DRAFT DOCUMENT

Title: Principles and Practices for the Cybersecurity of Legacy Medical Devices

Authoring Group: Medical Device Cybersecurity Working Group

Date: April/May 2022

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.

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

1.0 Introduction

Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020, hereinafter also referred as “IMDRF N60 guidance”) has 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 timepoint manufacturers anticipated devices would be clinically used —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 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 for implementing cybersecurity of legacy medical devices. It is intended to provide Stakeholders will have 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.

2.0 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, as well as the focus on potential for patient harm remain unchanged.

It 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 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 are also outside the scope of this guidance as they often do not have to adhere to 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 phase;
- 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.

3.0 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 *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.

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

3.5 *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).

3.6 *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, labeling, or assembly that is intended to be included as part of the finished, packaged, and labeled device

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

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

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

3.10 *Coordinated Vulnerability Disclosure (CVD):* process through which researchers and other interested parties work cooperatively with a manufacturer in finding solutions that reduce the risks associated with disclosure of vulnerabilities (AAMI TIR97:2019)

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

3.11 *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)

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

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

3.14 *Embedded computer system*: computer system that is part of a larger system and performs some of the requirements of that system (ISO/IEC/IEEE 24765:2017)

3.15 *Embedded operating system*: operating system software for an embedded computer system (ISO/IEC/IEEE 24765:2017)

3.16 *End of Life (EOL):* Life cycle stage 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.

3.17 *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.

3.18 *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 during the expected lifetime.

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

3.20 *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)

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

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

3.23 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)

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

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

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

3.27 *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)

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

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

3.30 *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)

3.31 *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)

3.32 *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)

3.33 *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)

3.34 *Software Bill of Materials (SBOM)*: list of one or more identified components 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. The primary focus of this effort is software components; however, hardware is not excluded. (NTIA Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) 2019-11-12)

3.35 *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.

3.36 *Stakeholder*: individual or organization having a right, share, claim, or interest in a system or in its possession of characteristics that meet their needs and expectations (ISO/IEC TS 24748-1:2016)

3.37 *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 1 to entry: Parties involved are usually supplier ("first party") and purchaser ("second party") interests.

3.38 *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)

3.39 *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)

3.40 *Total Product Life Cycle (TPLC)*: development, support, limited support, and EOS phases in the life of a medical device.

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

3.41 *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.

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

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

3.44 *Vulnerability scan*: a computer program to identify vulnerabilities in networks, computer infrastructure or applications.

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

4.0 General Principles

This section provides general guiding principles for legacy devices for all stakeholders to consider when developing, regulating, using, and monitoring medical devices. These themes, 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

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) and decommissioning; where it is noted that decommissioning could occur following 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 needs to include the stages of: development, support, limited support, and EOS, where EOS is considered the time point where the responsibility for cybersecurity is transferred to the HCP. 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 end of support to ensure that MDMs and HCPs can adequately prepare for each life cycle stage

4.2 Shared Risk Management

Medical device cybersecurity is a shared responsibility between stakeholders, and with legacy devices, notably between MDMs and users. To appropriately manage risk for legacy devices, MDMs should design and support their devices in a way that optimizes cybersecurity in the support phase and minimizes the security risk after EOS in the future. Users should actively engage with MDMs to obtain an SBOM, ensure that the device operates in the recommended environment, and plan for the device’s EOS date.

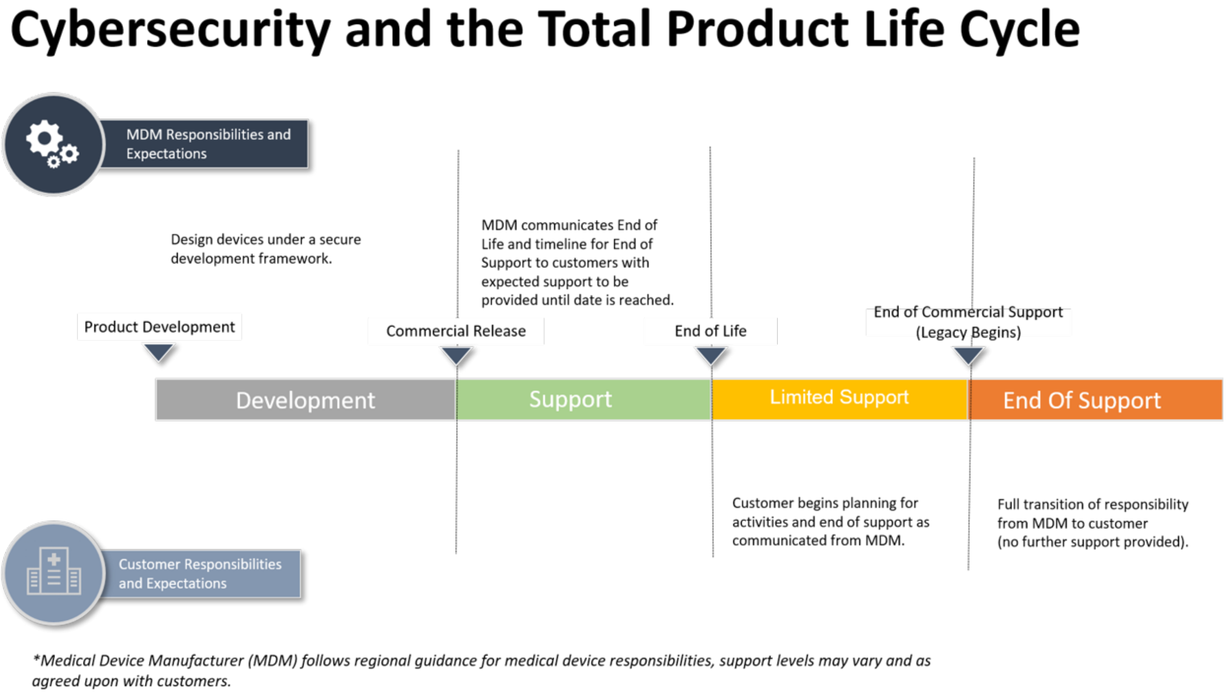
4.3 Communication

Effective protection against threats requires open and transparent communication between stakeholders. MDMs are expected not only to design and develop medical devices with planned EOL and EOS stages, but also clearly communicate those stages as soon as possible; preferably as a part of device procurement and installation. This enables users to appropriately plan for EOL and EOS by obtaining information from the MDM to inform next steps regarding device maintenance Since in EOS a device would not be reasonably protected against current cybersecurity threats, the HCP could either decommission the device or assume responsibility for maintaining its security.

5.0 Overview of IMDRF/N60 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 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 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. Some jurisdictions may refer to the stages with different terms. However, the concepts described in each stage should be applicable universally. Also, please note that though the life cycle stages may occur for different time durations (e.g., the support phase may be longer than the limited support phase).


Cybersecurity and the Total Product Life Cycle
MDM Responsibilities and Expectations
Product Development
Commercial Release
End of Life
End of Commercial Support (Legacy Begins)
Development
Support
Limited Support
End Of Support
Customer Responsibilities and Expectations

Design devices under a secure development framework.

MDM communicates End of Life and timeline for End of Support to customers with expected support to be provided until date is reached.

Customer begins planning for activities and end of support as communicated from MDM.

Full transition of responsibility from MDM to customer (no further support provided).

Medical Device Manufacturer (MDM) follows regional guidance for medical device responsibilities, support levels may vary and as agreed upon with customers.

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

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 its life cycle. Another outcome of development 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

5.2 Support (Stage 2)

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

1. Used for providing patient care;
2. Containing major software, firmware, or programmable hardware components (e.g., CPU) which are all supported by their developers[1]; and,
3. Which may or may not be currently marketed and sold by their respective MDMs.

Stage 2 devices should receive full cybersecurity support such as software patches, 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 integration 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.

In all cases, devices in stage 2 offer the best opportunity for manufactures and providers to establish and implement support practices. 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.).

Some Stage 2 practices may carry over into later stages of the legacy progression, while others may be succeeded by another practice.

5.3 Limited Support (Stage 3)

Devices within the Limited Support stage (stage 3) are defined as devices still used for providing patient care that:

1. Have been declared EOL by the MDM and are not currently marketed or sold by their respective MDM; or,
2. 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

[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

effectiveness **are** 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 as 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 patches where possible.

Devices in this category may exhibit a wide range of security integration 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 section.

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. However, 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 devices still used for providing patient care that:

1. Have been declared EOS by the MDM and are not currently marketed or sold by their respective MDM; or,
2. 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 they can no longer assure support for devices before entering 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 Phases

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 3rd 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 3rd party software component is known in advance, the MDM should have appropriate plans in place to address the risk from the component’s phase transition in the device design. To manage the risks that may arise from sudden, desynchronized EOL/EOS declarations and statuses, MDM's may leverage the following framework for assessing risks that may trigger transition to different life cycle phases:

i. 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.
    - If there are no patient safety impacts, then the device remains in the current life cycle phase (i.e., support or limited support) phase and the end user is made aware the component has gone EOL/EOS.

ii. If there are patient safety impacts and the device is in the Support phase, MDMs should attempt to mitigate the risk of the unsupported component via an update or other design change. When in the Support phase, 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 decision whether a phase transition is appropriate at this time.
    - 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 phase
    - If the risk is mitigated such that the device may be reasonably protected but the mitigation includes unsupported components, transition to Limited Support. Use of a mitigation which leverages unsupported components is not considered best practice and should be a last resort. MDMs are expected to publicly communicate this transition (see section 8.1.1e for additional specifics regarding this communication) and provide the more detailed security documentation needed to facilitate the transition (see section 8.1.1)

iii. If there are patient safety impacts and the device is in the Limited Support phase, 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 sector, should inform whether a phase transition is appropriate at this time.
    - If the risk is mitigated such that the device may be reasonably protected, the device may remain in the limited support phase and the end user is made aware the component has gone EOL/EOS
    - 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 9.1.1b for additional specifics regarding this communication).

The framework above is intended for sudden 3rd party component EOL/EOS declarations. Generally, the software level of support provided for device maintenance is articulated in the device maintenance plan and the software component's EOS date may also be included in the SBOM.

6.0 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 missing 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 points of a device's TPLC.

6.1.1 MDM Recommendations

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

a. **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 the use of a secure development framework. Appropriate areas of controls, and specific recommendations, may include:

    i. Security design and controls based on the intended use of the medical device, as well as:
    - Security risk assessments
    - Threat modeling
    - Security testing
    - Customer facing product security documentation and communication

    ii. Post-market monitoring of cybersecurity vulnerabilities capabilities, such as:
    - Identification of vulnerabilities
    - Vulnerability risk identification based on the device security design, controls, and mitigations.

    iii. Ensuring availability of security patches and mitigations based on device risk, such as through:

- Coordinated and clear communication to all affected users with regard to the vulnerability and its corresponding mitigations
- Identification of 'other' mitigation options when a security patch is unavailable.

b. **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 are no transfer of responsibility recommendations at this stage because the MDM has not provided a device to the HCP.

7.0 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 phase of a device's life cycle to ensure ongoing secure operations. Specifically, it is critically important that communications during the Support stage are comprehensive and routine to support robust risk management activities by all parties. 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.

7.1.1 MDM Recommendations

a. **Provide Product Security Documentation**- MDMs should provide product security documentation to enable HCP risk management during procurement and deployment of medical devices. Appropriate documentation may include:

   i. Manufacturer Disclosure Statement for Medical Device Security (MDS2);
   ii. Software Bill of Materials (SBOM);
   iii. Security test reports (e.g., penetration testing) or third-party security certification;
   iv. 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).

b. **Provide Product Life Cycle Documentation-** MDMs should communicate clearly on the key life cycle milestones, including cybersecurity limited support and EOS dates of devices as part of procurement and installation processes. 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 directly (see section 7.2.1(c) for additional information on postmarket expectations). If not provided at procurement and installation, best practice is to provide this information 2-3 years in advance of EOL/EOS as appropriate. MDMs can support HCPs and other customers by clearly communicating the following information:

  i. affected device
  ii. the device's operating system(s)
  iii. device instances the customer has deployed
  iv. identification of software components
  v. expected date of service changes
  vi. the extent of any available maintenance after those changes
  vii. additional compensating controls

c. **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 to HCPs to enable them to adjust their risk management strategies as needed to respond to new or changed risks.

d. **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.

e. **Provide Proactive Communications for 3rd Party Components-** It is possible that the software and other digital components within a medical device will reach of 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:

  i. Track the support status of the 3rd party components used within their device

ii. Assess the risks that may exist if and when those 3rd party components become unsupported

iii. Communicate the risks and any recommended mitigations to HCPs

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

7.1.2 Healthcare Provider Recommendations

a. 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.

i. 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 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.

ii. 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 and MDMs should proactively identify when responsibility for the risk of using an unsupported device transfers from one party to the other.

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

i. EOL date (if known)
ii. EOS date (if known)
iii. Upgrade strategy for device software components (e.g., operating system, third party software, application software)
iv. Transfer of responsibility from shared accountability (MDM and HCP) to HCP is updated during the life of the device
v. Ports and services necessary to the device to function appropriately
vi. Firewall rules that can be leveraged to isolate the device and maintain function
vii. Anti-malware capabilities and appropriate definitions (what can be scanned)
viii. Security scanning capabilities and appropriate scanning definitions (how to scan)
ix. Security logging capabilities

x. Device backup and restore procedures
xi. Notification method to receive vulnerability notifications
xii. Administrative accounts and the ability to manage through a privilege access management tool

c. **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. Areas of communication include:

i. Risk rated vulnerability disclosures, with updates as appropriate, through a push mechanism to appropriate HCP contacts
ii. Mitigation recommendations to control risk of known vulnerabilities
iii. Indicators of compromise to be looking for on the device or through passive monitoring of traffic
iv. Updated SBOM throughout the device's life cycle in machine readable format
v. Options to address outdated software components (i.e., operating system, third party software) one year prior to reaching end of support

7.2 Risk Management

7.2.1 MDM Recommendations

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

i. Even when an unsupported component has exploitable vulnerabilities, there can be other compensating controls within or outside of 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.

b. **Guidance to HCPs:** When the medical device approaches the EOL date, the MDM should provide clear guidance 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 (a-f), 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.

c. **Postmarket expectations:** There are certain activities that MDMs are expected to complete in the postmarket for devices and these expectations apply to the TPLC for medical device cybersecurity. Specifically, these expectations are:

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

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

   iii. Performing field safety corrective actions if necessary (e.g., recall, modification, change IFU, etc.) In some cases (e.g., depending on the life cycle stage), the MDM may not take a formal action, they might just communicate

   iv. 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)

   v. 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)

d. **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 after EOL (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, and 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, the HCP will need to take increased responsibility for implementing security measures around devices.

a. **Baseline Security Considerations-** While MDM baseline security recommendations are most relevant during the Development stage, for HCPs, baseline security recommendations become critically relevant during the Support stage. Baseline security recommendations for HCPs may include:

i. Network security controls are applied to devices by assessing the importance and criticality of devices through a risk assessment process:
ii. Critical devices identified through the risk assessment process almost always require additional network and physical controls and regular monitoring.
iii. Maintaining active communication with MDMs for support and patching recommendations.
iv. Employing configuration management to identify all current assets and track future configuration changes.
v. Maintaining IT security monitoring and patching processes that support cyber hygiene and vulnerability remediation.
vi. Protection from unauthorized access through logical and physical security controls.
vii. Cybersecurity training and awareness programs.
viii. Vulnerability Management

b. **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 here.

c. **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 devices 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.

d. **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 deprecates 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.

e. **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.

f. **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 devices 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 behavior.

   - *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 behavioral information.

g. **Inventory Considerations:** Proactive planning for EOS begins when the device is installed. 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:

   i. Current life cycle stage

   ii. Expected EOS date

   iii. SBOM

   iv. Vulnerability status & software patch status

   v. Operational environment (network diagram)

   vi. 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 EOS and after it, should the HCP understand and accept the risk to continue using the device, regular clinical benefit/risk analyses comparing the use of the legacy device past its EOS date with risk compensation measures versus purchasing a new or upgraded device should be considered.

h. 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:

i. Development, upkeep and upgrading of IT infrastructure

- 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.

ii. Acquisition and Use of SBOMs

- 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. This 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.
- 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.
- As a device approaches EOL and EOS, 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.

iii. Integration and installation of any new device on the network

- 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.

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

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

i. **Decommissioning Considerations:** IMDRF N60 guidance section 6.6.2 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. This section provides recommendations for both MDM's and HCP's responsibilities and expectations for this life cycle transfer of responsibility which have been divided based on the TPLC (i.e., support, limited support, and End of Support phases) when the medical devices are being procured and deployed in the healthcare premises.

7.3.1 MDM Recommendations

a. **Timeline Considerations:** As a best practice, the transfer process to move cybersecurity responsibilities to the HCP's begins approximately 2-3 years before the End of Support. This 2-3 year notice allows the HCP to evaluate, plan and budget for equipment replacements.

b. Pathway to transition to new/upgraded 'supported' device: Before the Support phase 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:

   i. Detailed information on Medical Device(s) impacted by the EOL and eventual EOS
   ii. 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

At this time, the HCP may want to consider the following:

a. Whether they think they are capable of managing the device
b. Whether support from a 3rd party may be available to help manage the device

c. Are the devices worth replacing?
d. What resources (if any) are available to support device replacement?

8.0 Limited Support Life: 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 escalates during this life cycle phase. Specifically, the type and granularity of information provided increases to enable HCPs to better understand the risk they are inheriting.

8.1.1 MDM Recommendations

a. Continue to provide services and documentation from the communications “Support” life cycle phase (Section 7.1.1 a-f) as far as it is practical and appropriate. This includes vulnerability communications.

b. 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:

i. Alerts indicating that some maintenance has stopped when parts of the medical device (i.e., device software) are no longer supported
ii. Security notifications and advisories
iii. Device-specific information advisories about compensating controls
iv. Any intended use restrictions which result from phase changes

c. Provide Product Security Documentation- On top of providing the recommended security documentation in “Support” life cycle phase (Section 7.1.1 a and c), MDMs should provide the following documentation:

i. Updated security documentation that indicates any compensating controls that are recommended given the reduced support which may include:
   - Firewalls
   - VPNs;
   - Whitelisting;
   - Network Isolation

ii. Expectations for device deployment environment.

d. **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/phase out and business continuity planning for HCPs.

e. **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 and when the device moves to a different stage, so that relevant parties—including resellers and organizations potentially looking to purchase devices secondhand—may understand the potential risks of continuing to use such devices.

8.1.2 Healthcare Provider Recommendations

Communications from 7.1.2(c) 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 (a-e)). As HCPs may be evaluating whether to purchase resold or secondhand 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 life cycle phase in Section 7.2.1. However, the frequency and therefore level of effort associated with proactive vulnerability management as a part of risk management activities may decrease.

8.2.2 Healthcare Provider Recommendations

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

i. Research whether the desired device is in EOL/EOS

ii. If it is, HCPs should carefully consider the risks of using an EOL/EOS device

iii. 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.

b. **Considerations for HCPs when approaching EOS:** After EOL, when the MDM's EOS date is approaching, both through active communications from the MDM and through notifications from the inventory management systems, it is recommended that the healthcare delivery organization consider the following questions (non-exhaustive list) to help identify if the risks of operating the device without support are adequately controlled:

i. What time frame beyond the expected service life is the device projected to be used for clinical care?
ii. Will there be maintenance costs over the time period the device is projected to be used for clinical care?
iii. How do the maintenance costs compare to upgrading the device?
iv. How could a new or upgraded device improve clinical care while also improving cyber resiliency?
v. Does the HCP have the tools to maintain the security of this device?
vi. Does the HCP have the financial resources to maintain the security of this device?
vii. Does the HCP have the expertise to maintain the security of this device?
viii. What would be the risk to patients should this device be compromised?
ix. What would be the risk to patients should the organization be compromised due to this device?
x. What would be the risk to patients should this device not be used and replaced by an alternative?
xi. Can this device operate beneficially without being connected to the network?
xii. What other controls can be put in place?

8.3 Transfer of Responsibility

This phase 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.

a. 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).

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

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

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

e. Available product security documentation (including SBOM)

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

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

   i. H/W component replacements if available (e.g., monitor replacement, cabinet, hardware disk drive, etc.)

   ii. Reloading s/w, restoring device system state.

   iii. 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.

- **a.** Cybersecurity monitoring for the device.
- **b.** Vulnerability management
- **c.** Implementation of compensating controls, including physical and logical access controls
- **d.** Ensuring the deployment environment is appropriate for adequately securing the EOS device.
- **e.** Implementing an incident response plan
- **f.** Establishing a business continuity plan
- **g.** Conducting regular risk assessments as outline within the HCP's Risk Management Process.

9.0 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.

9.1 Communications

9.1.1 MDM Recommendations

During this phase, the HCP should already be informed that its medical device has reached the "End of support" life phase, having been made aware in advance of the EOS date. At this phase, 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.

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

b. **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 secondhand—may understand the potential risks of continuing to use such devices.

c. **Communicate risks received as part of postmarket 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 (a-c)). As HCPs may be evaluating whether to purchase resold or secondhand 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

MDMs should continue actions related to post market expectations (section 7.2.1(c)i-iii and 7.2.1(c)v). However, the field safety corrective actions mentioned in 7.2.1(c)iii may be limited (e.g., consist primarily of communication to the end user). Yet if there is a significant risk to patient safety such as in a WannaCry type scenario, there may be a need for additional reactive risk management actions as a part of vulnerability management such as those highlighted in section 7.2.1(c)v.

9.2.2 Healthcare Provider Recommendations

a. **Consider EOL/EOS Risks When Evaluating Whether to Purchase Resold or Secondhand Device** as described in 8.2.2(a)

b. **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:

i. Ensure the implementation of a strong, talented, appropriately resourced (i.e., resource to manage increasing risk), cybersecurity program that has endorsement from senior leadership;
ii. Ensure the implementation of a robust inventory management system, with automation if possible;
iii. Include the legacy device in on-going organizational risk management activities;
iv. Proactively monitor trusted sources of information such as Information Sharing Analysis Organizations, Information Sharing and Analysis Centers, dissemination agencies such as Computer Emergency Response Teams (CERTs), regulators, vulnerability databases (e.g., those for third-party components), etc.;

v. Enhance countermeasures including but not limited to: network segmentation, user access roles, security testing, network monitoring, disconnection from the network; and

vi. Periodically evaluate alternative products available and revisit the decision to operate a device past its EOS.

9.3 Transfer of Responsibility

9.3.1 MDM Recommendations

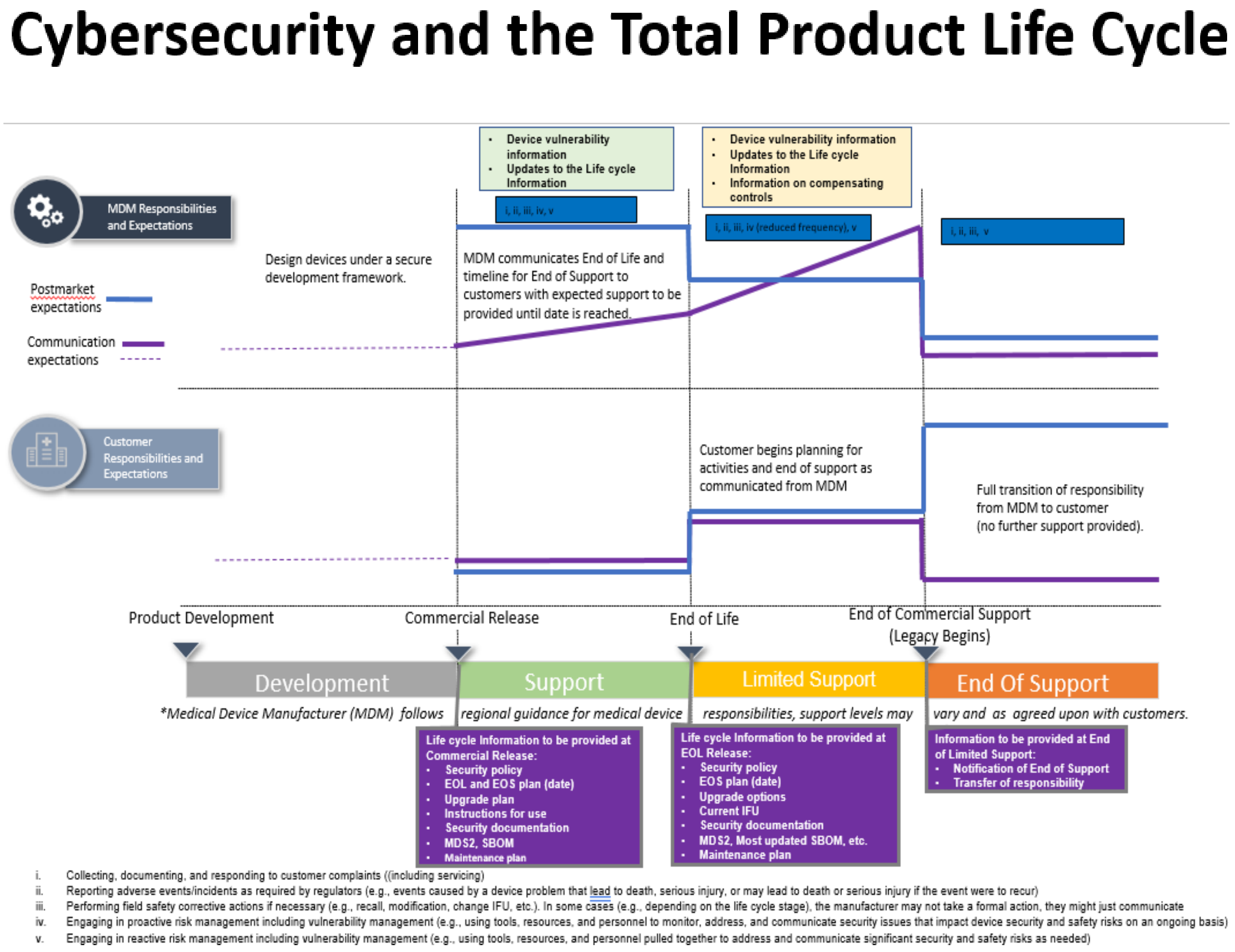
At this stage, the transfer of responsibility to the end user is complete. MDMs have communicated that the device is EOS and that there has been a transfer of responsibility.

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.

10.0 Summary of Cybersecurity TPLC Responsibilities/Expectations

Sections 6-9 above, provide additional granularity on the responsibilities and expectations for MDMs and HCPs within the context of four (4) TPLC stages: 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 in the postmarket for devices across the TPLC for medical device cybersecurity. A summary cybersecurity TPLC figure (Figure 2) is provided below which 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

MDM Responsibilities and Expectations

Postmarket expectations

Communication expectations

Design devices under a secure development framework.

- Device vulnerability information
- Updates to the Life cycle Information

i, ii, iii, iv, v

MDM communicates End of Life and timeline for End of Support to customers with expected support to be provided until date is reached.

- Device vulnerability information
- Updates to the Life cycle Information
- Information on compensating controls

i, ii, iii, iv (reduced frequency), v

i, ii, iii, v

Customer Responsibilities and Expectations

Customer begins planning for activities and end of support as communicated from MDM

Full transition of responsibility from MDM to customer (no further support provided).

Product Development

Commercial Release

End of Life

End of Commercial Support (Legacy Begins)

Development

Support

Limited Support

End Of Support

*Medical Device Manufacturer (MDM) follows regional guidance for medical device responsibilities, support levels may vary and as agreed upon with customers.

Life cycle Information to be provided at Commercial Release:
- Security policy
- EOL and EOS plan (date)
- Upgrade plan
- Instructions for use
- Security documentation
- MDS2, SBOM
- Maintenance plan

Life cycle Information to be provided at EOL Release:
- Security policy
- EOS plan (date)
- Upgrade options
- Current IFU
- Security documentation
- MDS2, Most updated SBOM, etc.
- Maintenance plan

Information to be provided at End of Limited Support:
- Notification of End of Support
- Transfer of responsibility

i. Collecting, documenting, and responding to customer complaints ((including servicing)
ii. Reporting adverse events/incidents as required by regulators (e.g., events caused by a device problem that lead to death, serious injury, or may lead to death or serious injury if the event were to recur)
iii. Performing field safety corrective actions if necessary (e.g., recall, modification, change IFU, etc.). In some cases (e.g., depending on the life cycle stage), the manufacturer may not take a formal action, they might just communicate
iv. 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)
v. 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)

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

11.0 Considerations regarding compensating controls after EOS for a Medical Device

A compensating risk control measure 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 us 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 the device operational, it should consult the product security documentation provided by the MDM during the Limited Support and EOS phases 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 X contains general recommendations for compensating controls and while these recommendations are provided in the context of EOS, they may also be applicable before EOS. Feasibility of implementation will depend on the specific device and its operating environment and may 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.
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. 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 X: 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-educated 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 behavior (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.

12.0 References

12.1 IMDRF Documents

1. Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020 (April 2020)
2. Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations IMDRF/SaMD WG/N12:2014 (September 2014)

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

12.2 Standards

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

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

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

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

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

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

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

11. 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

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

13. 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

14. 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

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

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

17. 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

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

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

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

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

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

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

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

25. 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

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

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

28. 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)

29. 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)

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

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

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

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

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

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

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

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

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

39. MDCG 2019-16 - Guidance on Cybersecurity for medical devices (December 2019
July 2020 rev.1)

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

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

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

12.4 Other Resources and References

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

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

45. 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

46. NIST Special Publication 800-12 Rev 1 Introduction to Information Security (June 2017)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

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

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

49. MITRE CVSS Healthcare Rubric
https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

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

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

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

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

54. 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

55. Medical Device Coordination Group (MDCG) 2019-16: Guidance on Cybersecurity for medical devices https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native