responsibility between the MDM and HCP.

   For devices that are not able to be supported by the MDM and have not been replaced by the HCP, the cybersecurity responsibility will transfer to the HCP. In order for the HCP to identify all available options, the MDM should identify the following information:

   a. Detailed information on Medical Device(s) impacted by the transition to the Limited Support Stage and eventual transition to the EOS Stage
   b. Configurable security options that may be implemented at EOL/EOS
   c. Upgrade options available to the HCP

      - Software (s/w) only
      - Partial - s/w and hardware (h/w)
      - Complete replacement
        - Replacement options & strategy
        - Available device models and functionality

7.3.2. Healthcare Provider Recommendations

During the Support Stage, the HCP may want to:

1. Assess their ability to manage the device from a cybersecurity and clinical use perspective.

2. Identify possible support from 3rd party which may be available to help manage the device.
3. Assess device replacement opportunities.
4. Identify additional resources which are available to support the device.

8. Limited Support Life Cycle Stage: Responsibilities/Expectations

This section of the document details stakeholder responsibilities in the Limited Support Life Cycle Stage as it relates to communications, risk management, and transfer of responsibility.

8.1. Communications

Communication between MDMs and HCPs should increase during the limited support stage. Risk information should be provided to HCPs so they can make informed decisions on the risks they are inheriting. Information on mitigation and device replacement options should also be made available.

8.1.1. MDM Recommendations

1. **Release Customer Notifications Indicating Move to Limited Support:** MDMs should release a customer notification (e.g., public disclosure via company website or direct notification to HCPs) 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 and business continuity planning for HCPs.

2. **Release Public Information Indicating Move to Limited Support:** MDMs should release a public notification (e.g., public disclosure via company website or other, permanently available resource) that explains the support status of the device. It should be updated if the device moves to a different stage, so that relevant parties—including resellers and organizations potentially looking to purchase devices second-hand—may understand the potential risks of continuing to use such devices.

3. **Continue to provide services and documentation** from the communications in the Support Stage (Section 7.1.1) as far as it is practical and appropriate. This includes vulnerability communications.

4. **Provide Life Cycle Planning Information:** MDMs should continue to communicate timelines for cybersecurity EOS dates to allow ample time for customers to prepare for EOS and the associated customer responsibilities. Possible communications include:

    a. Alerts indicating that some maintenance has stopped when parts of the medical device (i.e., device software) are no longer supported
    b. Security notifications and advisories
    c. Device-specific information advisories about compensating controls
    d. Any intended use restrictions which result from life cycle stage changes

5. **Provide Product Security Documentation**: On top of providing the recommended security documentation in the Support Stage (Section 7.1.1.1 and 7.1.1.3), MDMs should provide the following documentation:
    a. Updated security documentation that indicates any compensating controls that are recommended given the reduced support, which may include:

i. Firewalls
ii. VPNs
iii. Network Isolation

b. Expectations for device deployment environment.

8.1.2. Healthcare Provider Recommendations

Communications from 7.1.2.3 should be continued and HCPs should ask the MDM any questions they have about the additional and more granular information they are receiving (i.e., 8.1.1). As HCPs may be evaluating whether to purchase resold or second-hand devices, they may also want to ask whether additional support may be available such as through extended contracts or third-party support.

8.2. Risk Management

8.2.1. MDM Recommendations

MDMs should continue actions related to post-market expectations and monitoring from the Support Stage in Section 7.2.1. However, the frequency and level of effort associated with proactive vulnerability management as a part of risk management activities may decrease.

8.2.2. Healthcare Provider Recommendations

1. **Consider EOL/EOS Risks When Evaluating Whether to Purchase Resold or Second-hand Device:** HCPs may choose to purchase resold or second-hand devices. In doing so, they should undertake the following actions to help manage any potential cybersecurity risks:

    a. Research whether the desired device is in Limited Support (i.e., has reached its EOL date) or is in EOS.

    b. If it is, HCPs should carefully consider the risks of using a device that has reached EOL/EOS date.

    c. If HCPs choose to purchase the device, they should:

        i. Determine whether support is available, such as through extended contracts or third-party servicing.

        ii. If support is available, then HCPs should include language in their contracts with the vendor organization to require and/or include support. If support is not available from vendor, the HCPs should consider how the HCPs will support the device.

2. **Considerations for HCPs when approaching EOS:**

    After EOL, the HCP is notified that a device's EOS date is approaching both through active communications from the MDM and notifications from inventory management systems. The HCP must further prepare for EOS and should consider the following questions to help identify whether the risks of operating the device without support are adequately controlled. The list of questions below is not exhaustive.

a. What time frame beyond the expected service life is the device projected to be used for clinical care?

b. Will there be maintenance costs over the time the device is projected to be used for clinical care?

c. How do the maintenance costs compare to upgrading the device?

d. How could a new or upgraded device improve clinical care while also improving cyber resilience?

e. Does the HCP have the tools to maintain the security of this device?

f. Does the HCP have the financial resources to maintain the security of this device?

g. Does the HCP have the expertise to maintain the security of this device?

h. What would be the risk to patients should this device be compromised?

i. What would be the risk to patients should the organization be compromised due to this device?

j. What would be the risk to patients should this device not be used and replaced by an alternative?

k. Can this device operate beneficially without being connected to the network?

l. What other controls can be put in place?

For additional recommendations and considerations, HCPs may refer to the Responsibility Transfer Framework within the HSCC HIC-MaLTS.

8.3. Transfer of Responsibility

This Limited Support Stage serves as a transitional period for the MDM and HCP to coordinate and prepare for eventual transition to End of Support or product upgrade/replacement. During this period, both parties evaluate device and support options and make recommendations to get to a future state. Limited Support arrangements may be available to maintain a shared security responsibility during that transition. Availability and scope of the Limited Support can vary and should be fully understood and acknowledged by each party. Should that future state remain unchanged, and the unsupported product is left in service and cannot be supported by the MDM, then security responsibilities are on the HCP to support the ongoing use and care for that device.

Cybersecurity support responsibilities will be transferred to the HCP. If the HCP is unable to assume certain responsibilities, the MDM may consider a gradual transfer of responsibility where feasible.

8.3.1. MDM Recommendations

To ensure a smooth transfer of security responsibilities to the HCP, the following list of considerations should be reviewed and evaluated.

1. Identify available software updates to give the customer the ability to have all available applied (or made available for the customer at EOL/EOS milestone).

2. Security documentation provided by the MDM should provide information helpful to the HCP to enable network security controls.

3. Network requirements identified that give the HCP information on ports and IP addresses needed for the device to operate.

4. Network requirements allow the HCP to ‘harden’ and block all unnecessary ports and IP addresses from accessing the medical device (from the network).

5. Available product security documentation (including SBOM).

6. Other information, as available, related to cybersecurity best practices for medical devices that could help the customer cyber security posture.

7. Communicate limited support options available which may or may not contain:

    a. H/W component replacements if available (e.g., display monitor, cabinet, hard disk drive, etc.)

    b. Reloading s/w, restoring device system state

    c. Addition of network hardware security appliances (separate from the medical device) if available

8.3.2. Healthcare Provider Recommendations

To ensure a smooth transfer of security responsibilities to the HCP, the following list of considerations should be reviewed and evaluated.

1. Cybersecurity monitoring for the device

2. Vulnerability management

3. Implementation of compensating controls, including physical and logical access controls

4. Ensuring the deployment environment is appropriate for adequately securing the EOS device

5. Implementing an incident response plan

6. Establishing a business continuity plan

7. Conducting regular risk assessments as outline within the HCP’s Risk Management Process

9. EOS Life Cycle Stage: Responsibilities/ Expectations

This section of the document details stakeholder responsibilities in the EOS life cycle stage as it relates to communications, risk management, and transfer of responsibility. EOS is a significant milestone in the device lifecycle, and the HCP should be aware when additional cybersecurity responsibilities are transferred to them and prepare accordingly.

9.1. Communications

9.1.1. MDM Recommendations

By the time a device enters the EOS Stage, the MDM should have informed the HCP of the EOS date and when the device will reach the EOS stage. At this stage, additional cybersecurity support responsibilities may transfer to the HCP. If the HCP is unable to assume certain responsibilities, the MDM may consider a gradual transfer of responsibility where practicable.

1. **Provide Product Security Information for Security Maintenance:** MDMs should provide relevant product security information to HCPs to best enable them to manage device cybersecurity risks without the assistance of the MDM. This information may include:

    a. Any additional responsibilities HCPs will assume to ensure the device remains secure, which may include site-specific controls (e.g., firewalls, network isolation, VPNs).
    b. Support available beyond the cybersecurity EOS date.
    c. Available upgrade path for the device.
    d. Decommissioning information: MDMs should provide information that enables the HCP to decommission the device at a future date.

2. **Release Public Information Indicating Move to EOS:** MDMs should release a public notification (e.g., public disclosure via company website or other, permanently available resource) that explains the support status of the device. It should be updated so that relevant parties—including resellers and organizations potentially looking to purchase devices second-hand—may understand the potential risks of continuing to use such devices.

3. **Communicate patient risks received as part of post-market expectations via reactive vulnerability management, as appropriate.**

9.1.2. Healthcare Provider Recommendations

HCPs should ask the MDM any questions they have about the information they are receiving at the beginning of EOS (i.e., 9.1.1). As HCPs may be evaluating whether to purchase resold or second-hand devices, they may also want to ask whether additional support may be available, such as through extended contracts or third-party support.

9.2. Risk Management

9.2.1. MDM Recommendations

After EOS, the MDM is still responsible for certain post-market activities dependent upon jurisdictional regulations (see section 7.2.1.3). If there is a significant risk to patient safety, such as in a ransomware scenario (e.g., WannaCry), there may be a need for additional responsive risk management actions [such as those highlighted in section 7.2.1.3].

9.2.2. Healthcare Provider Recommendations

1. **Consider EOL/EOS Risks When Evaluating Whether to Purchase Resold or Second-hand Device** as described in 8.2.2.1

2. **Considerations for HCPs when using a device past its EOS:** Should the HCP accept the risk in using a medical device past its EOS date, it is recommended that they:

    a. Ensure the implementation of a strong, qualified, appropriately resourced (i.e., resource to manage increasing risk), cybersecurity program that has endorsement from senior leadership.
    b. Ensure the implementation of a robust inventory management system, with automation if possible.
    c. Include the legacy device in on-going organizational risk management activities.
    d. Proactively monitor trusted sources of information such as Information Sharing Analysis Organizations, Information Sharing and Analysis Centres, dissemination agencies such as Computer Emergency Response Teams (CERTs), regulators, vulnerability databases (e.g., those for third-party components), etc.
    e. Enhance countermeasures including, but not limited to, network segmentation, user access roles, security testing, network monitoring, and disconnection from the network.
    f. Periodically evaluate alternative products available and revisit the decision to operate a device past its EOS.

For additional recommendations and considerations, HCPs may refer to the Responsibility Transfer Framework within the HSCC HIC-MaLTS.

9.3. Transfer of Responsibility

9.3.1. MDM Recommendations

At this stage, the transfer of responsibility to the user is complete. MDMs have communicated that the device is EOS and that there has been a transfer of responsibility.

9.3.2. Healthcare Provider Recommendations

Acceptance of Responsibility/Risk or Transition to New/Upgraded device: Given a variety of pressures, it is not uncommon for HCPs to continue to use medical devices past their expected service life. In many cases, it is evident to users that a device fails or does not operate as intended, triggering internal service or decommissioning. In other less obvious cases, support for protection against threats may also become non-existent. In both cases, the potential for patient harm exists. It is imperative that the HCP have a strong inventory management system in place and when the EOS date approaches for each medical device, careful considerations are made with respect to the risks the legacy device poses as well as the maturity of the cybersecurity program within the organization.

10. Summary of Cybersecurity TPLC Responsibilities/ Expectations

Sections 6-9 above, provide additional detail on the responsibilities and expectations for MDMs and HCPs within the context of four (4) TPLC stages for cybersecurity: Development, Support, Limited Support, and EOS; particularly as it relates to risk management, communication, and transfer or responsibility. Also described in sections 6-9 are certain activities that MDMs are expected to complete post market for devices across the TPLC for medical device cybersecurity. A summary cybersecurity TPLC, shown in Figure 2, displays the associated level of effort for given responsibilities and expectations as a function of the transfer of responsibility across the TPLC.

Cybersecurity and the Total Product Life Cycle

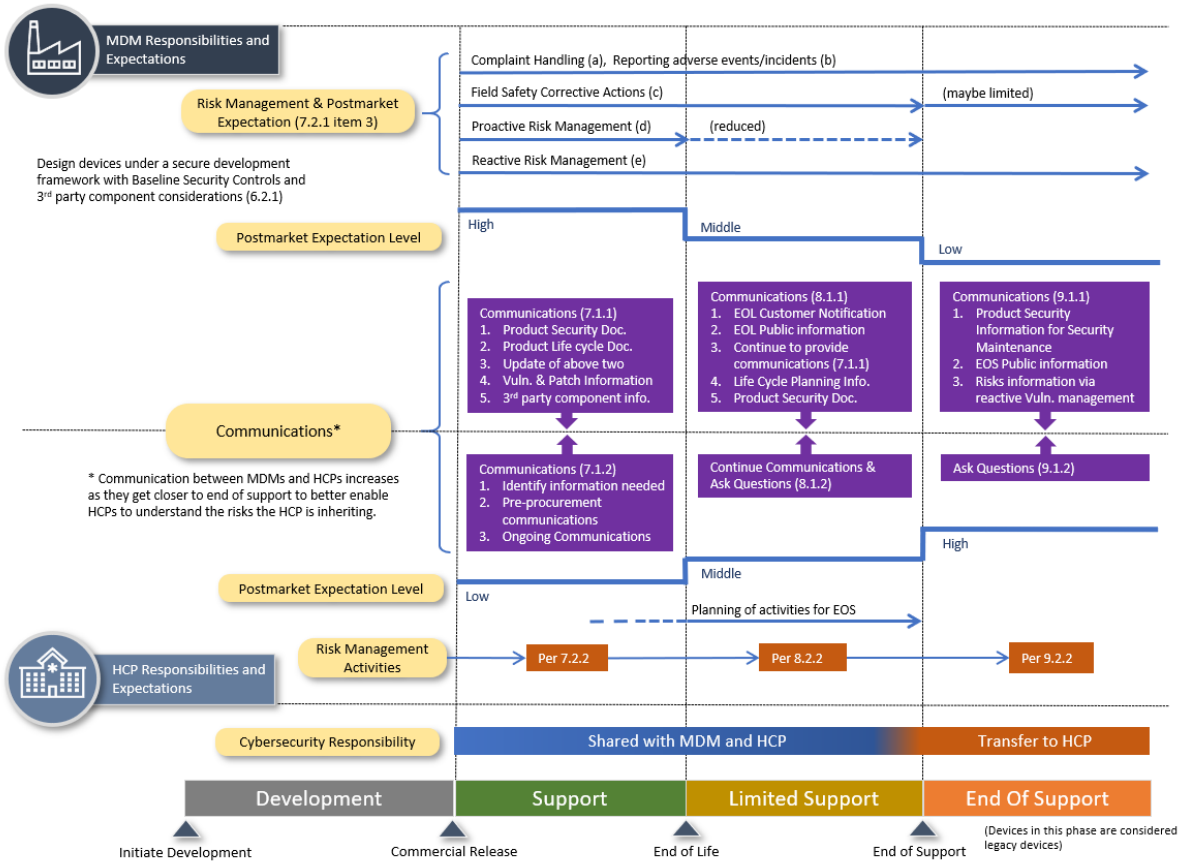

Figure 2: Detailed legacy device framework as a function of product life cycle for cybersecurity

11. Considerations regarding compensating controls after EOS for a Medical Device

A compensating risk control measure (also called “compensating controls”) is a 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). In the event of identified health and safety risk or other non-compliance, the MDM shall implement further correction, corrective actions and, where applicable, preventive actions to bring the device into compliance.

Once a device has reached EOS as communicated by the MDM, an HCP may decide to keep the device operational despite the risk involved of using legacy technology and the lack of security support by the MDM. Reasons for continued use could be but are not limited to: when the length of time for which the device will be used for clinical care exceeds its supportability, there is no viable alternative on the market, or budgetary limitations.

If an HCP decides to keep using the device after EOS, it should consult the product security documentation provided by the MDM during the Limited Support and EOS Stages as described in section 8 and 9 of this guidance. This documentation includes minimum compensating risk control measures applicable to the device itself and the operating IT environment.

11.1. Compensating Risk Control Measures

Implementing compensating risk control measures may have a significant cost for the HCP, both in terms of technical provisions and resources. As such, the HCP should consider the costs of compensating risk control measures versus the cost and benefits of acquiring new devices.

Table 1 contains general recommendations for compensating controls. While these recommendations are provided in the context of EOS, feasibility of implementation will depend on the specific device and its operating environment and must not compromise the clinical and intended use of the device. The control measures listed are not exhaustive and it may be appropriate to utilize more than one or a combination of control measures. Technological innovations should also be considered when implementing compensation risk control measures.

Type of control	**Compensating risk control measures**
Physical access	Restrict physical access to the device to authorized personnel only by placing the device in a restricted area with the appropriate physical entry controls in place. Use of tamper evident seals as appropriate.
Removable media	Restrict the use of removable media such as USB drives by policies in the systems Basic Input Output System/Unified Extended Firmware Interface Forum (BIOS/UEFI), through operating system policies or by physical means.

Network isolation	Isolate the device from the hospital network(s).
Network segregation	Set up a virtual local area network (VLAN) for the device and the other infrastructure/services the device communicates with.
Monitoring	Monitor the device and network for suspicious activity by using an Intrusion Detection System, Intrusion Prevention System or Security Information and Event Management.
Remote access	Remove remote access capabilities from the device.
Firewall	Place the device behind a physical or virtual firewall and only open the ports of the firewall for the network communication that is strictly necessary.
Anti-malware	Install an anti-malware solution on the device, after consultation with the manufacturer. For devices that are isolated from the network (stand-alone), use a solution that does not need definition updates, e.g., an artificial intelligence (AI)-driven anti-malware solution.
Backup and restore	Implement backup and restore procedures to protect against loss of data in case of calamities.

Table 1: Examples of Compensating Risk Control Measures

11.2. Education

While the implementation of technical and physical compensating control measures can aid in keeping devices more secure after EOS, a well-trained staff is just as important to protect HCPs against cybersecurity threats. As such, HCPs are encouraged to provide cybersecurity training to create security awareness and introduce cyber hygiene practices among all users. This should 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 behaviour (e.g., random shutdowns/ restarts, security software disabled). In addition, clinical personnel should be informed of the security limitations of the device after it has been declared EOS and on security best practices, they should be adhering to in order to mitigate any risk when operating the device.

12. References

12.1. IMDRF Documents

1. Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity IMDRF/CYBER WG/N73FINAL:2020 (April 2022)

2. Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020 (April 2020)

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

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

12.2. Standards

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

6. AAMI TIR 97:2019, Principles for medical device security—Post market risk management for device manufacturers

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

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

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

10. IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

11. IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

12. IEC 81001-5-1:2021, Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle

13. IEC 80001-1:2021, Application of risk management for IT-networks incorporating medical devices – Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software

14. 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

15. 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

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

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

18. 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 (HCPs) on how to self-assess their conformance with IEC 80001-1

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

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

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

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

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

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

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

26. 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

12.3. Regulatory Guidance and Draft Guidance

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

28. China: Guidance for Premarket Review of Medical Device Cybersecurity (March 2022)

29. 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)

30. 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)

31. FDA (Draft): Cybersecurity in Medical Devices: Quality System Considerations and Content Premarket Submissions (April 2022) [This guidance is draft at the time of this N73 publication and is not for implementation. It will be superseded by a final guidance.]

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

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

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

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

36. Germany (BSI) - Security requirements for eHealth applications Technical Guideline (BSI TR-03161) (April 2020)

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

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

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

40. Medical Device Coordination Group (MDCG) 2019-16: Guidance on Cybersecurity for medical devices (December 2019)

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

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

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

12.4. Other Resources and References

44. CERT® Guide to Coordinated Vulnerability Disclosure

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

45. The NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

46. 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

47. NIST Special Publication 800-12 Rev 1 Introduction to Information Security (June 2017)

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

48. Medical Device and Health IT Joint Security Plan (January 2019)

https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

49. MITRE medical device cybersecurity playbook (October 2018)

https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

50. MITRE CVSS Healthcare Rubric

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

51. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf

52. Health Industry Cybersecurity Practices: Managing Legacy Technology Security (HIC-MaLTS)

53. Open Web Application Security Project (OWASP)

https://www.owasp.org/index.php/Main_Page

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

55. ECRI approach to applying the NIST framework to MD

https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical-Devices.aspx

56. 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