Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Manage Risks

Secure Medtech

Health Industry Cybersecurity

Managing Legacy Technology Security (HIC-MaLTS)

MARCH 2023

Table of Contents

I. Foreword – Use of "Technologies" versus "Devices"

When the HSCC Legacy Task Group was originally instantiated, it was focused on legacy medical devices in particular as a source of risk. The group was called, in fact, the Legacy Devices Task Group.

However, devices are only a subset—a large and critically important subset, but a subset nonetheless—of the technologies within healthcare environments that can become legacy, and can pose legacy related cyber risks. To fully manage cyber risk in a modern healthcare environment, HDOs must consider FDA regulated devices, non-FDA regulated devices, laboratory equipment, building and facilities technologies, mortuary equipment, general information technologies, and many more. And because these technologies also age, becoming more vulnerable and/or unsupported, the same legacy pressures traditionally identified as affecting medical devices also affect these other technologies. Consequently, as the work continued, the group began considering legacy cyber risk in the broader context of "technologies," and not just devices.

The recommendations made in the document are largely focused on one of two sets of stakeholders: Medical Device Manufacturers (MDMs) or Healthcare Delivery Organizations (HDOs). At face value, then, they leave out these other, non-regulated medical device technologies.

However, the recommendations can and should be considered more broadly:

- For HDOs in particular, the vast majority of the recommendations—especially those related to supplier management—can be leveraged to apply not only to processes, practices, and procedures for working with MDMs specifically, but other technology providers as well.
- For MDMs, many of the supplier management recommendations may be useful when applied to their own technology providers, as well as their manufacturing environment and remote support infrastructure.
- For other technology providers, the MDM design and risk management recommendations may be useful in designing, deploying, maintaining, and eventually

declaring “end of life” of their various products, where those products may be used in a healthcare setting.

With this in mind, and in recognition that effective healthcare cyber risk management must consider technologies far beyond devices, the Task Group decided to use “technologies” rather than “devices,” with devices included as a type of technology used in healthcare environments. It encourages readers and users of this document (HIC-MaLTS) to do the same.

II. Introduction

Cyber threats to the healthcare sector are a well-documented reality of modern healthcare delivery. Ransomware attacks against hospitals, clinics, service providers, and other healthcare delivery organizations (HDOs) routinely deny access to patient records, billing systems, and other digital technologies deployed throughout modern healthcare environments. Vulnerabilities discovered in the digital infrastructure relied upon by modern healthcare delivery organizations (HDOs) to deliver quality care pose patient safety and privacy risks that include delay or denial of treatment, manipulation or corruption of necessary treatment or other digital healthcare data, and the risk of intentionally or unintentionally tampered software, among other potential risks. And the massive and increasing complexity of today’s connected healthcare ecosystem gives rise to its own risks: of unanticipated and poorly understood interdependencies; of unknown inherited security weaknesses; of overreliance on vendor solutions; of systems that fail to adequately account for human factors related to cybersecurity controls; and of inconsistencies between software and equipment lifecycles, among others. As a result, technology changes faster than security, and boundaries are blurred.

In addition, the healthcare sector itself is evolving through the adoption of digital consumer wellness and fitness technologies, as well as the shift towards remote care models, which were greatly accelerated by the COVID-19 pandemic. As a result of these drivers, healthcare now frequently occurs outside of hospitals and clinician offices. Telehealth, remote care, and home health are all driving the integration of healthcare technologies with, for example, patients’ home networks, and require transmission of data across uncontrolled networks (home, public) and cloud services. Further, valuable data that can be derived from personal lifestyle devices (e.g., fitness trackers, smart watches) can now augment clinical data and decisions. Ensuring that a hospital or clinician’s office is “cybersecure” alone is no longer sufficient; modern care

delivery requires that all disparate pieces of the evolving healthcare ecosystem be considered, and appropriately secured as well.

But while the healthcare sector is embracing these advancements, and continuously evolving to bring more and better care to patients, it faces a very real, and very complex challenge from its past: legacy technologies. As now recognized by the International Medical Device Regulators Forum (IMDRF), and in this document, "legacy" technologies are those devices, IT systems, programs and applications, and other technologies present in healthcare environments, which cannot be reasonably protected against current cyber threats[1]. Many legacy technologies may present risks that cannot be sufficiently mitigated (e.g., patched or otherwise updated) to address cyber threats, as current best practices recommend. Others contain insufficient, poor, 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. In organizations lacking the staff and resources to routinely refresh their infrastructure, which is not uncommon, these legacy technologies and their associated risks can persist indefinitely.

Legacy technologies in healthcare are a proven risk to the sector. They have been repeatedly identified as root causes in after-action evaluations of security incidents, as pressing policy considerations for the United States Congress, the U.S. Department of Health and Human Services (HHS), and other governmental and private sector bodies to examine, and as continuing and stubborn challenges for both HDOs and medical device manufacturers (MDMs) to manage as they try to stay ahead of modern cyber threats. If the cybersecurity capabilities and resilience of the sector are to be meaningfully improved, legacy technology issues must be addressed.

This document represents the Healthcare Sector Coordinating Council's (HSCC) efforts to do just that. It is the culmination of nearly three years of work by 67 industry and government member organizations including MDMs, HDOs, their trade groups, government representatives, health IT companies, independent service organizations, security consultancies and others—to investigate, evaluate, and propose recommendations to address the legacy technology challenges facing the healthcare sector.

---

1 https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

III. About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's ability to deliver services and assets to the public. The HSCC Joint Cybersecurity Working Group (JCWG) is a standing working group of the HSCC, composed of more than 300 industry and government organizations working together to develop strategies to address emerging and ongoing cybersecurity challenges to the health sector.

IV. Executive Summary

This document is specifically meant to address legacy technology challenges in healthcare. It builds upon and supplements existing efforts and reports such as the Health Care Industry Cybersecurity Task Force Report (congressionally-mandated report on the state of healthcare cybersecurity), the HSCC Medical Device and Health I.T. Joint Security Plan (medical device cybersecurity best practices), and the HSCC Health Industry Cybersecurity Practices publication (healthcare delivery cybersecurity best practices), and others from the HSCC and sector.

Advancements in healthcare delivery to enhance the quality, access, and cost of patient care has led to the constant evolution of medical technologies, coupled with the increasing reliance on interconnectivity to provide access to electronic data, to allow for remote functionality, enhance workflow, outcomes, and more.

In light of this, the discussion that follows takes on common healthcare cybersecurity challenges:

- Similar to many non-healthcare enterprise environments, healthcare networks are evolving beyond the traditional and well-defined protected enterprise networks, to a more 'ubiquitous' environment which extends to third-party (e.g., cloud) providers, non-standard devices, remote device monitoring, insurance providers, and patient telehealth communication;
- Healthcare networks host a significant amount of valuable data, including electronic protected health information (ePHI), payment card information (PCI), and personally

identifiable information (PII), making healthcare networks a target rich environment for cyber threat actors and others;

- The many different types of medical devices and the diverse locations in which they are used possess unique risk profiles and include diagnostic, therapeutic, wearable, implantable, and "software as a medical device" (SaMD) features, among others, that can be used in hospitals, clinics, and other non-clinical/home healthcare settings;
- The use of off-the-shelf (OTS) components and software within medical technologies may result in inconsistent support lifecycles among device hardware and software components of the device;
- Wide variation among organizations in terms of size, capabilities, cybersecurity maturity, and resources contribute to a lack of process maturity within the sector;
- Inconsistency among organizations in providing visibility, communication, and resolution of potential technology vulnerabilities;
- Understanding of shared responsibility for maintaining the security of technologies between Medical Device Manufacturers (MDMs), Healthcare Delivery Organizations (HDOs), and other healthcare stakeholders remains uneven;
- Organizational approaches to technology lifecycle management, where successful execution of legacy technology best practices relies heavily on technology leadership roles (e.g., CTO, CISO), are not guaranteed to exist at every MDM and HDO, resulting in the absence or misalignment of incentives surrounding the replacement of legacy technologies;
- Gaps and deficiencies in investment in comprehensive systems security architecture approaches, engineering best practices and processes, and use case-appropriate security technologies;
- Providers and manufacturers show overreliance on technologies without a full appreciation for the systems-of-systems context in which the solutions will be deployed or how the technologies should be maintained over time, which could result in undesired outcomes such as patient safety risks or security compromises;
- Inconsistent application of existing best practices and slow adoption of improved practices against current cyber threats;
- The variation in resources among MDMs, HDOs, and other healthcare stakeholders requires that effective solutions be scalable across many types and sizes of organizations, particularly smaller providers with limited resources and expertise.

The purpose of this document is to identify the respective and shared responsibilities required of healthcare stakeholders in the security management of legacy medical devices and technologies, and to provide current industry best practices, recommendations, and references for optimizing clinical security and resiliency, and patient safety.

V. Terminology: Definitions and Discussion

It is standard practice for documents such as this one to include terminology sections to help clarify and contextualize its contents. This section accomplishes that goal, but it also accomplishes an additional goal: to overcome challenging terminology discrepancies unique to legacy technologies.

Healthcare technologies, like all technologies, must be regularly replaced as their functionality decreases, support wanes, or newer, more advanced options are released, and as such, those responsible for managing these technologies must have consistent terminology for referring to the different stages of a technology's lifecycle. Over time, many terms have organically arisen to address this need. When discussing legacy technologies, oftentimes phrases such as "end of life," "end of support," "end of guaranteed support," and more are used to describe legacy technologies at these various stages. But these terms are not always used uniformly: one organization's "end of support" might be another organization's "end of life".

This document's terminology section is therefore targeted at identifying the most commonly-known terms relevant to legacy technologies and providing consistent definitions for them. In doing so, this section is meant to help healthcare stakeholders and their partners use the same terminology, in the same ways, to ensure a better common understanding of cybersecurity within the sector.

1

End of Guaranteed Support

EOGS

Point after which the manufacturer no longer guarantees full support.

Note: During this life-cycle stage, there can be some level of support available by the manufacturer, but without a guarantee that the medical device can be maintained to its original specification and performance.

Disclaimer: This term is not identified as one of the IMDRF lifecycle stages.

SOURCE: AAMI TIR97:2019

2

End of Life

EOL

Life cycle stage of a product, starting when (1) the manufacturer no longer sells the product beyond its useful life (as defined by the manufacturer), and (2) the product has gone through a formal EOL process, including notification to users.

SOURCE: IMDRF Principles and Practices for Medical Device Security:2019

3

End of Support

EOS

Point after which the manufacturer has terminated all service support activities.

Note: Service support does not extend beyond this point

SOURCE: AAMI TIR97:2019

4

Healthcare Delivery Organization

HDO

Health care organizations include, but are not limited to, hospitals, nursing homes, limited care facilities, clinics, medical and dental offices, and ambulatory care centers, whether permanent or movable.

SOURCE: EQ56 AAMI

5

Independent Service Organization

ISO

Entities, other than the manufacturer or healthcare establishments, that maintain, restore, refurbish, or repair a finished device after distribution, for purposes of returning it to the safety and performance specifications established by the manufacturer and to meet its original intended use.

SOURCE: FDA Report on the Quality, Safety, and Effectiveness of Servicing of Medical Device

6

Legacy Medical Device (syn. Legacy Device)

Medical devices that cannot be reasonably protected against current cybersecurity threats.

SOURCE: Principles and Practices for Medical Device Security:2020; IMDRF/CYBER WG/N60FINAL:2020

Related: Current Legacy Device

A device which is currently in use within a healthcare environment, and which meets the IMDRF N60 definition of a legacy device.

SOURCE: HSCC Health Industry Cybersecurity-Managing Legacy Technology Security (HIC-MaLTS) (2023) *(this document)*

Related: Future Legacy Device

A device which does not yet meet the IMDRF definition of a legacy device, but will eventually meet the definition as it ages.

SOURCE: HSCC Health Industry Cybersecurity-Managing Legacy Technology Security (HIC-MaLTS) (2023) *(this document)*

7

Medical Device Manufacturer (syn. Manufacturer)

Any natural or legal person with responsibility for design and/or manufacture of a medical device with the intention of making the medical device available for use, under their name; whether or not such a medical device is designed and/or manufactured by that person themselves or on their behalf by another person(s). The term "person" includes legal entities such as a corporation, a partnership or an association.

SOURCE: IMDRF Definitions of the Terms Manufacturer, Authorized Representative, Distributor and Importer:2009

VI. Identifying a Potential Legacy Technology

A legacy medical device is defined by the IMDRF as a device "that cannot be reasonably protected against current cyber threats." That definition can be extended to technologies, e.g., a legacy technology is one "that cannot be reasonably protected against current cyber threats." The IMDRF definition provides a useful, basic description. However, some organizations may struggle to identify a potential legacy technology based upon the definition alone.

Many factors can impact the categorization of a technology as legacy. There is no one-size-fits-all approach to identification. Still, there are guiding principles which can help an organization to determine if a technology should be categorized as legacy for the purposes of this document.

A. For Healthcare Delivery Organizations (HDOs)

An HDO may find a potential legacy technology deployed within their environment if the technology:

- is past the manufacturer-declared EOL/EOGS/EOS,
- contains a critical software component (e.g., operating system) which is not supported,
- composed of one or more software components that, as could be determined by the software bill of materials (SBOM), are no longer supported and/or has/have reached EOL/EOGS/EOS,
- discovered through pen-testing or other process,
- there is a breach of the network / technology.

In addition, the complexity in managing the risk for the technology may be significant (time, resources, etc.) and should be accounted for in the lifecycle management plan.

B. For Medical Device Manufacturers (MDMs)

An MDM may find a potential legacy technology (including medical devices) within their portfolio if the technology exhibits one or more of the following characteristics:

- One or more software components (custom or off-the-shelf) no longer receive support;
- One or more hardware components (e.g., programmable logic, CPU, where the components can be custom or off-the-shelf) no longer receive support;
- Technology firmware no longer receives support;
- The technology contains known, exploitable vulnerabilities with limited mitigations;
- The technology does not have a mechanism to update software, firmware, and/or programmable logic.

It is important to remember that the characteristics outlined above are not all-inclusive nor indicative. A technology may exhibit one or more of these characteristics but still operate securely. Conversely, a technology may exhibit none of the listed characteristics, yet still be unable to be protected against current cyber threats. It is important for HDOs, MDMs, and other healthcare stakeholders to work together to evaluate potential legacy technologies and apply the best practices contained within this document.

VII. Core Practices

Management of legacy technologies in healthcare is a multi-faceted challenge. Although the functional or maintenance obsolescence, or even technology safety risks as a result of technology end-of-support, are not new problems, and have occurred and will continue occurring in non-cybersecurity settings, the inclusion of cybersecurity considerations heightens the frequency of such events and increases the urgency of addressing them. And although managing the cybersecurity of technologies is a recognized practice, a technology's legacy status requires additional considerations and often a unique and different approach.

This document details four "core" practices that effective legacy technology cybersecurity programs should incorporate: (1) governance, (2) communication, (3) risk management, and (4) future-proofing.

A. Governance

Governance is commonly understood as the formalized framework of rules and strategies that describe cybersecurity related policies, practices, procedures, education, training, and roles and responsibilities. Governance is generally based on applicable laws and regulations as well as an organization's goals, objectives, and mission. In all cases, to be effective governance activities must be adequately resourced.

Governance of medical technologies across design, development, production, deployment, and utilization are critical to monitoring and sustaining their performance, safety, and security. Governance determines how organizations identify, protect, detect, respond, and recover from cyber incidents.

It enables organizational leadership to:

- define cybersecurity goals and objectives;
- establish responsibilities (duties, privileges, and roles);
- enable accountability, proper supervision, and control;
- ensure information-flow and monitoring of implementations; and
- support compliance and medical technology lifecycle management.

The following subsections describe specific considerations that both HDOs and MDMs should consider when establishing or refining their governance strategies and programs to address legacy technology challenges.

1. HDO Considerations

HDOs benefit from governance that oversees the medical technology lifecycle from procurement to decommission, with an emphasis on cybersecurity risk management. HDOs should work with MDMs or independent service organizations (ISOs) to evaluate the security of technologies and manage risks. Effective governance requires defining a strategy, establishing a model and criteria for risk tolerance, and developing a lifecycle management plan, including an asset replacement roadmap.

a) Defining a Legacy Technology Risk Management Strategy

To properly manage cybersecurity of technologies used in healthcare environments as an enterprise-level imperative for patient safety, data integrity, and operational continuity, organizations should consider establishing a cross-functional Medical Technology Management Committee ("Committee"). The Committee, accountable to the organization's executive leadership, should be engaged in ensuring that medical technology cybersecurity is addressed within clinically relevant infrastructure processes and activities.

Depending on the organization, the Committee may report to a Chief Technology Officer, Chief Medical Information Officer, or other CxO; or, the Committee may have direct responsibility for these activities or serve as a governance body. In all cases, the Committee should be co-chaired at a senior level, involve both technology and clinical leadership, and facilitate cross-functional visibility and decision-making authority.

The Committee stakeholder groups should be holistic and representative of the HDO. It may include stakeholders such as:

- Nurse Managers
- Clinical Department Heads
- Medical Informaticists
- Clinical Engineering/Healthcare Technology Managers (including biomed and hospital service technicians)
- Information technology (IT)/information security (IS) (including cybersecurity)
- Environment of Care Committee Members

Additional stakeholders and partners could include MDMs, ISOs, or other manufacturers who perform multi-vendor services.

The Committee should be responsible for considering legacy technology planning, risk, and mitigation activities throughout the lifecycle of relevant technologies governed by the organization. The Committee may oversee processes and activities such as:

- Procurement requirements
- Risk Assessment and Prioritization
- Incident Response and Business Continuity
- Information Sharing
- Clinical Security Training Programs

- MDM/ISO Partnership Engagement
- Vulnerability Management
- Asset Lifecycle Management
- Disposal and Data Sanitation

Defining a legacy technology strategy should be a primary responsibility of the Committee. See the remainder of this document for recommendations on how to develop such a strategy.

b) Establishing a Model and criteria for Risk Tolerance

An HDO should select criteria to evaluate the cybersecurity of a technology based on their risk tolerance level, infrastructure capabilities, and cost-benefit considerations. Their criteria could determine need for replacement and anticipate future security requirements for the organization.

During cybersecurity risk assessments of a product, and taking into account the context in which that product will be used, it is advisable to use a comprehensive risk assessment approach rather than a pure vulnerability score[2], although the vulnerability score may be one of the input components to the risk assessment.

Traditional versus Cybersecurity Risk Assessments

Traditional risk assessment approaches estimate the Probability of Occurrence and Impact Severity. (*See* e.g. NIST 800-30, ISO 14971)

- Probability of Occurrence measures how likely it is that a certain risk may occur.
- Impact Severity measures the effect of harms, such as patient harm or financial harm, should the risks that are being assessed occur.

As cybersecurity threats have grown and changed, approaches for measuring cybersecurity risk have also evolved. Specifically, modern **cybersecurity risk assessments** recognize that the key factor with respect to cybersecurity threats is "Exploitability," rather than Probability of Occurrence. Exploitability estimates how easy it would be for an actor to exploit the vulnerability based upon that actor's skill level, proximity to the vulnerable device or system (i.e., possibility of remote execution), or evidence of active exploitation.

2 The published vulnerability scores for software components, such as the CVSS score in the National Vulnerability Database, are generated as a measure for the severity of a vulnerability and should not be used alone to assess risk. Such score describes only the intrinsic characteristics of a vulnerability and should be supplemented with a contextual analysis of the environment and with attributes that may be different and change over time. A comprehensive risk assessment system should be employed that considers factors in addition to standardized scores like CVSS and that may be specific to the implementation and/or use context. Further, this context may or may not be entirely applicable to the risk analysis of a new or different product that attempts to leverage knowledge of prior vulnerabilities to assess its own cybersecurity posture. Therefore, using a device-specific safety and security risk assessment process(es) is generally advised.

Various scales and methodologies for cybersecurity risk measurement are in use, but most commonly these measures are estimated based on a numeric scale (e.g., 1-4 or 1-5), and then plotted on a two-dimensional matrix and/or multiplied to provide a total score that enables prioritization. Scales may be weighted if needed.

HDOs may wish to familiarize themselves with MDM risk management practices in order to understand how they may influence or affect their own. Common MDM risk management approaches can be found at the following resources:

- A general risk management methodology is described in Chapter 9 of the AAMI Medical Device Cybersecurity Guide for HTM Professionals
- FAIR Institute Risk Model
- OWASP Risk Rating
- Joint Security Plan
- Further HDO guidance on risk assessment can be found in AAMI/ISO/IEC 80001
- Further MDM guidance on risk assessment can be found in AAMI TIR 57 and AAMI TIR 97

Organizations may have developed their own custom risk assessment methodologies over time. Provided that such approaches cover the concepts and considerations outlined by accepted methodologies, organizations may choose to use any risk-focused approach to assess risk.

c) Developing a Lifecycle Management Plan

A lifecycle management plan describes technology lifecycle milestones, such as manufacturer (MDM or other technology provider) declared EOS/EOGS/EOL, and may be used by organizations to help guide their technology management and replacement strategies.

A lifecycle management plan supports processes such as:

- identifying & acquiring technologies
- tracking inventory and managing technology
- planning & implementing risk remediation practices at each lifecycle phase
- planning technology replacement & decommissioning

Process decisions should be made within the context of an organization's overall governance strategy.

2. *MDM Considerations*

MDMs are responsible for remaining vigilant about identifying risks and hazards, including cybersecurity risks and hazards, throughout the total product lifecycle of the medical devices (and, potentially, non-device technologies) that they place into the market. In order to support external stakeholders in protecting patient safety, data integrity, and operational continuity throughout the lifecycle of a legacy device or technology, all MDMs, regardless of size, should have a governance structure that ensures that they can identify and manage legacy cybersecurity issues.

At a minimum, this requires documented policies and procedures that establish, coordinate, and demonstrate compliance with a process for product lifecycle planning, risk management, and mitigation activities with respect to legacy devices and/or technologies.

Some organizations may establish a management team composed of the cross-functional stakeholders within the MDM that may be responsible for providing relevant resources (e.g., personnel and technology), identifying issues, analyzing risks, prioritizing mitigations, designing any fixes, and communicating updates appropriately with internal and external stakeholders. Small or medium organizations may have individuals or teams that perform multiple of these functions. In other scenarios, some functions may be outsourced to strategic partners. Whatever the adopted organizational model, the activities defined below enable adequate handling of identified issues.

MDM stakeholders may include, but are not limited to:

- **Senior Leadership:** Senior leaders have ultimate decision-making authority and are typically the final sign-off on acceptance of risk and any actions that can impact the business. Their engagement in the governance body ensures any potential decision is understood in relation to the full business environment and has leadership buy-in.
- **Software, Hardware, and Firmware Engineers:** Engineers are experts that design, develop, assess, and maintain device or technology software, hardware, and firmware throughout the device or technology lifecycle. They also analyze potential issues and implement design changes. Their product knowledge and process expertise make them critical members of any governance body.
- **Product Security Professionals:** Product security professionals integrate cybersecurity into existing product lifecycle processes and assist product development teams with the implementation of cybersecurity.

- **Product Safety Professionals:** Product safety professionals assess potential safety implications of a security risk.
- **Quality Assurance (QA) and Regulatory Professionals**: QA and regulatory professionals assist in quantifying the impact of the issues to patient safety, product efficacy, and understanding requirements mandated by regulatory bodies. This knowledge ensures organizational governance bodies understand the implications any decisions have on patient safety and efficacy.
- **Information Technology Professionals:** IT professionals often engage directly with customers to support devices and technologies, and to deliver design changes. They also manage the organization's IT infrastructure, which may be impacted by product cybersecurity issues. Their involvement in the governance body ensures any decision takes into account the impacts to the business's IT infrastructure.
- **External Partners:** External partners can provide unique knowledge and perspectives to a governance body when they are included. For instance, Information Sharing and Analysis Organizations (ISAOs) can alert the governance body to potential threats before the organization might otherwise become aware. Additional stakeholders and partners including HDOs, ISOs, security researchers, and other third-party service providers could leverage Coordinated Vulnerability Disclosure programs (CVDs) of MDMs.

B. Communications

In a successful cybersecurity program, successfully managing cybersecurity risk requires robust, ongoing, and comprehensive communications between stakeholders. To ensure this occurs, the policies and procedures for ongoing communications between stakeholders need to be identified upfront (i.e., at technology procurement) and supported during the lifecycle of the technology. For example, it is critical that organizations agree:

- who should be communicating
- what they should be communicating
- when they should be communicating, and
- to whom they should be communicating to, i.e., which organizations and to whom within the receiving organization.

These decisions may be driven by considerations such as who owns the relevant technologies, and who needs to be included or informed in cyber risk management activities (see Governance, HDO Considerations, Defining A Strategy, and Governance, MDM Considerations for more information/recommendations).

For legacy technologies, it is important to inform those responsible for the integration and management of technology into the network about dependent technologies and data streams. Supplying a message to the wrong stakeholder can delay needed action and increase risks to impacted organizations or stakeholders.

- When MDMs communicate to HDOs, each type of communication (new product, alerts/recalls, upgrades, vulnerabilities, etc.) may have diverse stakeholder groups of individuals within the HDO.
- When HDOs communicate to MDMs, each type of communication (cyber assessments, vulnerabilities, upgrades, incident reports, etc.) may also have diverse stakeholder groups.

Proactively defining these types of communications and the stakeholder groups ensures that critical actions are seen by the right people promptly.

Further recommendations for communication policies and procedures can be found in ISO/IEC 29147:2018 and ISO/IEC 30111:2019.

1. *Considerations for Legacy Technology Communications*

Cybersecurity risks may impact multiple parties simultaneously, and may require joint action. It is important for HDOs, MDMs, and other healthcare stakeholders to understand each other's expectations and capabilities to best establish effective communications.

Communication considerations for an effective cybersecurity program can include:

- PHI/PII protections and ownership;
- Coordinated Vulnerability Disclosure programs;
- Security and supply chain documentation;
- Vulnerability management;
- Security and Privacy Agreements;
- Intellectual property protections;
- Licensing; and,

- Technology lifecycle information.

Other communication topics may be necessary as determined by the organization and its governance body.

Recommendations for model contract language covering these and other critical commitments between and HDO and MDM may be found in the HSCC Model Contract-Language for Medtech Cybersecurity (MC2) resource.

a) PHI/PII Protections and Ownership

Discussions about roles and responsibilities for access, management, and destruction of data that may be considered protected health information (PHI) or personally identifiable information (PII) should be well understood by both parties. In cases where a technology that transmits, stores, processes, and/or interacts with sensitive data is purchased, once the technology ownership transfers to the HDO, typically the HDO is responsible for ensuring the integrity and security of information on the technology including PHI and PII.[3] HDOs, MDMs, and other relevant healthcare stakeholders (including non-device technology providers) should have these conversations at or before the time of purchase.

When negotiating the purchase of a technology between parties, organizations should include language that addresses areas such as the removal of PHI/PII, passwords, and storage media, and remote access as well as the communication process that will occur at the time that the MDM or technology provider is going to move the product into EOS/EOL status.

To best position the parties to appropriately negotiate and assign responsibilities for PHI/PII protections and ownership, MDMs should describe processes in customer-facing documentation as appropriate that provide HDOs with the ability to monitor, audit, and remove sensitive data, such as PII or PHI, on relevant technologies. This allows HDOs to manage the lifecycle of the PHI/PII, including removal prior to retiring the technology from service. In situations where the technology ownership does not transfer to the HDO (e.g., leases, rentals, loaners, demo units etc.), proactively defining who is responsible for the monitoring, auditing, and removal of sensitive data on the technology during its life is paramount to assuring data security and privacy.

[3] However, MDMs and other technology providers should design their technologies and provide sufficient information to the HDOs to support this responsibility.

If HDOs have service providers or ISOs hosting or supporting technologies processing or storing sensitive data (e.g., XaaS arrangement), depending on the work performed, applicable laws and regulations, and/or the level of access to sensitive data, organizations may be required to have a HIPAA Business Associate Agreement (BAA) or Data Processing Agreement (DPA) signed with the service provider. Note that a BAA/DPA is typically not required to cover the possibility of an incidental exposure of sensitive data.

Further, to specifically address medical device cybersecurity risks as part of the vendor or service provider agreement, HDOs may use a formal Responsibility Agreement to help define security roles and responsibilities for all parties (see AAMI/ISO/IEC 80001-1).

It is best practice for HDOs to have policies and procedures for removing sensitive data on a technology prior to it leaving their facility, both in instances of repair (shipping a unit out of the facility for maintenance), as well as when the technology is being permanently retired from service. The steps necessary to ensure this data security must be provided by the MDM as part of the labeling. For cloud-hosted data, whether the technology leveraging the relevant cloud is owned by the HDO or not, discussions about responsibility for destruction or anonymization of data not on-site (in a cloud) must also be undertaken. It may be the responsibility of the HDO to ensure the data is destroyed, but it may be the MDM that will actually conduct the destruction.

b) Coordinated Vulnerability Disclosure Programs

Coordinated Vulnerability Disclosure Programs allow third parties to disclose vulnerabilities in hardware, software, and services directly to the vendors of the affected product. As medical technologies age and become legacy, they need to continue to be monitored for vulnerabilities and patched if possible. Through the implementation of a Coordinated Vulnerability Disclosure (CVD) program, MDMs and other technology providers can coordinate vulnerability disclosure, remediation efforts, and public communication to reduce risk to an acceptable level.

Through a coordinated program, CVD adds another layer of due diligence to the way organizations manage vulnerabilities.

Organizations that don't establish and maintain CVD programs risk having cybersecurity incidents and vulnerabilities publicly disclosed prior to mitigations or remediation strategies being ready for their organization and their customers. Consequently, it is highly recommended that organizations establish CVD programs to help manage cybersecurity and legacy technology communications.

The following resources may assist organizations in establishing or further refining their CVD programs:

- https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf [NTIA document(s)]
- HSCC Medtech Vulnerability Communications Toolkit (MVCT)
- ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure
- ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes
- Medical Device Innovation Consortium, October 2018, Medical Device Cybersecurity Report: Advancing Coordinated Vulnerability Disclosure
- Healthcare & Public Health Sector Coordinating Council, Medical Device and Health IT Joint Security Plan (JSP) (Section VII.C.iii)
- International Medical Device Regulators Forum, March 2020, Principles and Practices for Medical Device Cybersecurity (Section 6.3)
- Health Information Sharing and Analysis Center, September 2020, Medical Device Cybersecurity Lifecycle Management (Section 4.3)
- CMU/SEI-2017-SR-022: The CERT Guide to Coordinated Vulnerability Disclosure

c) Security and Supply Chain Documentation

Security and supply chain related documentation are valuable considerations that can play a role in technology pre- and post-procurement risk management. While it may be ideal to obtain such information for legacy technologies, it may not always be practically feasible for the MDM or other technology provider to furnish it. If this information is desired, HDOs should discuss if and how security and supply chain related documentation may be created and obtained from the MDM or other technology provider.

MDS² Forms

One such document is the Manufacturer Disclosure Statement for Medical Device Security (MDS²). This is a standardized form intended to be filled out and maintained by MDMs to communicate information about their devices' security and privacy characteristics to not only current device owners but also potential buyers, typically HDOs. Currently, many MDMs provide MDS² forms upon request.

Software Bills of Materials (SBOMs)

Another useful artifact related to software supply chain transparency is the Software Bill of Materials (SBOM). An SBOM is a formal inventory of software components, including information about those software components. SBOMs provide a transparent mechanism to manage the security risks of the software supply chains by enabling faster identification and response to vulnerabilities, towards the goal of reducing the feasibility of cybersecurity attacks. For reference, the MDS² form contains a question asking whether a product has an associated SBOM.

An item to consider tracking within the SBOM is EOL and/or support status information. While current industry-accepted baseline SBOM formats do not include a recognized "minimum element" for EOL or support status information (either separately or in combination), given the universally-understood connections between increased cybersecurity risk and out-of-date or otherwise unsupported software, organizations may wish to negotiate with vendors about information on EOL of SBOM components as supplemental documentation.

Information contained in the MDS² and SBOM can aid healthcare organizations in the technology procurement process as well as in their risk management. It should however be noted that harnessing their benefits requires a thorough understanding of the information supplied and how it can be put to practical use. Specific recommendations for leveraging SBOM and supply chain documentation can be found in Section VIII.E.

d) Vulnerability Management

For all technologies, the responsibility and mechanics of vulnerability management must be agreed upon and well-understood. When negotiating these roles and responsibilities, organizations should consider:

- How is the responsibility for monitoring the technology, including its hardware and SBOM, for disclosed vulnerabilities shared, and how is this responsibility documented?
- On what interval are these vulnerability discovery and remediation cycles expected to occur?
- Who performs remediation activities such as patching, and how are those efforts documented?
- When critical, actively exploited vulnerabilities are discovered, how does remediation occur, and on what timeline?

The cadence of these activities should be established early in the technology acquisition process and retrofitted into the lifecycle of existing technologies that lack definition in these areas.

With respect to patching considerations, Section VII.C.4in the Cybersecurity Risk Management section, and Section VIII.F in the Challenges & Recommendations Section goes into more detail.

e) Security and Privacy Agreements

To help define roles and responsibilities between themselves and their partners, HDOs and MDMs should adopt security and privacy responsibility agreements based on business and legal requirements, including Business Associate Agreements (BAAs), Data Processing Agreements (DPAs), and Responsibility Agreements (per ISO/IEC 80001-1). However, these standard agreements typically lack additional specific details on areas such as vulnerability management, appropriate cybersecurity training for staff based on roles and responsibilities (including for enterprise and/or operational technologies), or technology-specific security controls. These items need to be identified prior to the technology purchase/contract negotiation. For example, a procured medical device might store data in a remote location. In these cases, security and privacy agreements should include language that addresses such remote data storage.

Recommendations for model contract language covering these and other critical commitments between and HDO an MDM may be found in the HSCC Model Contract-Language for Medtech Cybersecurity (MC2) resource.

f) Intellectual Property Protections

During negotiations regarding assigned roles and responsibilities related to medical technologies, HDOs, MDMs, and other technology providers or healthcare stakeholders should ensure issues related to intellectual property protections are included. These parties should agree to intellectual property protections, including through Non-Disclosure Agreements (NDAs), while still supporting the ability for HDOs to maintain technologies, and engage with federal, state, local, tribal and territorial officials during incident management. As part of these agreements, the need for intellectual property protections and the security servicing needs of the HDOs should be considered and balanced.

For example, devices and other relevant technologies should be developed and designed in such a way that normal repair and maintenance functions, including software patches, do not reveal intellectual property owned by the MDM. Service functions, keys, and tools should provide access to return the product to the initial specifications put forth by the MDM and documented in the labeling of the product.

g) Licensing

Some MDMs and other technology providers license the software on their technologies. As the technology progresses throughout its lifecycle, there may be trigger events which warrant license transfer conversations between HDOs, MDMs, or other relevant parties, as license transfer may impact cybersecurity maintainability of the technology. For example, end of support, completion of service training between HDO and MDM and other contractually agreed upon events may trigger license transfer.

h) Technology Lifecycle Information

MDMs should communicate to customers relevant details and key dates related to the expected lifecycle of medical technologies. This includes information on how long to expect support (including applicable warranties), when the technology will reach lifecycle milestones (e.g., EOGS, EOS, EOL), and other similar considerations. Proactive communication is necessary to help customers plan for upgrades to technologies that still receive support, and to provide mitigations to current risk of unsupported technologies.

(1) Component EOL Communication Considerations

Medical devices, as well as other technologies used in healthcare environments, often incorporate a wide variety of hardware and software components that interact with and depend upon each other. This coexistence can create tension when support for a particular software or hardware component ends before support for other components within the system. This occurs most often when a software component, such as an operating system (e.g., Microsoft Windows 7), is no longer supported by its original developer (e.g., Microsoft). When support is desynchronized in this way, performing cybersecurity risk management becomes more complex. In the absence of official patches for these no-longer supported components, vulnerabilities often must be mitigated through compensating controls, which can mean an additional burden for both the HDO and MDM. In such situations, even if the technology is within the originally-communicated support period, it could be considered a legacy technology because it may no longer be capable of being reasonably protected against current cyber threats.

Expectations between technology usability and cybersecurity change because of this discrepancy. Devices and other technologies that still perform their intended function, even in the absence of software component support, may be difficult for HDOs to retire or replace for

fiscal or operational reasons. Ultimately, the MDM and other technology providers must provide clear information to the HDO about the real risks of a technology with unsupported components, and the potential upgrade pathways, so that the HDO can make an informed risk decision.

(2) Recommendations for Managing Device Lifecycle Communications

HDOs, MDMs, and other relevant parties should collaborate to ensure that: (1) the following communications occur; (2) the information included within the communications is as up-to-date and accurate as possible; and (3) it is received by the most relevant recipients. Additional recommendations and details on how to accomplish these goals are available in the HSCC Medtech Vulnerability Communications Toolkit (MVCT).

- ***Direct Customer Notifications:*** Direct customer notifications should be sent to affected stakeholders as agreed to by the relevant parties, including the persons/distribution lists as identified by the customer and as noted within their service record. Communication of approaching EOGS, EOS, and EOL dates should take place as soon as milestones are announced, preferably 3 years prior to these milestones. This notification allows customers to begin planning for necessary risk mitigation activities, including updates and upgrades of relevant technologies.
- ***Ensuring Accurate and Up-to-Date Contact Information:*** MDMs and other technology providers should establish processes for updating customer contact information, customer records, and medical device or technology inventory status at least annually. Since accurate customer information and install base information is necessary to ensure timely and accurate communication, it should be ensured that these are maintained accordingly.
- ***Transparency of EOGS and EOS Dates:*** Notifications to the public should be accessible through, but need not be limited to, the manufacturer's website, customer portal, or contracts. EOGS, EOS, and EOL milestones for each product should be identified when they are established, and be made available to customers.
- ***Inclusion of EOGS/EOS/EOL Dates in Technical Documentation:*** Accompanying technical documentation provided to customers should include, if known, information pertaining to EOGS, EOS, and EOL dates. As appropriate, this may be supplemented by agreement(s) stating that the responsibility for maintaining security and assumption-of-risk for use of the technology beyond the EOGS/EOS dates

may transfer to the customer at this point, consistent with applicable legal requirements (e.g., postmarket responsibilities).

C. Cybersecurity Risk Management

Performing cybersecurity risk management for legacy technologies presents three main challenges: 1) the volume of current legacy technologies to assess, 2) the lack of information available on their security controls, and 3) the risks associated with "future" legacy technologies that must be appropriately managed, and actions that should be taken to ensure that these technologies do not become legacy unexpectedly.

> ***Note: "Future" Legacy Technologies, and "Unexpected" Legacy***
>
> A **future legacy technology**, as defined in this document, is a technology that does not yet meet the adapted IMDRF definition of a legacy technology, but will eventually meet the definition as it ages. Because all technologies age, all technologies will eventually become "legacy."
>
> **"Unexpected" legacy** occurs when a change in threats or circumstances results in a technology meeting the adapted IMDRF definition of a legacy technology prior to its anticipated, "expected" EOL/EOGS/EOS date. Because "unexpected" legacy status creates risk management challenges, efforts should be made to avoid it.

As this document is focused on legacy technologies, it will not cover organizations' standard risk management practices for managing the cybersecurity risk of technologies more broadly (for that, please review these resources[4]). Instead, this section will focus on legacy risk management practices, which are an extension of standard risk management practices for technologies overall. It will explore these two unique facets of legacy technologies and techniques for addressing them.

4 The Health Industry Cybersecurity Practices (HDO best practices); the Joint Security Plan (MDM best practices); NIST SP 800-37 Rev. 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

1. HDO Risk Management Considerations

a) Managing Current Legacy Technologies

In developing strategies, policies, and procedures for managing growing cyber risks, organizations may leverage a comprehensive technology cybersecurity risk management program that works well for future legacy technologies entering the organization but may find that this process is too time-consuming to use for thousands or tens of thousands of current legacy technologies.

HDOs should contact respective MDMs and other technology providers for information and support regarding legacy technologies, including risk assessments, software supply chain information, and other areas covered by this document. Where MDMs or other technology providers do not have or cannot provide necessary assistance, two main strategies to mitigate risk may be followed by organizations in this situation: a) orchestrating an assessment "surge" and b) presuming risk.

(1) Assessment Surge

In a legacy technology assessment "surge," an organization performs a high quantity of technology risk assessments in a short period of time, which typically requires temporarily augmenting their internal staff with additional resources (e.g., contractors, professional services firms).

In preparation for this surge, it is important that organizations identify which technologies need to be assessed. Organizations should leverage their existing inventory and asset management policies and procedures, to the extent they exist, and may wish to supplement these with recommendations in this document (see: Section VI., Identifying a Potential Legacy Technology, and Section VIII.D, Inventory/Asset Management).

Once an organization has ensured their inventory is accurate, complete, and current (to the greatest extent possible), this approach generally proceeds to an exercise in identifying additional key technical attributes for legacy technologies, such as operating systems and network services running. Then, technologies may be categorized based on their inherent risk (e.g., impact to safety, privacy, organizational resilience) to determine the depth of assessment. Finally, technologies follow an organization's existing risk assessment and risk management processes (e.g., information collection, assessment, remediation tracking).

To assist in this "surge," organizations may leverage Passive Network Monitoring (PNM) products that have been introduced to the market, including those that have been specifically designed to address the unique challenges of medical devices and other technologies used in healthcare environments. These types of tools can greatly simplify the task of technology data collection and management. They derive technology security properties by passively observing and analyzing network traffic, complement it with externally collected data (e.g., manufacturer MDS2, SBOMs), and provide asset and risk information. In addition, they also detect and alert to abnormal network behavior that may indicate a security event and can therefore also be used to reduce legacy technology exposure.

The advantages of an assessment-surge based approach, be it conducted manually or with automated tools, are that the organization can: (1) better understand the vulnerability landscape for legacy technologies (e.g., more clarity on operating system versions and other security-critical software components), (2) address specific current risks in a targeted fashion (e.g., disabling an unused and vulnerable protocol), and (3) prioritize at-risk technologies in their long-term replacement planning. The disadvantages are the initial cost, which can often go into the millions of dollars for large health systems, and the return on investment (i.e., there may be limited options for reducing risk given the technology age).

(2) Presuming Risk

In the separate strategy of presuming risk, the organization assumes that all legacy technologies are vulnerable to exploitation and focuses on compensating controls.

An advantage of presuming risk and the appropriate application of compensating controls is that this approach can significantly reduce the exposure of entire classes of vulnerabilities, versus addressing vulnerabilities on a case-by-case basis. In addition, resources are spent compensating for risks versus simply identifying risks. The disadvantages of this approach are that non-trivial costs can be incurred compensating for risks that potentially aren't present on the technology, and critical risks that couldn't be compensated for could still be present. In addition, it could also reduce functionality and/or change workflows, if things like communication protocols or ports are disabled.

Organizations that presume risk may look to the following resources, among others, for recommendations and best practices for compensating controls that address risks that may be present:

- AAMI/ISO/IEC 80001 series

- AAMI: Medical Device Cybersecurity: A Guide for HTM Professionals (2018)
- OWASP Secure Medical Device Deployment Standard;
- HHS Cybersecurity Program: Zero Trust in Healthcare (2020)
- ETSI TR 103 305-1: Critical Security Controls for Effective Cyber Defense; Part 1: The Critical Security Controls
- National Cybersecurity Center of Excellence (NCCoE): Internet of Things Cybersecurity Guidances

(3) Other Strategies

Organizations looking to apply their technology risk management program to legacy technologies may find that they simply do not have adequate information to determine what security risks may be present in legacy technologies and what security functionality may be available. Specifically, the legacy technologies may not have MDS² forms or SBOMs, and/or the MDM or technology provider may not be able (or may decline) to respond to technology security inquiries. In those cases, two main strategies may be employed: (1) collaborative outreach and (2) technical investigation.

If neither collaborative outreach nor technical investigations reveal sufficient information for risk management of legacy technologies, organizations may consider replacement.

(a) Collaborative Outreach

Collaborative outreach is simply connecting with other organizations to see if they have the missing technology information. Such organizations may include:

- HDOs
- Health-ISAC
- ISAOs,
- Third-Party Service Providers
- HSCC
- Cybersecurity vendors, and/or
- Other relevant organizations

Large healthcare systems especially may have had longer-running technology security programs and may have collected this information as part of their risk assessment processes. If they don't have this information, they may have performed their own technical investigations (see below), and may be willing to share those results in lieu of the source information.

(b) Technical Investigation

Technical investigation is using a variety of tools to determine the underpinning technical components (and by extension, the vulnerability points) of a technology. Various means can be employed to identify the key technical attributes of a technology (e.g., its operating system or network protocols). For example, a basic Nmap fingerprint scan can often differentiate a Windows versus Linux-based technology, and use of a network switch span port with a packet capture tool can help identify what ports and protocols are in use by the technology. If the inherent risk warrants it, organizations could also engage a third party to perform a hardware and software composition analysis to gather additional information (e.g., whether internal storage is encrypted).

Technical investigation should only be done when the technology is not in use for patient care, as investigative techniques like scanning can result in patient care disruptions, such as required reboots. Organizations pursuing technical investigations may want to pursue them within a controlled lab environment, or within other controlled environments.

b) Managing Future Legacy Technologies

Given the challenges associated with managing legacy technology risk, it is important to remember that each new technology entering the organization will, one day, be a legacy technology. For that reason, it is important to ensure visibility of future expected EOGS/EOS/EOL events, and continuity of the risk management program to avoid accumulating a future backlog and to ensure that all relevant materials are collected at the time of purchase.

HDOs can implement a risk management process (or expand an existing technology risk management process) to include specific considerations for legacy technologies to identify and manage the unique risks. This includes establishing criteria that can be applied to manage and mitigate risk based on factors such as:

- governance
- budget
- risk tolerance
- organizational as well as technology-specific clinical capabilities, dependencies, and impacts

- prioritizing and planning for short- and long-term replacement of legacy technologies and/or compensating controls.

Stakeholders that typically are included or may provide useful input into this process are:

- Health Technology Management (HTM) or Clinical Engineering
- Information Security and Information Technology
- Risk Management and/or HTM Security Risk Management (if established as a separate role)
- Clinician Representative (e.g., physicians, nurses, technologists)
- As needed, administrative functions like Procurement, Supply Chain, Finance or Compliance
- As needed, Business Leadership or Board Members
- As needed, external stakeholders like security experts, industry organizations, or manufacturers themselves

A useful resource to support the development of a legacy technology risk management program is the ISO/IEC 80001 series of standards as it provides a framework for:

- Defining and assigning Security Roles & Responsibilities
- Establishing a Technology Risk Management process
- Identifying supporting processes and practices, like Responsibility Agreements, approval workflows, or contracting.

Considerations for Smaller and Mid-Size Organizations

Unfortunately, many mid-sized or smaller organizations cannot afford to staff dedicated roles, and individuals may have to wear several hats. In combination with the severe budget restraints typically found at these organizations, this can make addressing legacy technology risks even more challenging. External contractors including ISOs may be able to provide or augment risk management strategies and solutions. In addition, government and industry organizations like HSCC, H-ISAC, MedISAO, CISA, AAMI , or the FBI's Infragard CyberHealth Working Group (CHWG) can provide useful resources to help jumpstart or supplement a program. Certain states may also operate state fusion centers that HDOs can leverage. For an expansive listing of available information sharing and best practice groups, organizations may examine the HSCC Health Industry Cybersecurity-Matrix of Information Sharing Organizations resource.

The requirements as well as the capabilities of different organizations will vary widely based on size, staffing, and risk tolerance. Practical guidelines on the implementation of a medical device security program are provided by AAMI"s Medical Device Cybersecurity – A Guide for HTM Professionals[5], including:

- Stakeholders and their Roles, Responsibilities, Training, and Education in Cybersecurity
- Managing the Asset: Inventory and Configuration Management
- Medical Device Cybersecurity Risk Assessment
- Medical Device Cybersecurity Risk Mitigation: Establishing Effective Governance
- Appendix with Cybersecurity Risk Management Flow Chart and Examples of Medical Device Cybersecurity Tools, Policies, and Procedures

These recommendations may be extensible to other technologies used in healthcare environments as well.

Organizations should look at the Governance section (Section A) and Risk Management section (Section C) for specific discussion and recommendations related to these areas.

(1) Recommendations to Address Legacy Risk Management throughout Technology Lifecycles

While the most significant challenges related to legacy technology risk management arise when the technology becomes legacy, to effectively manage legacy technology risks, it is important that organizations take steps throughout the technology's lifecycle to mitigate or potentially avoid certain legacy challenges. The following sections provide recommendations at each stage of a technology lifecycle to address these challenges.

(a) Product Assessment Stage

As part of routine operations, HDOs identify needs for new infrastructure such as technologies used in their environments. Once a need has been identified, but before a technology is purchased, HDOs should assess the technology.

A formal Technology Risk Assessment Process should be in place prior to the need of acquiring new technology. If not considered, the lack of certain risk management practices can lead to legacy technology issues either from acquisition or later in a technology's lifetime. To mitigate

5 https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA

legacy concerns, standard risk management practices should examine the following aspects specific to the technology itself:

- Product documentation that identifies necessary security questions and concerns, such as MDS² disclosure statements, SBOM information, and system diagrams like architecture, data-flow, or networking diagrams;
- Identification of a technology lifecycle plan, including EOS, EOGS, EOL, and other related milestones;
- An overview of the associated vulnerability management program;
- The MDM or technology provider's vulnerability disclosure process, including their coordinated disclosure program;
- The technology's patching program;
- Customer communication channels, including portals, direct representatives, or others;
- Service-related SLAs, identified in contracts; and,
- Responsibility transfer considerations (discussed more in Section VII.C.3).

Standard risk management practices should also examine characteristics specific to the MDM or technology provider selling the product, including:

- The maturity of their technology security program;
- An overview of how technologies are developed, with security design and controls;
- Past history/experience of working with the MDM or technology provider, if any;
- Overall quality of the technology or technologies being assessed, based on clinical features and design (including input from clinical staff);
- Organizational ability and/or willingness to adhere to, e.g., HSCC Model Contract clause recommendations.

Any mitigations should be communicated to the appropriate teams during the acquisition and implementation stage.

HDOs may lack the resources, including staffing and funding, to comprehensively carry out each of these recommendations for all relevant technologies within their environment. Nonetheless, HDOs should aim to address as many recommendations as possible, and to continuously mature their policies, processes, and procedures to include additional recommendations as resources become available or capabilities improve.

This process should allow for review and approval of new technologies before purchase to ensure consideration of appropriate risk factors, while compensating for possible over-

emphasis on other factors (e.g., single physicians requesting specific technologies). This process can evaluate factors of different competing technologies including functionality, supportability, roles and responsibilities for security, as well as identify required mitigations for acceptance of any associated risks. The process should assure alignment with clinical needs and ensure technologies meet customer expectations around workflow and performance.

(b) Acquisition Stage

During this stage, HDOs should include the negotiation of the contract and the approval of the requisition after desired technologies are identified and assessed. Terms and conditions of the contract/purchase agreement should align with the outputs of the acquiring HDO's assessment stage.

This may include:

- Disclosure of the technology's support and lifecycle roadmap
- Future legacy considerations (e.g., expected technology life)
- Contracting to include specific language for technical and procedural security requirements
- Vulnerability disclosure and mitigation process
- Roles and responsibilities for risk mitigation, e.g., patching and the patching process
- Communication methodologies for the HDO, MDM, or other party to share information and discuss risk. For additional details, please see the Responsibility Transfer Framework section.
- Transfer of responsibility at the End of Support stage, including purchasing of licenses and service keys. For additional details, please see the Responsibility Transfer Framework section.
- Determining how often updated documentation, including SBOMs, will be provided, and through what methods
- Ensuring all relevant updates have been requested
- Technology hardening and disabling of unnecessary ports and services

More information about model contract language can be found in the HSCC Model Contract-Language for Medtech Cybersecurity (MC2).

(c) Implementation Stage

During the implementation of a technology within an HDO or other environment, any defined security measures identified in the assessment stage should be applied. This may include implementing network traffic limitations, removal of default passwords, ensuring all relevant updates have been requested and applied, or other mitigation techniques to limit risk or otherwise appropriately implement the technology. The implementation should ensure any of the contractual language requirements around procedural security are implemented as well. This ensures a closed loop from assessment and acquisition to implementation.

Next, asset management-related information needs to be captured. Specifically, data on security-relevant software components and IT settings should be included, as well as technology and component support statuses. At installation, all current information such as IP address, MAC address, and SBOM information should be captured and documented in the asset inventory. Additional recommendations for items to track are discussed in the relevant Challenges and Recommendations sections.

There are generally two places this asset information can be housed. Typically, Clinical Engineering or HTM departments keep this information in a Computerized Maintenance Management System (CMMS). CMMS systems are usually in place to meet regulatory requirements and generally hold more information than IT and security information. Similarly, IT departments usually have a Configuration Management Database (CMDB) which can also track IT and security information. Generally, these two systems do not interface and therefore information may need to be entered and maintained in two different systems. Where necessary, organizations should consider how to effectively leverage and integrate these systems into one source of truth.

Because of the complexity of managing full suites of technologies used in healthcare environments, support plans and sustainment plans should also be developed during the implementation stage. These plans should include security risk details, such as security roles and responsibilities, patching, endpoint protection upgrades, vulnerability scanning, and monitoring for newly discovered vulnerabilities and penetration testing. Plans should take into account the clinical availability of technology and may include training end users on security related issues involving the technology/system.

(d) Support/Maintenance Stage

Servicing technologies during the support/maintenance stage, and prior to the EOL/EOGS/EOS of the lifecycle, should consider the unique risks and requirements for these technologies. While the technology is under support, patches are generally available from the MDM or technology provider. During this stage, teams should execute the plan developed in the implementation stage including:

- Patching
- Keeping inventory details up to date (e.g., operating system, network information, software version, firmware version)
- Monitoring for newly discovered vulnerabilities
- Monitoring for malicious network traffic and remote connections
- Communicating regularly with the MDM or other technology provider regarding, e.g., patches, EOL milestones, and upgrades.

As technologies age, organizations should expect and plan for more time, skills, and/or resources being required by HDO clinical engineering and/or IT to support technologies used in healthcare environments.

(e) End of Support Stage

"End of Support" or "EOS" may refer to either: (1) the technology itself entering its planned EOS lifecycle stage; (2) an individual component within the technology, including an upstream software component, becoming unsupported; or (3) the technology entering an EOS stage for another reason. Where EOS terminology is being used in discussions or documentation, it should be understood whether the EOS designation refers to the technology or a technology component, and for what reason the EOS transition is occurring.

It is strongly recommended that HDOs, MDMs, and any relevant parties collaborate so that the majority of EOS stage transitions are planned ("expected"), thereby allowing both parties to allocate necessary resources (including funding, personnel, and time) to decommission, replace, and/or implement compensating controls for EOS technologies as needed.

To accomplish this, HDOs and MDMs should ensure to the greatest extent possible that they are integrating relevant agreements and assignments of roles and responsibilities into contracts and other documents. However, cases may arise that may lead to "unexpected" EOS declarations which may occur due to circumstances outside of the MDM's or other technology

provider's control. For example, upstream software components may become EOS, which then ripples down to EOS for technologies.

Individual third-party technology components may be declared EOS by their original developer. This can cause changes to how the MDM or other technology provider provides support. To address this, MDMs should track their technology component usage and provide this information to HDOs. Updates to this information should be made and provided to the HDOs as this information changes, and HDOs should track and respond to this information as it is received. MDMs should provide communications to HDOs about relevant components' statuses, including EOS declarations or changes in support status. This enables both HDOs and MDMs to perform impact assessments and act accordingly.

In all cybersecurity EOS declarations or transitions, HDOs should leverage the "Responsibility Transfer Framework" outlined in Section VII.C.3 to help inform their next steps. As discussed in that framework, HDOs may choose to continue using EOS technologies, and the framework is intended to help guide HDOs do so as safely and effectively as possible.

It is important to note that technologies should be regularly reassessed using the "Responsibility Transfer Framework" as new vulnerabilities related to the technologies are discovered, new network architectures are implemented, or other changes are made within the HDO environment that could impact the risk of continuing to use the technology. HDOs should ensure they are periodically reevaluating these risks to ensure continued patient safety.

After end of support, HDOs may leverage third party service providers and/or specialized security service/tool vendors to assist with managing ongoing cyber risks to technologies. These may include patch management, assistance with software upgrades, and if software support is unavailable, information on potential compensating controls that the HDO may be able to implement.

(f) Decommissioning Stage

As upgrades or changes are made to their infrastructure, HDOs may replace or decommission technologies. HDOs are advised to implement practices and other procedures to ensure the review and/or removal of residual patient data and other sensitive data (e.g., user and network credentials, intellectual property) on technologies that:

- have been identified for decommission,
- have been or will be de-installed, or

- are temporary/replacement technologies that may be ultimately used at other organizations. [6]

The NIST Special Publication on Guidelines for Media Sanitization may be useful in developing and implementing these practices. [7]

HDOs should establish a policy to execute Responsibility Agreements (per ISO/IEC 80001-1) or BAAs (per HIPAA) for all appropriate business activities and define requirements for destruction of data upon technology deinstall or other applicable situations to include the scope of data destruction policies (e.g., patient data, clinician data, facility data, etc.). This should include remotely managed devices and technologies, such as those that may be operated by or in a clinician's or patient's environment (e.g., their office or residence).

Note that with the lines being blurred between traditional, discrete physical technologies and software-based technologies combined with cloud-based services will require that data removal beyond the actual technology be assessed and defined. If relevant data exists outside of the technology that is being decommissioned, it is important for the HDO to consider how this data will be appropriately sanitized. For cloud systems, BAAs or SLAs may be used to document and enforce appropriate data sanitization procedures.

MDMs and other technology providers can support HDOs decommissioning practices through providing documentation:

- about the nature and extent of data storage,
- on the appropriate process to wipe data from the technology, and
- about the capabilities inherent in the technology that could support data sanitization.

Furthermore, MDMs and other technology providers may consider establishing processes to address situations in which they inadvertently receive technologies or parts with patient data, including informing the HDO that such a situation has occurred, and providing documentation that the data was destroyed or returned to the HDO, as appropriate.

It is prudent to assess whether any data to be securely erased/wiped has been stored elsewhere in compliance with regulatory requirements and customary retention period. If this is the case,

---

6 These may include devices or technologies sent out for repair, pre-owned, re-manufactured, refurbished, rentals, loaners, leases, or remotely managed devices.

7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf;

HDOs should ensure that it is sanitized or retained in compliance with all applicable legal requirements.

The HDO configuration repository (CMMS or CMDB) can flag devices that require data wipe prior to, or as part of, deinstall. HDOs should be aware that certain MDMs or service providers may offer "secure wipe" services to legacy device, and HDOs can maintain a listing of available services. HDOs should validate that this service meets the needs of the organization. If an electronic data wipe is not available for legacy devices, HDOs should ensure the physical storage media is removed and/or destroyed to prevent data loss or compromise.

2. MDM Risk Management Considerations

MDMs should implement security, safety, and risk management processes and activities that include specific considerations for legacy devices to identify, reduce, and manage the risks of medical technologies, including legacy technologies.

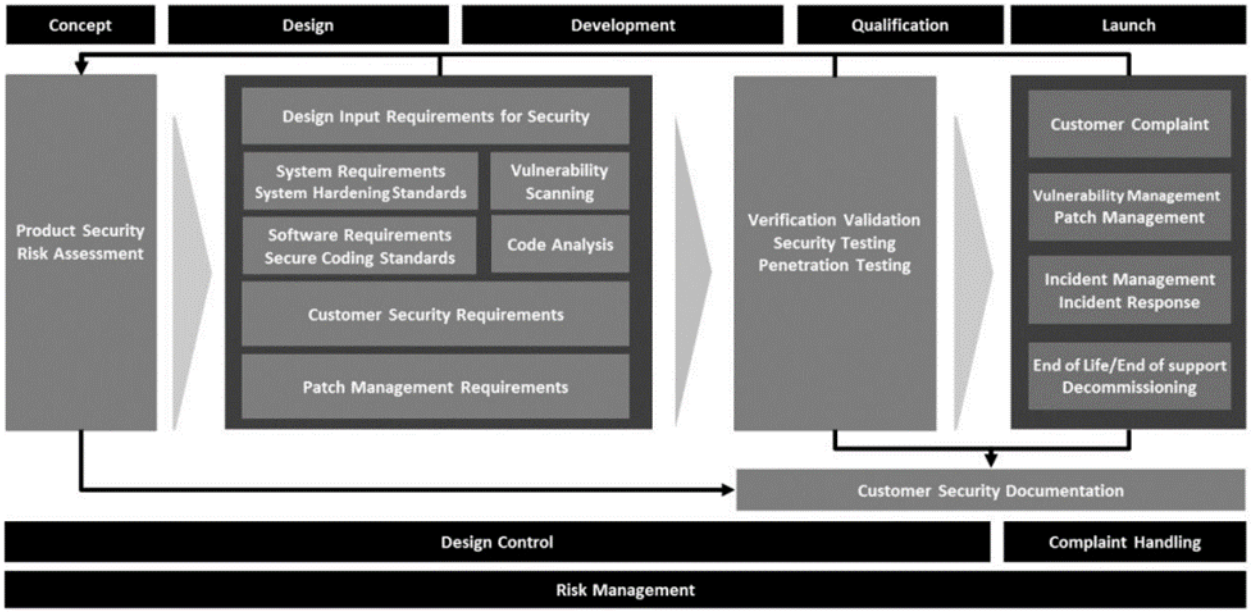


Figure 1 JSP

Some useful resources that support the development of a legacy device risk management program include, but are not limited to:

- AAMI TIR57 – Principles for medical device security – Risk Management
- AAMI TIR97 – Principles for medical device security – Postmarket risk management for device manufacturers

- IEC 81001-5-1 – Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle
- NEMA/MITA CSP 2-2021 – Lifecycle Best Practices Framework for Medical Imaging Devices

Security risk management typically involves the following stages, illustrated by Figure 1. As can be seen, it is important to integrate potential safety risk management factors into security risk management and vice versa over the lifecycle.

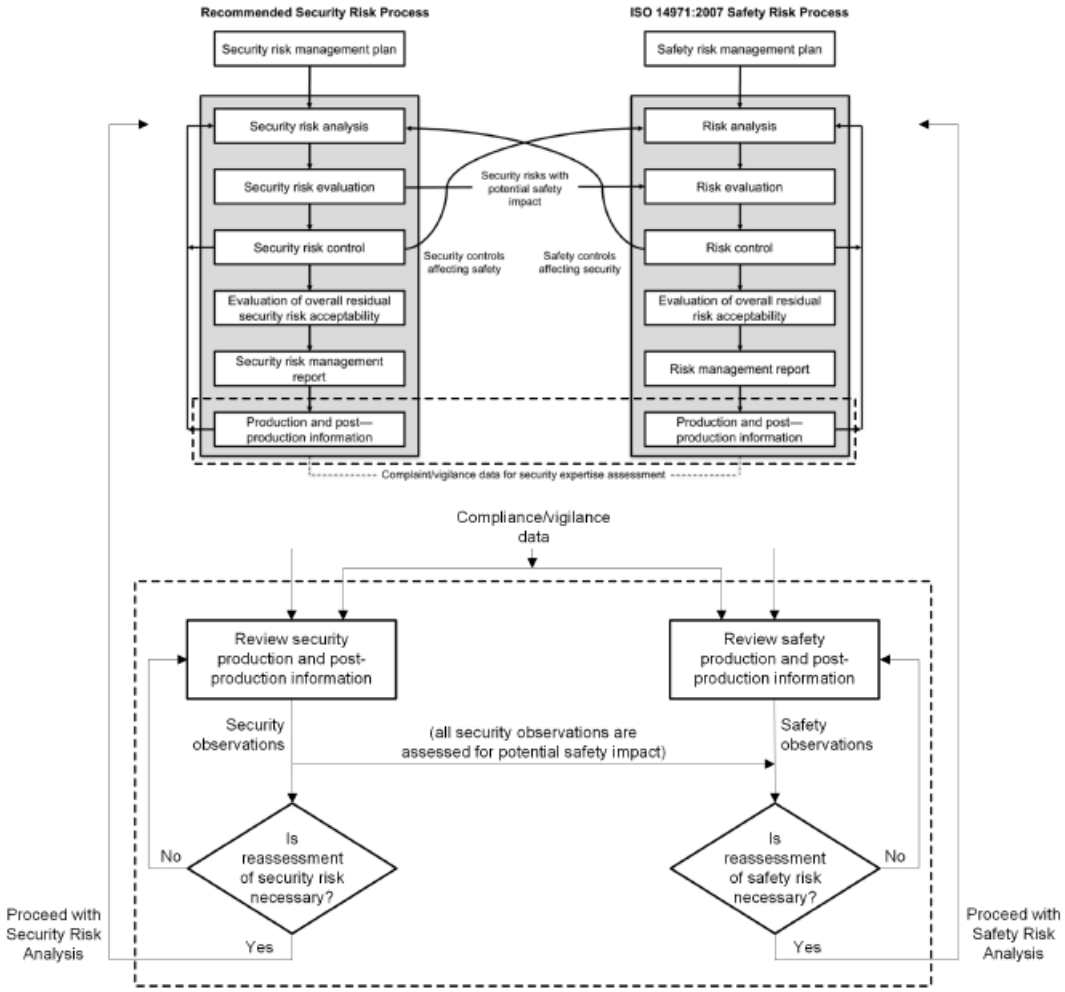


Figure 1—Postmarket decision-making flow diagram

Reproduced with permission

To summarize, an effective risk management process will typically entail the following stages that apply to both the management of security risk and patient safety risks:

- Risk management planning
- Establishment of risk acceptability criteria
- Risk assessment, which includes:
    - Risk analysis (identification of assets and vulnerabilities)
    - Risk estimation
    - Risk evaluation
- Application of risk controls
- Evaluation of overall residual risk acceptability
- Risk management reporting
- Production and post-production activities
    - Risk monitoring
    - Risk and incident response

It is crucial to note that security risk controls may have an impact on patient safety risks and safety risk controls may have an impact on security risks. This relationship applies for the duration of lifecycle of products in both the pre-market and post-market stages.

It is also important to note that the risk management processes identified above may exist in conjunction with other enterprise risk management (ERM) activities to ensure that MDMs are managing business, privacy and other non-product specific risks.

The risk management process for legacy devices should include considerations of the following:

- Given the one-to-many or many-to-one dynamic between MDMs and HDOs, it is foreseeable that the initial MDM risk assessment and risk controls associated with legacy devices may need additional reassessment within HDO environments due to contextual variations (i.e., different risk criteria or risk tolerance). The MDMs must play a role in ensuring that information needed by HDOs to perform those contextual (re)assessments appropriately is available.
- It is best practice for MDMs to send communications to HDOs warning of approaching device EOL/EOGS/EOS dates. As part of these communications, MDMs should provide to HDOs any updated relevant security documentation where applicable, such as architecture views, SBOMs, or compensating controls. HDOs should leverage this information to perform security risk assessments to consider possible impacts to device function.
    - Risk assessments for future legacy devices need to be comprehensive and holistic to avoid patient safety risks or major disruptions to clinical or data workflows. In

these circumstances, appropriate communication is needed with HDOs to ensure that localized compensating controls can be accounted for as part of the HDO risk management process.

- MDMs should include as part of the EOL/EOGS/EOS communications the recommended steps that HDOs should take to prepare devices for EOL/EOGS/EOS, including contact changes or license transfer.
- MDMs and HDOs should collaborate to ensure communications are established between all relevant parties for device maintenance after EOL/EOGS/EOS, where applicable, including third party servicers.
- MDMs should review the Responsibility Transfer Framework that this document recommends HDOs use when assessing EOL/EOGS/EOS devices, so that they understand the processes that HDOs might follow, and how that may impact the MDMs own processes.
- HDOs can and do decommission devices. MDMs and HDOs should collaborate on effective methods for safe, secure decommissioning, as well as on upgrade pathways to new devices.

3. Responsibility Transfer Framework

To mitigate or eliminate legacy technology risks, organizations (including HDOs) would cease to use technologies once they have reached their EOL/EOGS/EOS or have otherwise become legacy. However, there are many valid reasons that HDOs and other organizations continue to use legacy technologies, including:

- balancing the expense of replacing technologies (especially those that continue to safely and effectively perform their clinical or other functions) with other organizational needs
- the lack of an acceptable replacement for the technology
- potential unacceptable disruptions to workflow

Recognizing this reality, it is important for HDOs to have access to information and best practices regarding how to manage legacy technology risk as safely and effectively as possible in situations where they intend to continue using legacy technologies. The following section outlines a Responsibility Transfer Framework to support this decision-making process.

Please note that this is a best practices document related to managing legacy technology risks. Prior to implementing the recommendations, organizations should review their own internal policies and procedures, as well as regulatory requirements, to ensure appropriate compliance.

(1) Initial Evaluation

When HDOs obtain medical equipment, lifecycle plans for that equipment should be established. This process was discussed in the governance/lifecycle section. When equipment reaches EOGS/EOS in particular, generally the manufacturer stops supporting devices, which includes the availability of security updates (e.g., patches). Preferably before a technology reaches EOL/EOGS/EOS, but at least at the time of a technology's EOL/EOGS/EOS date, the HDO should risk assess the technology to determine whether the risk of keeping the technology active outweighs the risk to the organization from consequences that may arise from the lack of support inherent in EOL/EOGS/EOS technologies. That assessment should also include the analysis of the feasibility of implementing compensating controls to reduce the risk of keeping unsupported technologies in the environment while maintaining the technology's intended use. Below are some factors HDOs should take into account when completing the Risk Assessment of the EOL/EOGS/EOS technologies.

(2) Risk Assessment

The risk assessment should be a holistic attempt to weigh the risks of decommissioning the technology against the increased exposure for cyber risks. Factors that should be taken into account are: (1) safety and effectiveness, (2) clinical, and (3) technical.

(a) Safety and Effectiveness Factors

The first question the HDO should evaluate is whether safety and effectiveness are impacted when the technology is performing its intended function after EOL/EOGS/EOS. Generally, EOL/EOGS/EOS is a date set by the MDM or other technology provider, and the technology does not stop functioning from a clinical perspective on that date, and in theory can continue to be used. However, there may be some instances where that technology is connected to a cloud solution or some other system that will stop working on that EOGS/EOS date. The impact to that technology at the EOGS/EOS date needs to be understood.

In addition, the type of EOL/EOGS/EOS use case has to be well understood. In general, there are three different use cases for EOL/EOGS/EOS technologies.

1. The hardware is supported by the vendor, but the software (e.g., operating system) on the technology is no longer supported.

2. The hardware is no longer supported by the MDM or other technology provider, but the software is still supported. In this instance, the MDM or other technology provider may choose to EOL/EOGS/EOS the technology, but patches are still available through other third parties.
3. Both the hardware and software are unsupported.

Depending on the technology use case, different aspects of support need to be evaluated. For example:

- Are there third-party providers that are capable of supporting the technology? What types of protections/mitigations can they provide? Are these protections/mitigations sufficient?
- If hardware is no longer supported, are there third parties who can provide those parts, disposables, and consumables to the HDO?
    - Are there known vulnerabilities in the hardware/firmware that need to be tracked or mitigated? What are the risks/impacts of any known vulnerabilities?
    - How is the HDO going to handle future vulnerabilities related to the hardware?
- If software is no longer supported, are software patches, version patches or other patches available via other avenues (OTS/SOUP/COTS)?
    - Does the HDO have expertise to install and test those patches without affecting the safety and effectiveness of the technology?
    - Are there legal requirements (e.g., postmarket surveillance, licensure) that may be applicable, and does the HDO believe it is mature enough to manage them if so?[8]
    - Is the HDO prepared to take on any applicable regulatory requirements if they choose to patch a device or technology without the MDM's or other technology provider's support (e.g., postmarket surveillance)? [9]
    - How is the HDO going to handle future vulnerabilities related to software?
- Is there training available to learn how to use and support the technology after EOL? Is this MDM training or 3rd party training? How inclusive/comprehensive is it?

[8] See, e.g., FDA's draft Remanufacturing Guidance.

[9] See, e.g., FDA's draft Remanufacturing Guidance.

(b) Clinical Factors

Clinical benefits and risks, including the impact to the hospital/health system of removing/retiring the technologies being assessed, need to be evaluated. If the technology is serving a purpose that cannot be easily replaced, or if retiring the technology or technologies has an impact on the services able to be provided at the site (or within a region), those risks to patient care need to be evaluated. Additionally, consideration should be given to whether discontinuing the technology would lead to operational, economic, or potential life safety impacts.

Operational impacts may include removal of a type of service the HDO offers, impacts to the quality of service provided, or the number of patients able to be served.

Economic impacts may include risk to revenue and/or expenses including reduction in services, penalties for reimbursements, liabilities for legal matters, or increases in malpractice costs.

Questions that should be considered to assess the risks to patient safety include:

- Will patients be physically harmed if the technology is negatively impacted during a cyber incident?
- Are there compensating clinical interventions care providers can conduct to reduce the life safety risk of harm to patients?
- If the risk does not rise to the level of physical harm, is there impact to the quality of care, or the timeliness of service?

In addition to patient safety risk, life safety impacts should include assessments of workflow impacts:

- What is the impact of removing that technology from that workflow?
- Is the technology part of an integrated system, such as radiology systems, telemetry, or patient monitoring, where removal of a technology or service could disrupt clinical workflows?
- Are there compatibility dependencies with other systems?
- If compensating controls are required to reduce risk, what is the impact on clinical workflow; i.e., would the presence of compensating controls impose a negative impact on the clinical workflow?

Next, other stakeholder and cultural considerations should be taken into account:

- Can the clinical workflow be adapted to support the removal of the technology from the network?
- If compensating controls can be put in place to reduce the risk, are those acceptable to all stakeholders?
- Is it the organization's practice to allow clinicians to overrule cybersecurity risks, and if so, are associated legal and malpractice risks considered?
- What other privacy, legal, consent, or business risks should be considered?

(c) Technical Factors

In addition to the safety and effectiveness and clinical impact, other technology risk factors should be evaluated:

- Is the technology exposed to any vulnerabilities contained within CISA's known exploited vulnerabilities (KEVs)[10] list?
- Is the technology exposed to any other known cybersecurity vulnerabilities (e.g., vendor, ICS-CERT, NVD)?
- Are those vulnerabilities exploitable in the environment?
- Is that exploitation local or remote?
- What impacts could occur if the vulnerabilities are exploited?
    - Could a successful exploit be confined to the individual technology, or could it lead to larger system compromise?
    - How would an exploit be identified or detected?
- Can identified risks be mitigated, such as through the implementation of compensating controls?

If the technology has known risks that cannot be reasonably mitigated by the organization, the organization must assess the risk level and determine whether that risk is worth accepting.

How the technology interacts with its environment (e.g., hardware ports, other devices, systems, and the network) needs to be well understood. If the technology is connected, the HDO should take the following considerations into account to understand the risk:

- Has the MDM or other technology provider made available a diagram illustrating the technology's network properties and its connections?

10 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Is there an external connection (e.g., via VPN, site-to site, or cloud)?
- Does the technology include or require remote protocols, ports, or services?
- What ports are required to be open, and what risks do those ports pose?
- What security controls are already in place to protect that connection (e.g., VLAN, segmentation, two factor authentication)?
- Can additional security controls be put in place to further protect that technology?
- What are the costs and impacts of those compensating controls?

As discussed in the Safety and Effectiveness section, the technical ability of the HDO to continue to support EOL/EOGS/EOS technologies needs to be assessed. Technical skills, tools, and training need to be evaluated as well as knowledge and ability to comply with relevant legal requirements (see draft FDA guidance related to device repair versus remanufacturing[11]). Teams should be prepared to understand, evaluate, accept, and document the risk for support of these technologies.

These risk assessments should be a transparent process that weighs the benefits of keeping the technology against the increased risk for cyber incidents. HDOs' budget and resource requirements to replace the technology need to be weighed against the budget and resource requirements to continue to use the technologies past EOL/EOGS/EOS.

(3) Implementing The Risk Assessment(s)

Once the relevant risk assessments are performed, HDOs should either (1) decommission the technology or technologies (if the risk is too high) or (2) continue to operate the technology or technologies.

(a) Decommissioning Legacy Technologies

If HDOs perform their risk assessment and determine that they will decommission legacy technologies, they should follow their documented policies and procedures for doing so. They may also wish to review Section VII.C.1.b)(1)(f) for additional recommendations.

11 https://www.fda.gov/media/150141/download

(b) Continuing to Use Legacy Technologies

If HDOs perform their risk assessment and determine they will continue operating legacy technologies, they should consider the following factors on how to do so as safely and effectively as possible. Additional details and recommendations for many of these factors are discussed in the Challenges and Recommendations section.

There is a spectrum of risk management techniques to consider to effectively and efficiently manage technology EOL/EOGS/EOS, ranging from keeping the technology after EOL/EOGS/EOS, to proactive replacement prior to anticipated EOL/EOGS/EOS. However, the techniques along this spectrum all incur accepting some risk. This ranges from risk acceptance of maintaining a legacy technology without MDM or other technology provider support, to utilizing the device with reduced capabilities, deploying compensating controls, or replacing the technology.

Inventory Management: The first step toward effective inventory management of EOL/EOGS/EOS technologies is knowing all technology ages and potential longevity. In addition to basic information provided by the MDM or other technology provider, additional metadata available from Manufacturer Disclosure Data (MDS²) forms and available SBOM data should be added to the technology inventory information. For continued use of legacy technologies, inventory management is important to understand which legacy devices are in use, where they are (i.e., not moved outside of compensating control environments), update status, and other relevant details.

Lifecycle Planning: Another useful task is to formalize the process of technology decommissioning by having a standard checklist available for use. Procedures should be in place to plan for early replacement of technologies nearing their EOL/EOGS/EOS, and to have checklists for accepting new/replacement technologies. This will minimize future risk associated with operating these technologies by fully vetting them prior to implementation. Developing multiple EOL/EOGS/EOS options is optimal.

Ongoing, Proactive Evaluation: Lastly, to effectively manage future risk associated with existing technologies, organizations should be proactive in evaluating technologies continuously. HDOs should actively seek out information on technology support status from sources other than the MDM or other technology provider.

Keeping Technologies: For technologies that the organization decides to continue to use past their declared EOL/EOGS/EOS, the organization will need to take over primary surveillance and monitoring of the technology, including potentially addressing any future

vulnerabilities. This added burden may be significant and may require additional risk management capabilities. This may increase the liability to the organization and the projected cost and workload should be carefully evaluated against the rationalization of continuing to use the device past its declared EOL/EOGS/EOS.

Conversely, a proactive approach to maintaining use of EOL devices would be to increase overall organizational security protections to minimize the additional risk of maintaining EOL devices in use. Again, the added cost and workload of implementing these additional best practices and procedures should be carefully weighed against the perceived benefit of retaining EOL devices.

It bears repeating that the recommendations in this document guide HDOs and MDMs toward the imperative that patient safety requires cyber safety.

4. Patching Lifecycle Recommendations

Reliance on patching as a key part of security risk management originated in the enterprise IT and commercial software spaces. Regular updates of applications and platforms is well-established best practice using IT management tools that automate patch distribution, management, and deployment.

However, patching is still a reactive security process that requires significant effort by both those organizations who must design, develop, validate, verify, and release patches, and by those who must identify the existence of, retrieve, install, and validate them. Moreover, patching often leaves a window of vulnerability in between the discovery of an issue and a patch being developed, deployed, and applied to mitigate any associated risks, placing unpatched systems—and those that rely upon them—at risk.

As a result, it is important to question whether patching as an IT-originated security strategy can be successful in the much more complex and restrained ecosystem that exists within healthcare systems. Given the technical, operational, and financial restraints, as well as the complexities and dependencies inherent in healthcare delivery networks, it is extremely challenging to be able to patch fast enough and often enough to meaningfully address the myriad cyber threats faced by the sector.

Nevertheless, patching must unfortunately remain a primary risk mitigation mechanism in the healthcare sector, and the remainder of this section describes patching best practices throughout each “stage” of a patch’s lifecycle. However, enterprises across the sector should

invest significant time, resources, and consideration into how to move away from overreliance on patching to address cyber threats, including through architecture and platform choices for both the technologies and the systems in which they reside, as well as policy development, advancement in contracting and procurement best practices, and other avenues that may push the capabilities and maturity of the sector forward.

A Special Note on Patients, Clinicians, and Patching

While the majority of patching activities should and will be handled by cybersecurity and other experts within HDOs, MDMs, and ISOs, with certain technologies and/or in certain settings, patching may fall to patients or clinicians. Such technologies and settings may include medical device applications, infusion pumps, programmers or related peripherals for cardiac devices, and home healthcare settings, where patients or clinicians may install routine patches without supervision or assistance.

It is critically important that these circumstances be appropriately identified, and the patches and all associated requirements—such as retrieving, installing, and identifying and reporting any issues—be designed to allow patients and clinicians to successfully complete patching activities without requiring specialized expertise. The best practices for doing so may vary from technology to technology and one MDM or technology provider to another, but all parties involved in a technology's patching lifecycle should carefully consider and design their products and patches to assist patients and clinicians with a straightforward, reliable patching experience. One consideration is to ensure that patients and clinicians understand when and to whom they should report any issues, such as contacting their physicians and/or the manufacturer.

a) Patching Lifecycle

While "patching" is generally a well-understood concept, the process of discovering the need for a patch, developing it, and then actually applying it involves many stages. This section breaks the patching lifecycle into these separate stages and provides recommendations for each.

The concept of identifying a cybersecurity signal is a term introduced by U.S. FDA in the 2016 Postmarket Cybersecurity guidance. The document defines a cybersecurity signal as "any information which indicates the potential for, or confirmation of, a cybersecurity vulnerability or exploit that affects, or could affect a medical device. A cybersecurity signal could originate from traditional information sources such as internal investigations, postmarket surveillance, or complaints, and/or security-centric sources such as CERTS (Computer/Cyber, Emergency Response/Readiness Teams), such as ICS-CERT, ISAOs, threat indicators, and security

researchers. Signals may be identified within the HPH Sector. They may also originate in another critical infrastructure sector (e.g., defense, financial) but have the potential to impact medical device cybersecurity."

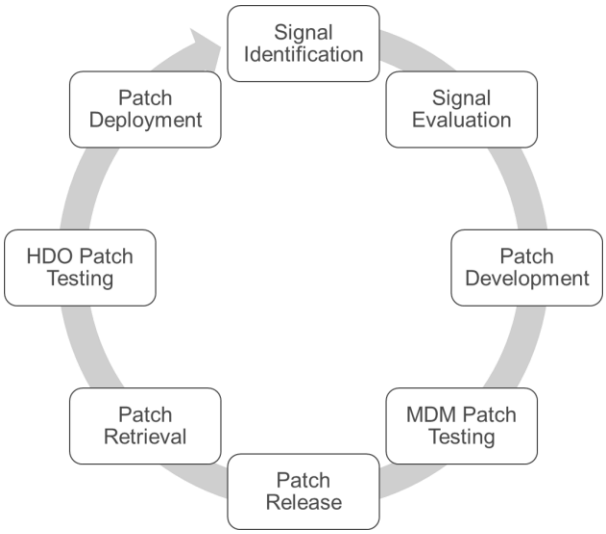


Figure 1 Patch Management Lifecycle

(1) Signal Management

The first phase of the patching cycle starts with cybersecurity signal management. Cybersecurity signals are derived from multiple sources, and HDOs, MDMs, and other relevant healthcare stakeholders should have an established process to monitor and assess/evaluate signals to determine the need for patching. The process should include detailed steps to cover the sources of signals, monitoring process, assessment process and roles/responsibilities within the organization. The signal evaluation process should specify criteria which should be used to qualify the signals and determine risk acceptability. The signal management program should be regularly reviewed for adequacy and ability to meet current cybersecurity threats.

HDOs and MDMs are encouraged to review the Cybersecurity Risk Management section for more detailed recommendations. They may also wish to review the additional resources identified in each section.

(2) Signal Identification

As part of shared responsibility for the security of technologies used in healthcare environments, HDOs, MDMs, and other technology providers have a role in identifying

cybersecurity signals. This responsibility varies depending on the composition of the technology and should be clearly articulated in the customer labelling for the devices. For example, a software-only medical device may give HDOs responsibility for monitoring operating systems vulnerabilities as opposed to an infusion pump where MDMs may have more responsibility for identifying and patching those devices.

MDMs and HDOs can receive cybersecurity signals from different stakeholders who have an interest in maintaining security of the technologies used in healthcare environments. The below diagram shows different sources for signals for MDMs and other technology providers.

Figure 2 – MDM and Other Technology Provider Signal Sources

MDMs and other technology providers should identify their primary sources of cybersecurity signals and determine who will be responsible for monitoring these sources and then communicating the signals identified in this process. This signal collection activity may broaden as MDMs and other technology providers mature their processes. Typically, this responsibility falls on the product security teams to monitor, identify, and work with R&D/Engineering teams to evaluate the signal.

HDOs also receive cybersecurity signals from variety of sources as shown in the below diagram.

Figure 3 – HDO Signal Sources

HDOs should identify their sources of signals and determine roles and responsibilities within the organization for monitoring, coordination with MDMs, other technology providers, and third parties, any applicable regulators, and to manage the patch management cycle.

HDOs, MDMs, and other technology providers should also implement processes to periodically review the signal management process to ensure it is adequate for the current cybersecurity threat and make modifications accordingly. The review should include performance of different signal sources, adequacy of the sources, shared responsibility, quality of signals, etc.

HDOs, MDMs, and other technology providers are encouraged to review the Cybersecurity Risk Management section for more detailed recommendations. They may also wish to review the additional resources identified in each section.

(3) Signal Evaluation

Once an organization has identified a signal that may require a patch, the next step is to evaluate the signal, the potential risks, and whether a patch is the appropriate risk mitigation mechanism.

Potential Parties

Parties performing this evaluation may include:

- MDMs
- Technology providers
- HDOs
- The signal reporter (security researchers, HDOs, regulators, etc.)
- Third-party component developers/manufacturers

General Recommendations

MDMs and other technology providers performing this assessment should follow their established procedures for evaluating patch need. Typically, this process will include a risk assessment in addition to an evaluation as to whether a patch is the most appropriate and effective risk mitigation technique. MDMs and other technology providers should be sure to comprehensively document this process, including justifications for moving forward with a patch, choosing an alternate risk mitigation mechanism, or concluding that action is not needed.

MDMs and other technology providers should also consider whether communicating with customers about potential or known signals may enable faster and more efficient risk management. For example, for well-publicized signals, it may be useful for MDMs and other technology providers to proactively inform customers and/or the public as to whether their products are affected, or whether an investigation is ongoing to determine whether their products are impacted. Similarly, it may be useful for MDMs and other technology providers to establish dedicated procedures, including points of contacts, for HDOs and other customers to be able to reach out and request information on known or potential signals. This may include customer-facing portals or email subscriptions for updates and/or notifications of affected signals for affected products.[12]

It may be the case that signal reporters and third-party component developers have already performed their own risk assessments. MDMs and other technology providers should ask for and review these assessments, where possible, and use them as inputs to their own assessment processes.

MDMs and other technology providers are encouraged to review the Cybersecurity Risk Management section for more detailed recommendations.

(a) Recommendations if There is Disagreement as to Risk

It is possible that there may be disagreement between parties as to the determination of the risk and the need for mitigation. For example, in the 2017 global outbreak of the WannaCry ransomware, some HDOs, MDMs, and other technology providers reached conflicting

[12] The HSCC Vulnerability Communications Working Group is also working on this issue at time of publication.

conclusions about the risks presented and the necessary risk mitigation measures - including patches - that would be needed.

To address this issue, MDMs and other technology providers should ensure that customers and other relevant parties have a mechanism through which they may provide timely feedback on MDM/technology provider risk assessments. Further, an escalation path should be available if there remains disagreement on the risks and actions needed. These paths may involve escalation within the MDM or other technology provider from a product security team member to a lead, for example, or it may involve consulting with the CISA and/or FDA (for medical devices).

The exact design of these mechanisms and escalation paths are beyond the scope of this document, but HDOs, MDMs, and other parties are encouraged to consider their organizational needs and design such mechanisms and paths as appropriate.

(4) Patch Development

Once an organization has determined that a patch is the appropriate remediation measure for a given risk, the next step is to develop it.

Potential Parties

Parties developing patches may include:

- MDMs
- Technology providers
- Software supply chain (manufacturers, open-source)
- Third-party component developers/manufacturers

General Recommendations

The primary goal of a patch is to eliminate or remediate to the greatest extent possible a given risk without introducing additional risk. MDMs, technology providers, and other relevant parties should design patches with that goal in mind. At the same time, MDMs, other technology providers - and all parties throughout the healthcare ecosystem - should acknowledge that patching technologies used in a healthcare environment can be a difficult and disruptive process, and that, where possible, patches should be designed to lessen the burden on clinical operations. Doing so increases the chances that patches are applied in a timely manner with a minimum of collateral consequences, thereby improving the security of the enterprise and the sector as a whole.

To facilitate timely, efficient, and minimally disruptive patching, MDMs, other technology providers, and other parties designing patches should, where appropriate and possible:

- Apply security engineering best practices (e.g., hardening, allow-listing) to devices when designed so that the frequency of patches is reduced throughout the technology's lifecycle
- Ensure MDMs and other technology providers include patch development as part of the technology secure development and risk management plans and allocate appropriate resources to develop and validate patches in a reasonable timeframe
- Support or provide a test environment that eliminates or mitigates end customer need to test in the end user's operational environment, i.e., the network used to deliver care
- Perform adequate testing and other validation to ensure patches are reliable
- Make it possible to deliver, retrieve, and/or install patches remotely
- Enable retrieval of MDM or technology provider validated patches
- Enable cryptographic integrity-checking of patches to ensure they have not been modified or compromised in transit
- Enable installation of manufacturer-validated patches by end users without the need to coordinate with the manufacturer or other parties
- Design patches so that their installation does not require significant downtime
- Design patches to have notification of successful installation
- Ensure patches are revertible, i.e., that they can be "rolled back" if the update fails, while also protecting against downgrade attacks
- Ensure patches may be scheduled, i.e., that overnight or off-hours patching is an option
- Design patches to require minimal or no calibration of the technology after application
- Ensure patches are properly versioned, and that such versioning takes into account Platform and Application versioning:
    - Platform versioning: ensure each platform is versioned, and versioned separately
    - Application versioning: for application-specific software, ensure each application is versioned, and versioned separately

Two areas of patch design deserve special mention:

Patches that May Need FDA Review v. Patches that Do Not Need FDA Review

In general, when updating a medical device to implement new functionality or to address newly identified risks and/or cybersecurity vulnerabilities, MDMs will need to assess whether the change(s) require reporting or premarket submissions to regulators. Because submitting patches for review by the FDA necessarily introduces delay into the patching process, manufacturers should be deliberate in their patching design choices so as to minimize these delays, while ensuring the safety and effectiveness of patches, and compliance with all applicable regulations (*See: Summary of FDA Guidance on Patching, page 59)*.

To effectively manage cybersecurity risk, it is important that organizations are able to patch technologies as quickly as possible. At the same time, because patching is resource-intensive and can be disruptive, it is also important that organizations patch on a predictable schedule, but as infrequently as possible, while still controlling the risks.

These two goals may sometimes be contradictory. For example, it may be that to address routine maintenance and non-urgent cybersecurity issues, "bundling" as many patches into a single release as possible lessens the burden on users like HDOs. This bundling may include patches that require FDA review and patches that do not require FDA review, where the potential delays caused by the regulatory requirements of the latter do not create unacceptable risk. However, where urgent cyber risks do exist, it may be advisable to avoid this bundling, because the ability to patch quickly is critical.

To enable faster and less disruptive patching, MDMs, other technology providers, and other parties designing patches should, where possible and appropriate:

Establish two separate patching streams, one for patches that may need FDA review and one for patches that do not need FDA review

- Design patches to be modular, i.e., each patch is discrete and can be applied separately
- Design patches so that they only include changes that may need FDA review or only include changes that do not need FDA review, where possible, so that patches that don't require FDA review are not delayed
- Avoid delaying patches that do not need FDA review until routine patches are deployed, or similar
- Avoid "bundling" or rolling together patches that may need FDA review and patches that don't need FDA review.

Summary of FDA Guidance on Patching

The FDA has provided recommendations on whether certain changes require FDA regulatory submissions in various guidance documents.

One of the first aspects MDMs will need to assess is whether the changes are considered enhancements or if they require recall reporting under 21 CFR Part 806 as outlined in the FDA guidance Distinguishing Medical Device Recalls from Medical Device Enhancements.

For cybersecurity vulnerabilities and risks, the assessment of whether changes are considered enhancements or require recall reporting is further discussed in the FDA guidance Postmarket Management of Cybersecurity in Medical Devices (hereafter referred to as the "Postmarket Cybersecurity Guidance"). The determination between whether a change is an enhancement or if it requires recall reporting is based on the assessment of whether a particular cybersecurity vulnerability presents either a "controlled" or "uncontrolled" risk of patient harm as defined in the Postmarket Cybersecurity Guidance.

- For controlled vulnerabilities, the Postmarket Cybersecurity Guidance indicates that changes made solely to address controlled cybersecurity vulnerabilities are typically considered device enhancements as defined by the FDA guidance Distinguishing Medical Device Recalls from Medical Device Enhancements and would therefore typically not require premarket submissions to the Agency or 21 CFR Part 806 recall reporting. For premarket approval (PMA) devices with periodic reporting requirements under 21 CFR 814.84, newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity routine updates and patches should be reported to FDA in a periodic (annual) report.
- For uncontrolled vulnerabilities, the Postmarket Cybersecurity Guidance indicates that changes to address uncontrolled vulnerabilities will require 21 CFR Part 806 reporting unless the enforcement discretion criteria described in the Postmarket Cybersecurity Guidance are met.

Additionally, MDMs will also need to determine whether the changes require premarket review by the Agency. This determination is described in the following guidance documents based on the associated device classification. Additional premarket submission needs may be determined based on the associated regulatory requirements (i.e., performance standards, guidelines, premarket data requirements, etc.) as specified in the special controls for the device.

- Deciding When to Submit a 510(k) for a Software Change to an Existing Device
- Deciding When to Submit a 510(k) for a Change to an Existing Device
- Modifications to Devices Subject to Premarket Approval (PMA) – The PMA Supplement Decision-Making Process

Patching Communications

To fully understand the risks that a security issue may present, it is critical that HDOs be provided with not only a given patch, but with adequate information about the patch and the risks that it is addressing.

To enable better situational awareness and more informed risk management, MDMs, other technology providers, and other parties designing patches should ensure patches are packaged with comprehensive communications. These communications may be provided prior to the patch being available, if appropriate, or packaged with the patch when it is released.

These lifecycle communications should include:

- Links to existing relevant vulnerability communications, including from the MDM/technology provider itself or from other organizations like CISA
- When the patch will be provided, if the patch is not available immediately
- If there will be limitations on who may install patches, the communication should detail approved parties
- Details on the risk that the patch is addressing
- Details on the patch itself
- Accurate patch installation time estimations
- Any post-installation testing procedures to verify that the technology continues to work as intended, the issue is resolved, and/or the risk is mitigated
- If applicable, updates to labeling, user manuals, etc.

The following resources provide more detailed recommendations on patch development procedures and best practices:

- Medtech Vulnerability Communications Toolkit (MVCT)
- Draft FDA Guidance on "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff"
- FDA Guidance on "Postmarket Management of Cybersecurity in Medical Devices"

(5) Patch Testing (Prior to Release)

It is important that patches be tested prior to their release to customers to ensure that the identified risk is mitigated and/or that the problem is resolved, and that functionality and/or performance is not negatively affected.

Potential Parties

Parties responsible for performing this testing may include:

- MDMs
- Technology providers
- Third-party component developers/manufacturers
- Contracted third-party testing services

General Recommendations

MDMs, other technology providers, and other parties testing patches should establish testing procedures, which may include:

- Module testing
- Verification testing
- Security testing (including, but not limited to, penetration testing)
- Regression testing
- Implementation and/or technical assessments
- Others as recommended by recognized standards or frameworks

The following resources provide more detailed recommendations on patch testing procedures and best practices:

- The Joint Security Plan
- UL 2900
- 81001-5-1
- IEC 62304
- The NIST Secure Software Development Framework (SSDF)

Where MDMs and other technology providers are testing patches developed by third-party component developers/manufacturers or other parties, MDMs and other technology providers should follow testing process recommendations provided by those parties in addition to their own procedures.

MDMs and other technology providers should comprehensively document this process and results, including why certain types of testing were performed and any other relevant information that may be useful to support a secure technology lifecycle.

(6) Patch Approval (If needed)

In certain cases, medical device patches may require resubmission to regulators such as the FDA. MDMs should review the "Summary of FDA Guidance on Patching" on Page 45 as well as relevant FDA guidance documents themselves, for further information.

MDMs should develop a device architecture and design patches such that regulatory review for security patches can be avoided where possible. If MDMs believe that a patch may need resubmission, MDMs should communicate that fact to customers so that reasonable expectations of patch availability and timelines are set.

Where resubmission cannot be avoided, MDMs should design and communicate to customers interim risk mitigation plans, including any recommended compensating controls. These plans should be as detailed as possible, and the mitigations should be designed to reduce risk while being as minimally disruptive to the HDO as possible.

(7) Patch Release

Once a patch has been developed and received any necessary approvals, it must be released to HDOs and other customers. This may include HDO-contracted third parties, such as ISOs.

Potential Parties

Parties releasing patches may include:

- MDMs
- Technology providers
- Third-party component developers/manufacturers

General Recommendations

The primary goal of a patch is to enable remediation of identified risks. At the same time, it is also important to ensure that patches are released using mechanisms that enable efficient and least disruptive deployment, and that comprehensive communications are provided alongside the patch that explain the associated risk, any appropriate details about the patch itself, and any appropriate details and/or recommendations about the patch installation process.

MDMs, other technology providers, and other parties releasing patches should:

- Provide comprehensive documentation that includes appropriate details about the patch, its installation process, and any other relevant information, including:
    - Information connecting the patch to the alert or notification previously sent to the HDO. For example, the communication may state something to the effect of, "[t]his patch UI12345/S/R addresses Alert 2022.12345/s/r."
    - How to determine if the patch is needed, such as through serial number identification, or if it has already been applied
    - An explanation of the issue the patch is meant to address, and how the patch does so
    - Any relevant scheduling information, especially if patches will require "sneaker-net" servicing (e.g., installation via physical presence at the device)
    - An accurate estimation of the time it will take to install the patch
    - An accurate estimation of how many reboots or other system disruptions the patch will require
    - Any verification, validation, and/or calibration procedures that the patch will require
    - Any dependencies that need to be managed, e.g., technology-to-technology or technology-to-backend, including updates to relevant security products or networking protocols (e.g., opening or closing ports)
- Ensure patches clearly indicate when they are fully installed
- Ensure all supporting functions are released at the same time where patches that need FDA review and patches that do not need FDA review are combined
- Enable remote retrieval of patches once they are released, where possible and appropriate
- Include any field change orders to ensure coordinated, validated patching
- Provide a process so that HDOs and other customers may verify patch integrity, i.e., package check-sums, CRGs, and/or code-signing[13]
- Provide an identity management process where only authorized individuals/organizations may retrieve patches, i.e., through customer portals

13 These should be restricted to cryptographic mechanisms like MACs and digital signatures (code signing). CRCs and non-cryptographically strong checksums are insufficient.

- Host patches in a secure environment to ensure the integrity of patches and the patching system itself
- Enable patches to be placed on removable media and provided to HDOs and other customers to install them at desired times, where remote retrieval is not possible or appropriate
- Design technologies to be able to check whether patches are available, where possible and appropriate

If MDMs, other technology providers, and/or HDOs and other customers leverage automated deployment systems, those systems should be validated, monitored, and "revertible" if needed. Automated deployment systems should allow users to set preferences, and the systems should not be able to override these preferences. In all cases, pre-testing before rolling out patches to all devices should be performed, rolled/staged releases should be used, and the systems should be designed so that patches may be downloaded automatically, but not installed until the user/customer acts.

A note on patch validation testing: some MDMs are beginning to design their medical devices and associated patches to enable automated validation testing, such that customers are not required to manually perform such processes. Such features may lessen the burden on HDOs and other customers in managing patch loads and may therefore be worthy of consideration by additional MDMs. However, the technologies to do so, any associated best practices, and the roles and responsibilities for managing potential risks have not been fully explored. MDMs, HDOs, and others within the ecosystem should continue to explore the feasibility and desirability of built-in, automated validation checking.

The following resources provide more detailed recommendations on patch release procedures and best practices:

- UL 5500
- UL 2900

(8) Patch Retrieval

Once a patch has been released, HDOs and other customers should retrieve the patch so that it can be tested and installed, and the associated risks mitigated in as timely a manner as possible.

Potential Parties

Parties retrieving patches may include:

- MDMs, including:
    - MDM staff for inventory not yet out in the field
    - MDM servicing staff
- Technology providers, including:
    - Technology provider staff for inventory not yet out in the field
    - Technology provider servicing staff
- Distributors, where inventory is being distributed by another party that is not the MDM or the technology provider
- HDOs, including:
    - Clinical engineers
    - System administrators
    - Network administrators
    - Application owners
- ISOs
- End users, including:
    - Clinicians
    - Patients

General Recommendations

Beyond ensuring that their processes and policies allow for timely, efficient retrieval of patches, it is critically important that HDOs and other relevant parties take into consideration potential patient care impacts, and design retrieval processes to be as minimally disruptive as possible. For example, technologies should not retrieve patches during patient treatments, as doing so may impose an added risk to patient safety should something go wrong.

Parties retrieving patches should:

- Ensure that identified applicable equipment has a patching schedule and process, which should include an existing, accurate inventory that tracks current versions of software and patches on the technologies
- Ensure patches are retrieved/received on a set schedule and that the retrieval process does not negatively impact patient care
- Favor systems (through contracting mechanisms or otherwise) that allow for remote retrieval of patches to lessen the burden patching imposes
- Ensure automated update systems, if used, are reliable, safe, and secure

- Develop and implement continuity plans to ensure that if there is an issue with a patch, patient care is not unduly impacted

(9) Patch Testing (Before Installation)

After retrieval of the patch, but prior to installation, patches should be tested. This testing helps mitigate risks that patching will cause downtime and patient care disruption.

Potential Parties

Parties testing patches may include:

- MDMs
- Technology providers
- HDOs
- ISOs, which are typically contractors of the HDO

General Recommendations

Depending on what entity (MDM, other technology provider, HDO, or ISO) retrieves the patch, that team should work with relevant clinicians to test the patch on the device prior to widespread deployment. This test can be done in several ways, depending on the architecture and infrastructure available within the HDO. Ideally and where feasible, an updated technology should be tested in a non-patient environment before widescale deployment.

If a test environment is not available, one technology should be selected and patched during a low patient volume time. The test should include clinical staff and IT staff confirmation to assure that the patch does not negatively affect the function of the technology, the environment in which it operates, or clinical workflow. If the patch is successfully tested and signed off by clinical and IT staff, then a plan can be put in place to patch all the remaining technologies.

If testing was not successful, the HDO should have a plan for what the next steps are. Ideally, the patch can be removed and the technology can be returned to service; after which, the HDO and MDM/technology provider should have a mechanism to discuss the testing/patching failure. MDMs and other technology providers should be ready to mitigate any patching issues and work with HDOs (and/or their third parties installing patches) to ensure that patching goes smoothly and does not negatively impact patient care. It is the HDO's responsibility to have a business continuity plan; however, the MDM or technology provider should be actively engaging with their customers to ensure that patches that are developed work properly and do not negatively impact technology operations. This partnership in resolving issues is critical.

The following resources provide more detailed recommendations on patch testing procedures and best practices:

- UL 2900

(10) Patch Installation

Once an HDO has tested a patch and is reasonably confident in the patch's reliability, the patch must be installed.

Potential Parties

Parties installing patches may include:

- MDMs (service technicians at HDOs, or MDM staff patching unsold inventory)
- Third parties (service technicians at HDOs, or technology provider staff patching unsold inventory)
- Distributors, where inventory is being distributed by another party that is not the MDM or the technology provider
- HDOs
- Third-party independent servicing organizations (ISOs), which may be hired by the HDO, the MDM, or other established partners
- Third-party component authors (push updates, etc.)
- End users, including:
    - Clinicians
    - Patients

General Recommendations

When installing a patch, it is important not only that the patch be successfully installed, but that doing so does not introduce patient safety risks. Where possible, organizations should design technologies and patches such that patient safety considerations are taken into account. For example, the technology can be designed to simply not allow patching activities while potentially in use with a patient or when they are needed to be available for emergency situations (i.e., emergency room (ER) and intensive care unit (ICU) technologies). Where such design considerations are not possible, organizations should ensure they have policies in place to prevent potential patient care impacts. Ideally, organizations should have both.

To guard against potential care disruptions or patient safety issues, parties installing patches should:

- Ensure that technologies retrieve patches only during identified appropriate time, such as a patch or maintenance window
- Ensure that patches cannot be applied while technologies are in use, or where updating would create a safety issue
- Check whether technologies have an auto-update capability, perform a risk assessment to determine whether that capability should be disabled, and enable/disable the capability as appropriate
- Backup configuration files, calibration data, patient data, and any other relevant files prior to installation
- Ensure that only authorized individuals may install patches
- Ensure there exists a rollback capability in case of issues

To assist with these installation best practices, MDMs, other technology providers, and others developing patches should include labeling or other appropriate documentation that clearly describes recommended update procedures. MDMs and other technology providers may also consider designing patches, where possible and appropriate, so that the technology itself backs up files and/or snapshots the system (including configuration, calibration, and patient data) prior to installation, and then deletes backed up files after successful install.

The following resources provide more detailed recommendations on patch installation procedures and best practices:

- ISO 81001
- ISO 80001
- UL 2900
- UL 5500
- NIST SP 800-40

(11) Patch Impact Assessment

After installation of a patch, it is important that it be assessed to ensure technology functionality continues as designed, that the patch has not disrupted the broader healthcare environment in which it operates, and that the patch has resolved the issue it was meant to address.

Potential Parties

Parties assessing patch impact may include:

- HDOs
- ISOs

General Recommendations

HDOs should follow their established procedures for verifying, validating, or otherwise assessing the impact of patches and device functionality. Where possible, these procedures should engage both information technology/security and clinical staff to ensure both the security and functionality of the device.

These procedures may include:

- Testing to ensure the technology functions as intended ("smoke" testing)
- Assessing whether the patch itself introduced any new risks, such as malware or unexpected communications

It is critically important that HDOs have well-documented, well-exercised plans in place for instances in which patches result in care disruption. These plans should include appropriate MDM or other technology provider contacts to ensure timely communication of any issues; these contacts may be identified in service contracts. In general, these plans may already exist as business continuity plans; HDOs should assess whether they appropriately consider disruption caused by IT or functionality outages or issues and update them if not.

To support HDOs, MDMs and other technology providers should ensure that they have established mechanisms through which HDOs may contact them to inform them of any issues, and that processes are in place for MDMs to address and ameliorate these issues within a reasonable timeframe.

D. Future Proofing

The majority of this document has focused on managing the risks posed by "current" legacy technologies: those technologies that are already deployed in healthcare environments, and which have already reached their declared EOL date, or otherwise may be unsupported or contain unsupported technologies. But the reality of continued technical advancements in the delivery of care, and in the simultaneous evolution of cyber threats, means that all technologies will one day be "legacy." As such, this section of the document focuses on "future" legacy

technologies: those technologies that do not yet meet the recognized "legacy" definition, but one day will.

Improving the way technologies are designed, deployed, and maintained is critical to meaningfully addressing the legacy technology challenge overall. The healthcare sector faces a significant legacy technology challenge because many current legacy technologies were not designed securely from the start, nor were they designed to remain secure over time. Unless and until this changes, the healthcare sector will remain caught in an endless loop of insecure and unsecurable "future" legacy technologies becoming insecure and unsecurable "current" legacy technologies, and it will remain exposed to the increasingly severe cybersecurity risks that such legacy technologies pose.

This section contains discussion and recommendations for how to improve policies, practices, and procedures for designing, deploying, and maintaining technologies used in healthcare environments so that the factors that contribute to making technologies "legacy" are mitigated and made manageable to the greatest extent possible. It includes legacy-specific recommendations related to:

- Threat modeling considerations
- Secure technology design, including software selection
- Secure technology deployment

1. Recommendations for Addressing Known Legacy Issues During Threat Modeling

To mitigate legacy technology risks, organizations should understand what those risks are or might be. Consequently, organizations should incorporate comprehensive threat modeling practices into their design procedures and consider sharing a summary of the results with customers. To specifically address current and future legacy technology risks, these practices should include considerations of:

- New and emerging cyber threats that may require mitigation measures such as software or hardware updates. Organizations may wish to consider implementing "modular" designs to facilitate this need.
- Components becoming unsupported, as a lack of support from upstream vendors, including software developers, may pose serious risks if vulnerabilities arise and fixes are unattainable. This may include planned EOL activities, as well as unplanned EOL or EOS announcements.

- Unauthorized access, such as cyber threats that may attempt to steal data, perform unauthorized functions, or install unauthorized software (e.g., ransomware), among others.
- Environmental or network "noise," as modern networks are inescapably "noisy," with purposeful, accidental, and potentially malicious scanning activities occurring regularly. Technologies must be resilient to such scanning and "noise," regardless of its origination. In particular, organizations should design technologies against:
    - Loss of essential functionality;
    - Denial of service;
    - Degraded performance;
    - Accidental information disclosure; and,
    - Others as relevant.
- Data confidentiality, integrity, and availability, as the delivery of care relies on the timely accessibility of accurate information, whether via manual retrieval (e.g., a clinician looking at a scan) or automated inputs and outputs (e.g., technologies retrieving and writing patient information to electronic health records). Further, patient privacy is critically important, and designs should ensure appropriate safeguards, including through encryption both at rest and in transit, and/or access control mechanisms.
- System-level risks, such as network or cloud outages where the technologies rely on distributed systems.
- System-of-system level risks, as many system-based technologies may themselves rely on other systems. Outages, security risks, and other issues to one system may pose risks to other, interconnected or interrelated systems.
- Physical security, as there are ways to impact the security of a technology using physical access (e.g., removing power, replacing a memory card, removing a hard disk). Organizations should consider potential limitations on customers' ability to prevent unauthorized physical access. Further, organizations should not discount the threat of simple theft: as noted by one working group member, "if it can be stolen, someone will try."
- All-hazards risk management, as non-cyber hazards such as power outages, weather events (e.g., hurricanes, wildfires), and others may impact the ability of technologies to continue to operate safely.

- Indirect cybersecurity risks, such as situations where security controls may introduce patient safety risks, such as unacceptable system latency. In addition, there may be situations such as those involving physical safety interlocks, where the possibility that an interlock may be overridden by cyber means may introduce serious safety risks. For example, in certain types of surgery, the use of both ventilators and lasers may be necessary, with interlocks imposed in between to keep the two from interacting. Given that ventilators create an oxygen rich environment that may then be combusted by a laser, appropriate threat modeling considerations in such designs would consider the risks of interlocks being overridden by cyber threats.

a) Threat Modeling Procedure Recommendations

When developing threat models, organizations should consider standardizing the granularity of modeling detail so that it will align with the level of detail provided by recognized vulnerability resources. This allows for ease of identifying where in the threat model a published vulnerability or other risk may reside.

(1) Describing Components within Threat Models

To the extent that open source or third-party components have already been identified, organizations may wish to standardize around the Common Platform Enumeration or "CPE" format[14], since this could enable a level of abstraction of their threat model to facilitate rapid integration of newly published vulnerabilities into that model. Once the vulnerability is appropriately localized in the threat model, analysts could then have a much more efficient and effective way to determine whether a given vulnerability is, in fact, an exposure in that particular application context. Ideally, this would also be consistent with how software components are identified in the organization's SBOMs, so that artifacts like the SBOM and techniques like threat modeling can seamlessly support vulnerability management.

(2) Describing Vulnerabilities and Weaknesses within Threat Models

When describing their own in-house-developed or first-party custom software in their threat model, organizations may wish to consider standardizing in the same ways, so that Common

14 https://nvd.nist.gov/products/cpe

Weakness Enumerations (CWEs)[15] can be readily associated with the organization's custom software components and also be readily mapped into the threat model and regularly surveilled as potential targets for exploitation. When describing vulnerabilities within their threat models, organizations may wish to standardize around the Common Vulnerabilities and Exposures or "CVE" format[16], and use standardized sources of vulnerability information like the National Vulnerability Database or "NVD."[17]

For additional recommendations and best practices related to threat modeling, see Playbook for Threat Modeling Medical Devices.

2. Recommendations for Secure Technology Design, Including Software Selection

A fundamental challenge with many technologies used in healthcare environments is that the lifecycles between the software and hardware included in devices often don't align, introducing a functional and economic bifurcation in technology management. This can occur because:

- The lifecycle events leading to a need for hardware replacements occur less frequently than the need for software updates (e.g., to address software vulnerabilities).
- Software often can be updated more easily than hardware.
- Software update requirements may surpass available hardware capabilities.
- The cost and feasibility of updating can be limiting.
- There may exist limitations on the ability to affect clinical factors like workflow or training, since updating may require workflow changes.

Where possible and appropriate, MDMs and other technology providers should consider moving toward designs that better harmonize the lifecycles of software and hardware to mitigate some of this bifurcation. In addition, MDMs and other technology providers should, where possible and applicable, consider how technologies used in healthcare environments can be designed to accommodate security features according to user specifications. Overall, technologies should be designed to be secure when released and securable over time.

15 https://cwe.mitre.org/about/index.html

16 https://www.cve.org/About/Overview

17 https://nvd.nist.gov/

MDMs are currently required to adhere to the Quality Management System regulations. Security considerations are part of risk management and should be mapped to and incorporated into quality management compliance activities. To facilitate this goal, MDMs should use a secure product development framework (SPDF) that incorporates security considerations throughout the lifecycle of a device, such as the risks and capabilities that the device has or may encounter. While other technology providers may not be required to meet Quality Management System security considerations, they should consider using an SPDF to facilitate effective risk management.

To design secure technologies, MDMs and other technology providers should:

- Design technologies so that software, hardware, and other components can be updated or replaced during the technology's lifecycle. For example, MDMs and technology providers may consider:
    - Forecasting for software, hardware, and other component end-of-life during technology lifecycles, and designing and executing plans to address EOL concerns. MDMs and other technology providers should communicate these plans to their customers as appropriate. Such forecasts should consider:
        - Shipping technologies with supported operating systems and other software. This may require identifying EOL/EOGS/EOS dates and ensuring development cycles account for necessary updates, as well as updating inventory before it is sent to customers.
        - Identifying and addressing potential cloud computing maintenance and EOL issues, such as the security and support status of microservices from the cloud service provider, and/or applicable Software as a Service (SaaS) and/or Platform as a Service (PaaS) functions. See Section VII.C.1.b)(1)(b) for specific recommendations on how to incorporate such considerations into procurement processes.
        - Identifying and addressing potential implantable medical device issues, recognizing that these devices are physically implanted within a patient's body, and therefore that special consideration needs to be given to how security, update, and other functional capabilities are designed and maintained over the lifecycle of the device. Designs should be developed to minimize to the greatest degree possible any surgical intervention necessary to actually access the physical device to fix potential issues.

    - Designing technologies for modularity, such that software, hardware, and other components may be independently updated without forcing the obsolescence of other components or the technology itself.
- Design technologies to facilitate customer regulatory and other legal requirements, such as HIPAA or Joint Commission requirements.
- Design technologies and systems which leverage cloud or other distributed functions so that they may operate in multiple environments, such as on-premise or cloud, and may be migrated between environments as infrastructure needs and strategies change.
- Design any data formats associated with technologies and their dependent systems in a way that reasonably preserves the data formats' usability and accessibility over time. This includes encryption protocols.
- Design technologies to leverage standards-based protocols that are supported and are likely to remain so, and implement evaluation processes to reassess their suitability over time, and replace as possible and/or needed.
- Develop or conform technologies to security baselines based on the technologies' risks and capabilities, preferably those that are known and/or publicly recognized.
- Design technologies to include detection and monitoring capabilities, so that they may fail safely and securely in response to cyber incidents.
- Design technologies so that they may preserve and/or communicate security notifications (e.g., software updates) and other security events that can be integrated into the larger system's event monitoring software, an independent capability, or another mechanism.
- Disclose any security control design limitations that exist "out of the box."

a) Recommendations for Selecting Software

Because many technologies used in healthcare environments rely on software in order to safely and effectively perform their clinical functions, it is critical that MDMs and other technology providers carefully consider the software that they integrate into their designs.

This document has discussed in detail many types of legacy "pressures" that arise over the lifecycle of a given technology, including EOL/EOGS/EOS declarations, unknown software supply chain and dependency issues, and a lack of updatability, among others. To anticipate, and to the greatest extent possible minimize, these future legacy pressures, MDMs and other technology providers should prefer software suppliers that:

- Provide ongoing software support (e.g., security updates) and indicate support milestones, including EOL/EOGS/EOS dates.
- Provide software supply chain information, including licensed dependencies.
- Provide necessary documentation to support MDM risk management and regulatory compliance.
- Engage in collaborative exchanges regarding the MDM's design and secure architecture requirements, specifically so the software supplier understands the desired end use of the product in the healthcare ecosystem and may be able to advise and/or make targeted changes to their product to address any relevant considerations (such as extended anticipated lifetimes, certain security controls, etc.).

Legacy pressures also arise from more general risk management challenges. Technologies that were not designed using secure development practices may be more prone to vulnerabilities or other security issues that may render them "legacy" unexpectedly, and MDMs or technology providers (including software developers) that lack robust cybersecurity risk management programs may not be able to address incidents or vulnerabilities that may impact their products, and that in turn impact MDMs, HDOs, and other healthcare stakeholders. Conversely, organizations with mature, sophisticated cyber risk management programs are more likely to be able to successfully address cyber threats that could—in the absence of such capabilities—translate into drivers of legacy challenges.

Consequently, to further anticipate and to the greatest extent possible minimize future legacy pressures, MDMs and other technology providers should prefer software suppliers that proactively engage in cybersecurity risk management activities, such as suppliers that:

- *Risk Management*
    - Identify possible risks and outline ways to eliminate or mitigate them.
    - Provide a consistent framework for assessing exploitability of a vulnerability.
    - Develop a formal supply-chain risk management program, including supplier validation, security in contracting, security testing, auditing, milestone management, and provision of supporting security documentation.
    - Participate in Information Sharing and Analysis Centers/Organizations (ISACs/ISAOs), including those specifically focused on healthcare and those focused on technology risks more broadly.
    - Engage and/or provide collaborative audit disclosures and/or cybersecurity assurance program results.

- *Secure Software Development Processes*
    - Maintain cybersecurity certifications or comply with cybersecurity standards.
    - Have a process that outlines the use of industry standard secure design elements, such as malware protection, Host Intrusion Detection and Prevention (HIDS/HIPS), and system hardening.
    - Provide for secure environments used for designing, developing, manufacturing, and distributing products/components.
    - Provide for regular security patching and data backup.
- *Vulnerability Management*
    - Provide a mechanism for external parties to report vulnerabilities (i.e., complaints, coordinated disclosure).
    - Provide a mechanism for disclosing to and working with MDMs and other technology providers prior to public disclosure, to ensure MDMs and technology providers can adequately assess and address risks.
    - Provide for the monitoring of software components for vulnerabilities.
    - Have a process for providing risk assessment, compensating controls, and planned mitigation.
    - Have a process for the disclosure/notification of known vulnerabilities/exploits.
    - Have a history of addressing known exploited vulnerabilities.

Moreover, MDMs and other technology providers should prefer software suppliers that are willing to disclose comprehensive information on how they perform cyber risk management, such as the elements listed above.

Other factors that MDMs and other technology providers may want to consider when selecting software may include suppliers that:

- Have a documented product cybersecurity program in compliance with all applicable laws, rules, and regulations.
- Prefer software suppliers that allow for the escrow or backup of code to enable risk management activities, such as responding to code corruption, deliberate tampering, or the closing down of businesses or disappearance of publicly available code.

It is important to note that this list of recommendations is not comprehensive; MDMs and other technology providers may identify additional preferences or considerations for software suppliers based on their own business needs, experiences, or for other reasons. In addition, it is likely that many software suppliers—even the most sophisticated ones—will not meet all of the

listed recommendations. Where a supplier's cyber risk management or other practices are insufficient according to MDM or technology provider policies, MDMs and other technology providers should implement supplier management best practices to fill in gaps.

Note that using software suppliers that meet these criteria does not absolve the MDM or other technology provider from performing a comprehensive risk assessment for their technology.

b) Alignment with Executive Order 14028 on Improving the Nation's Cybersecurity

Many of the elements listed in this subsection are requirements identified by Executive Order 14028 on Improving the Nation's Cybersecurity. Consequently, integration of these recommendations into MDMs' and technology providers' own software development practices, as well as their supplier management practices, may facilitate compliance with the EO, and/or create opportunities to "reuse" EO compliance efforts and artifacts for legacy risk management practices. It may also create opportunities to leverage existing or future tools, frameworks, or other mechanisms related to EO compliance for the purposes of legacy technology risk management. For example, the NIST guidance on "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities" was written in direct response to the EO, and provides significant detail and resources for EO compliance.

3. Recommendations to Facilitate Secure Technology Deployment

While it is critical that technologies are designed to be secure and securable over time, it is equally critical that they also are designed to be deployable in a secure and securable manner. Existing FDA guidances, as well as best practice documents like the Joint Security Plan and NIST CSF, ISO 80001, and the H-ISAC Medical Device Cybersecurity Lifecycle Management paper, provide overall recommendations for how to accomplish these goals. Technologies should be capable of operating within existing security structures, and consequently those security operations should not lead to hindered operations in the technology. The bullets below identify secure technology design recommendations to facilitate secure technology deployment:

- Follow supply chain best practices including for components that facilitate and support integration and deployment
- Design technologies to enable strong and adaptable authentication mechanisms that balance security and care delivery workflows. HDOs may have preferred security

mechanisms; however, they may not always provide for the best system design or application in a clinical or laboratory workflow. If certain security features are disabled by default, the HDO can enable them to fit their environment. For example, multifactor authentication may be inappropriate in some clinical use cases, but proximity-based access technology "badge-and-go" may be more appropriate. In addition, for remote service access multifactor authentication is more appropriate.

- Design technologies so that they are hardened by design, and so that they may be hardened further in the deployment process, and that the procedures for hardening[18] the technologies may be updated over time to address emerging risks. The Joint Security Plan offers significant details around how to harden and design a hardened technology, with appropriate standards references. Software vendors may provide hardening guidelines for their platforms, operating systems, databases, etc.
- Enable deployed enterprise security tools to interface with technologies to perform logging, auditing, or other security functions.
- Where feasible and appropriate, facilitate the use of security agents on technologies, where those agents appropriately consider potential patient safety impacts. This could include:
    - Designing and maintaining MDM or other technology provider versions of security agents;
    - Maintaining a list of MDM- or technology provider-approved third-party agents and their versions and regularly communicating these lists to HDOs;
    - Enabling the installation by HDOs of approved agents.
- Produce and communicate regularly updated and versioned MDS², SBOM, and relevant vulnerability information (e.g., VEX) as product updates and maintenance cause changes.
- Design flexible financing options for technology security capabilities and features, including patching, such that they can either be covered up front during the purchase of the technology (capital expenditures) or amortized over the lifecycle of the technology (operational costs). Organizations may wish to examine the HSCC Model Contract-Language for Medtech Cybersecurity (MC2) resource for examples.

18 Hardening, when applied to computing, is the practice of reducing a system's vulnerability by reducing its attack surface. Hardening may involve a reduction in attack vectors by culling the pathways, or vectors, attackers would use. UL 2900.

- Provide appropriate documentation to HDOs, such as network diagrams, data flow diagrams, and technical specifics. The labeling section of the 2022 draft FDA Premarket Cybersecurity Guidance provides a robust list. Recognized consensus standards and existing types of documentation, such as MDS² forms, SBOMs, and others, may capture some of this information.

VIII. Challenges and Recommendations

The previous section described the four "pillars" of a successful legacy technologies management program, and discussed the considerations and recommendations related to each. This section identifies individual issues that organizations managing legacy technologies may encounter, and provides recommendations for addressing, mitigating, or otherwise responding to them. It is important to note that not all of these recommendations will apply all of the time, to every technology. Organizations should consider the recommendations within the context of their own environments, assets, and resource constraints, among others.

They are listed in alphabetic order, and broken into several sections: a general description of the issue, relevant information to consider, and recommended best practices targeted at either HDOs, MDMs, or both.

A. Connectivity

Today, many technologies used in healthcare environments provide connectivity to additional public and private technologies and networks. Some technologies, especially old technologies, may not have been designed to accommodate the secure connectivity required in healthcare today. Healthcare provider networks may host a combination of connected medical devices, business technology, and IoT devices, which can create potential threats. Managing connectivity plays a crucial role in maintaining a secure environment.

Subtopic #1: A technology was not designed to connect to a network.

Many older technologies were not originally designed to connect to a network, or were designed to connect only to local networks. However, as health provider needs changed, the technologies may have been retrofitted to allow for greater connectivity. As a result, the retrofitted

technologies may be exposed to modern security threats they were not designed to defend against.

Recommendations for MDMs:

- Provide information to the HDO about how to securely connect the technologies to their network, if possible. This information should include any limitations or concerns related to technology behavior during network scanning.
- If secure connection is not possible, provide the HDO with appropriate compensating controls or any available mitigation information.
- If secure connection is not possible, provide the HDO with information regarding potential technology replacement/upgrade options, such as available technologies that possess the desired connectivity, clinical features, and other capabilities.
- Ensure sales, marketing, and other teams within the MDM or other technology provider have all necessary information on relevant connectivity limitations, so that they may appropriately advise or inform customers.
- Before retrofitting a technology for connectivity, perform any necessary analyses (including threat modeling) to ensure risks are understood and mitigated to an acceptable level.

Recommendations for HDOs:

- Ensure technologies are deployed according to MDM or other technology provider security documentation, where possible.
- Request information from MDM or other technology provider about how to securely connect the technologies to a network, if possible. This should include requesting information about technology behavior related to network scanning.
- Request any available mitigation information from the MDM or other technology provider
- Request available information regarding potential technology replacement/upgrade options, such as available technologies that possess the desired connectivity, clinical features, and other capabilities.
- Where there is sufficient need or benefit for connectivity, prioritize technology replacement.
- Ensure technologies are kept fully patched. In particular, before connecting technologies that have not been connected previously, apply all relevant patches.

- Assess and implement technical exposure reduction measures, e.g., network segmentation, firewalls, or passive network monitoring tools.

Subtopic #2: A technology was not designed to accommodate remote management.

Some technologies were not designed to allow for remote management of the technology. This makes distribution and installation for software updates, firmware updates, and security patches more difficult because the process requires additional, manual steps to perform. For instance, these update types may require that an individual be physically present in front of the technology to perform the update.

Recommendations for MDMs:

- Provide information to the HDO about if and how update responsibilities are shared between the MDM and HDO.
- Provide information about where, how, and the frequency with which update information will be communicated.
- Ensure methods for maintaining technologies, including providing updates, are agreed-upon.
- When using portable media to provide updates, such as USBs, ensure appropriate risk management measures are in place and are followed.
- Provide HDO information regarding potential technology replacement/upgrade options, such as available technologies that possess the desired connectivity and other features.

Recommendations for HDOs:

- Ensure technologies are deployed according to MDM security documentation, where possible
- Request information from the MDM or other technology provider about if and how update responsibilities are shared between the MDM, other technology provider and the HDO
- Request the MDM or other technology provider to indicate where, how, and the frequency with which update information will be communicated
- Request available information regarding potential technology replacement/upgrade options, such as available technologies that possess the desired connectivity and other features

- If the original manufacturer of a technology is unable to provide assistance for whatever reason (e.g., has gone out of business):
    - Evaluate the needs of the organization and the risk of continuing to use the device
    - Implement risk management measures, such as leveraging a third-party support service or implementing compensating controls
- Assess and implement technical exposure reduction measures, e.g., network segmentation, firewalls, or passive networking monitoring.

Subtopic #3: A technology deployment network hosts a combination of technologies with different connectivity requirements.

In most hospital environments, IT networks will contain many technologies with a wide range of connectivity requirements. This scale and variability can lead to security oversights and, potentially, contradicting security recommendations between technology providers.

Recommendations for MDMs:

- Provide information to the HDO about how to securely connect the technologies to their network, if possible, including but not limited to:
    - Ports required for functionality, as well as any other ports that may be enabled, and whether they may be safely disabled
    - Whether there exist default passwords, the passwords themselves, and procedures for changing the passwords, if possible
    - Whether USB connections are enabled by default, and how to adjust their settings
    - Any encryption that is deployed, including at rest and in transit
    - Whether there are logging/auditing features, and how to access/configure them if so
    - Others as relevant[19]
- If secure connection is not possible, provide the HDO any available mitigation information.
- Provide HDO information regarding potential technology replacement/upgrade options, such as available devices that possess the desired connectivity and other features.

19 See, e.g., the FDA Draft Premarket guidance re: labeling.

Recommendations for HDOs:

- Assess and implement technical exposure reduction measures, e.g., network segmentation or firewalls, where possible
- Ensure technologies are deployed according to MDM or other technology provider security documentation, where possible
- Request information from MDM or other technology provider about how to securely connect the devices to your network, if possible
- Request available information regarding potential technology replacement/upgrade options, such as available technologies that possess the desired connectivity and other features
- Prioritize technology in replacement planning
- Ensure technologies are kept fully patched. In particular, before connecting technologies that have not been connected previously, apply all relevant patches.
- If the original manufacturer of a technology is unable to provide assistance for whatever reason (e.g., has gone out of business):
    - Evaluate the needs of the organization and the risk of continuing to use the technology
    - Implement risk management measures, such as leveraging a third-party support service or implementing compensating controls

B. End of Life/End of Guaranteed Support/End of Support (EOL/EOGS/EOS)

Healthcare technology ecosystems are not static. Advances in care delivery and quality are constantly being made, encouraging the adoption of new processes, procedures, and - highly relevant to the legacy challenge - technologies. Simultaneously, cyber threats and the broader threat landscape continue to emerge, with their sophistication, potential severity, and associated tactics, techniques, and procedures always evolving. As a result of these and other pressures, either separately or in combination, technologies in healthcare environments become outdated, unsupported, and increasingly vulnerable to cyber or other incidents.

To address these pressures, both from a risk management standpoint (mitigating cyber and other threats) and from a commercial perspective (encouraging adoption of newer technologies), many MDMs and other technology providers will establish end of sale, EOL, EOS, or EOGS dates. These dates represent the point after which - absent extenuating

circumstances and depending on which type of date is declared - the MDM or other technology provider will no longer provide support to the technology, including security patches or other mitigations for cyber threats.

This creates challenges for HDOs, as financial, workflow, or other pressures may slow (or prevent) the adoption of new technologies within their environments.

This topic provides recommendations targeted at addressing three of the most common EOL/EOS challenges. For a more comprehensive discussion of the challenges and additional recommendations, see Section VII.C.3.

Subtopic #1: Recognize EOL, EOS, and/or EOGS dates.

Prior to the medical technologies becoming outdated or obsolete, it is important to recognize the rationale for medical technologies falling into the categories of end-of-life or end-of-support and end-of-guaranteed support. The rationale includes:

- business and/or strategy changes regarding product support.
- new technology is now available to support better patient outcome(s)
- third-party hardware, operating systems, and software components are no longer available and/or supported
- suppliers of third-party components and software are unable or unwilling to technically mitigate identified vulnerabilities
- technologies were designed at a time when modern cybersecurity best practices were not recognized or broadly adopted.

Technologies used in healthcare environments may therefore be declared EOL/EOGS/EOS for any one or a combination of these reasons.

This section provides recommendations for MDMs and HDOs as they become aware of the EOL/EOGS/EOS of the relevant technologies or software.

Recommendations for MDMs:

Technologies used in healthcare environments, including software as a medical device (SaMD) or software in a medical device (SiMD), integrate third-party software, open-source software, and hardware components. It is important to address the following and partner with the HDO where applicable:

- Changes or unique set up and configuration for medical technologies should be shared with the HDO where possible by the MDM. See Section VII.B and Section VIII.D for specific recommendations related to communications, labeling, and other documentation.
- Contracts between HDOs, MDMs, and other technology providers should include language specifying support timeframes, as well as identified points of contact for each party.
- Contracts with the third-party suppliers should include language to support remediation of vulnerabilities
- Criteria and choice of third-party suppliers should include, where possible, the supplier having a vulnerability policy and process to communicate and support mitigation of identified vulnerabilities
- Design of technologies used in healthcare environments where possible should consider the impact of third- party software vulnerabilities (e.g., performance, support, etc.) on decisions of EOL/EOGS/EOS
- Where possible, communicate EOL/EOGS/EOS dates to HDOs and provide any associated rationale. This communication should ideally take place at least three years prior to the EOL/EOGS/EOS date. Where known, EOL/EOGS/EOS dates should be communicated as early as possible.
    - While it is not always possible to definitively identify the expected timeline for support for every software/firmware component, the MDM or other technology provider should make every effort to make estimates and align this with the scheduled EOL/EOGS/EOS date.
- Best practices identified by the IMRDF recommend against selling medical devices that receive limited support, such as those nearing their EOL/EOGS/EOS dates.
    - MDMs and other technology providers should avoid selling technologies close to EOL/EOGS/EOS dates, where possible.
    - If MDMs or other technology providers choose to sell technologies close to EOL/EOGS/EOS dates, they should be transparent about the support status and the associated limitations, and they should include information related to a technology replacement or other upgrade paths.
- In cases where MDMs or other technology providers are providing replacement technologies or components to HDOs due to device failure or uncontrolled vulnerabilities that cannot otherwise be mitigated:

- Where possible, do not replace a technology with one close to EOL/EOGS/EOS dates.
- If it is not possible to avoid replacing the technology with one close to EOL/EOGS/EOS, be transparent about the support status and the associated limitations, and they should include information related to a technology replacement or other upgrade paths.

Recommendations for HDOs:

The technologies that are integrated into the HDO environment come from various manufacturers and cover a realm of software and hardware technologies. Given the continuously evolving threat environment and the number of technologies that exist within a given healthcare environment, partnership between HDOs, MDMs, and other technology providers is critical. It is important to address:

- HDOs should articulate their post-EOL/EOGS/EOS risk management processes with MDMs and other technology providers, to facilitate risk management efforts. Ideally, this process should be established during the acquisition stage. See Section VII.C.4 for additional details and recommendations.
- Third-party systems may exist that are integrated into HDO environments, but that are not owned or maintained by the MDM or other technology provider, and which interact with MDM or other technology provider products. In such cases, ensure that the HDO, MDM, or other technology provider is aware of these third-party systems, and define and agree to roles and responsibilities for managing any associated risks, including vulnerability and incident management and communication of EOL/EOGS/EOS dates.
- Decide whether to retain or decommission a certain technology past EOL/EOGS/EOS based on a thorough risk analysis that accounts for current and potential cyber threats. See Section VII.C.4 for additional details and recommendations.
- Best practices identified by the IMRDF recommend against purchasing technologies that receive limited support, such as those nearing their EOL/EOGS/EOS dates.

Subtopic #2: Plan for EOL/EOGS/EOS

Technologies used in healthcare environments, whether they are new or approaching EOL/EOGS/EOS, have software and third-party components that require continuous lifecycle monitoring. It is important that HDOs, MDMs, and other technology providers have robust plans for identifying, tracking, and addressing EOL/EOGS/EOS technologies in their environments. Without such plans, organizations will be hindered in planning for the

procurement and ongoing maintenance of technologies that may pose a risk to their environments.

Recommendations for MDMs:

MDMs should:

- Share their EOL/EOGS/EOS policy during the sales process as relevant to in-scope technologies, including but not limited to:
    - The MDM or other technology provider's usual process for when EOL/EOGS/EOS is announced
    - How support processes work
    - What might happen if circumstances force an unexpected EOL/EOGS/EOS
- Execute the policy throughout technologies' lifecycles by communicating to the HDO the status of EOL/EOGS/EOS of individual devices
- Include EOL/EOGS/EOS strategy and plan as part of their design control documents to include EOL/EOGS/EOS dates for all products and components including products obtained from third-parties.[20]
- Update and provide all relevant and validated security information (such as segmentation guide, port blocking, application allow-listing, etc.) and documents including MDS², SBOM, and service manuals to customers
- Perform risk assessments evaluating technology risk, including actual or approaching EOL/EOGS/EOS status, as well as remaining clinical benefits to inform HDO, MDM, and other technology provider lifecycle planning
- Disclose any relevant policies related to risk/responsibility transfer
- Provide any necessary documentation, information, or other materials to HDOs to enable their continued operation, support, and appropriate patching of technologies, such as encryption keys or digital signature capabilities, among others.

Recommendations for HDOs:

HDOs should:

- Communicate with the MDM on status of EOL/EOGS/EOS
- Acknowledge EOL/EOGS/EOS status

---

20 FDA premarket guidance.

- Review the MDS²/SBOM and work with the MDM or other technology provider for any unique configuration needs
- Investigate and implement compensating controls for technologies that operate on unsupported software, due to the lack of software updates and patches for obsolete software.
- Consider risk/responsibility transfer (see section, cross-reference)
- Consider replacing technology

Subtopic #3: Transfer of responsibility option after technologies have been declared EOL/EOGS/EOS or otherwise become legacy

It is important to consider that, even after a technology has been declared EOL/EOGS/EOS or has become legacy, it may still have useful life from the HDO perspective due to various factors. These factors include, but are not limited to: the technology still performs the clinical function for which it was purchased; the cost of replacing the technology; the technology becoming EOL/EOGS/EOS out of sync with the organization's established procurement cycle; and/or a lack of available alternatives to that technology.

Recommendations for MDMs and HDOs:

- Put in place formal processes for undergoing responsibility transfer
- See Section VII.C.4 for specific framework and recommendations

C. Third Party Servicers

Managing the risks inherent in legacy technologies can be challenging, especially for smaller and mid-sized manufacturers and HDOs. Qualified third-party servicers, such as Independent Service Organizations (ISOs) and Managed Security Service Providers (MSSPs), may be able to augment resources, expertise, and experience, as frequently these third-party servicers may be familiar with legacy equipment, having serviced it for other smaller HDOs or under MDM or other technology provider multi-vendor programs.

Although there is no "one size fits all" answer, the following list includes a few areas where leveraging third-party servicers may be useful:

Security Management:

- Security assessments:

    - Vulnerability scan, pen testing, etc.
    - Collection of security-relevant inventory data
    - Security risk assessment
    - Security maturity assessment
- Compliance assessments
- Establish best practices to address common security processes:
    - General legacy management
    - Security maintenance and patching, etc.
    - Secure network architecture and management best practices
    - Site installation procedure
- Improve risk visibility and create central repository of security-relevant information:
    - Create and maintain repository of security documentation, MDS², SBOM, test results, other security relevant information (e.g., vendor provided risk assessment), etc.
    - Enable automation – SCA tools, OWASP Dependency track/check; spreadsheets are not ideal
    - Enable standard approach – NTIA Working group (SWID, SPDX, CycloneDX)

HDO/MDM/Other technology provider communication:

- Managing, interpreting, and guiding on security documentation sharing between MDMs and HDOs.
- Postmarket support, e.g., support vulnerability information sharing and management.

Administrative:

- Staffing and security expertise:
    - Staff augmentation and outsourcing
    - Cybersecurity technical and process training
    - Security certification
- Pre-procurement and procurement support:
    - Security contract language
    - Vendor and supplier security risk assessment
    - Pre-procurement risk assessment
    - Capital planning to identify legacy risks and include legacy risk reduction in long term replacement planning
- Security policies and best practices

Financial:

- Third parties can help bridge funding gaps, e.g., mitigate cost of chargeable upgrades
- Offer purchasing options, e.g., lease vs. purchase or other models to help with legacy replacement cost mitigation
- Provide purchase-supporting services: SBOM review, contract review, security postmarket surveillance data collection, maintenance and upgrade plans and patch update plan (including OS, COTS, and SOUP).

When organizations leverage third party servicers, it is important to ensure that relevant partners are made aware of who the third party is, what the scope of their responsibilities are, and who the appropriate points of contact are at both the hiring organization and the third party. This can include the third-party receiving patches or other vulnerability information on behalf of the HDO, or communication with MDMs or other technology providers to coordinate a vulnerability response, among other potential examples. For additional information and recommendations regarding potential contracting issues, see the HSCC Model Contract-Language for Medtech Cybersecurity (MC2).

Organizations should note there is a lack of clarity regarding the distinction between "servicing" and "remanufacturing" of a device, and that remanufacturing has implications for the regulatory responsibilities of entities performing these activities. Organizations should consult the FDA remanufacturing guidance when it is finalized for additional information on how to manage roles and responsibilities to ensure that any third-party servicing activities are consistent with organizational policy.

D. Inventory/Asset Management

Complete visibility of the general IT inventory, other technologies used in healthcare environments, physical medical devices, and specifically the software-based medical device inventory is a prerequisite for any effective asset and cybersecurity management program. This inventory should include non-medical device Internet of Things (IoT) and other connected devices that sit on an HDO network. It provides an essential baseline for managing a technology security posture and is directly related to:

- Risk management
- Incident Response

- Vulnerability Management
- Maintenance and change management
- Replacement planning and procurement
- Decommissioning

Appendix 1 – Example Technologies Used in Healthcare Environments includes additional information on the types of technologies that HDOs may need to consider.

To be successful, HDOs need to develop a set of risk-inclusive and security-centric asset management policies and processes accompanied by the appropriate tools, resourcing, and staff.

Subtopic #1: Asset Visibility

Asset visibility must be comprehensive in breadth (visibility of all assets), depth (identification of all security-relevant parameters), accuracy (correct identification and categorization), and be up-to-date/current. Without an inventory that maintains these characteristics, all subsequent security and risk-based decisions may lead to additional or unintended risk, incorrectly applied remediation, incomplete risk mitigation, or missed technology criticality prioritization, among other concerns. Further, ongoing changes require that the inventory be regularly updated to remain accurate.

In practice, the inherent complexities of the healthcare environment and tool insufficiency provide challenges. Asset management tools commonly used in the IT environment struggle to identify IoT and medical devices accurately and effectively. Traditional maintenance and inventory management tools (e.g., CMMS) may not have the capabilities required to collect data on device software and security posture. Passive network monitoring tools focused on IoT and medical devices are relatively new in the marketplace, and are continuing to mature.

Recommendations for HDOs

HDOs need to look for a combination of core functionality that integrates asset management and passive network monitoring tools (PNM). Assets may be tracked in a CMDB, CMMS or full Asset Management system, with each class of system providing increased capabilities for the management of all security-relevant parameters. The introduction of PNM solutions has increased the automated profiling of all the technologies on the network, and continuously updates technology communication profiles.

From a cybersecurity perspective, the following data classes should be collected through automated systems (preferred) or manual processes. Other, non-security parameters are not listed.

- Technology identifiers (name, make, manufacturer, model, S/N, AE Title, firmware, etc.)
- Technology version and version of key software components (e.g., operating system)
- Technology network identifiers (IP, MAC, Wi-Fi, Serial-to-Ethernet Bridge, Serial Connection, Dual NIC Capable, Bluetooth, etc.)
- Technology interfaces (including which are enabled by default, current status (enabled/disabled), function/purpose, etc.)
- Technology network credentials
- Technology data storage (type and retention)
- Types of data stored on, accessible by, or transmitted by the technology (e.g., PHI, PII, credit card data or other financial information)
- Technology cryptographic capabilities for data at rest and data in transit
- Upgrade/update/patch status
- Supplemental information for cybersecurity (e.g., antimalware type, HIDS/HIPS/allow-listing, and status)
- EOL/EOGS/EOS information for technology or key software component, as well as potential legacy status
- Information on patch/update mechanisms and delivery
- System and IT dependencies
- Ownership, location, and security responsibility
- Vendor information including security contacts
- Supporting vendor documentation (e.g., MDS^2, SBOM)
- Whether the asset may have physical security requirements, such as guards against theft (e.g., locks or special tools).
- Whether a connection occurs to endpoints outside of facility (e.g., cloud, MDM server) and whether this connection is required for technology operation
- Other cybersecurity components/characteristics as relevant, and/or as they evolve

Subtopic #2: Unified Asset Management

Where possible, HDOs should attempt to take advantage of a single source of truth on their organization's entire IT & OT and Internet of Things (IoT) ecosystem, thereby empowering IT, HTM, and facilities personnel to monitor, maintain, and protect their facility's assets efficiently and uniformly.

If an organizational Medical Technology/IoT Management Committee has been assembled with membership from all these separate areas as outlined above, a common goal can be to integrate systems that will better coordinate asset tracking and the centralization of specific security information and risks. Data and workflow integration with other systems (e.g., risk management, incident response, vulnerability management) may be desired to optimize workflows and maximize reliability. Having this coordination can allow for HDO security teams to have better visibility into active medical devices and better assess threats and vulnerabilities from MDM or other technology provider notifications.

Tools may exist to enable this unified asset management, but organizations should carefully evaluate them for the desired features and ensure that contracts and other documentation clearly define necessary capabilities. For example:

- Tools must have the desired capabilities, such as:
    - Secure APIs and other data transfer mechanisms
    - Data cleansing, normalization, standardization, or other capabilities that allow databases to operate effectively on data
- General functionality provided should include:
    - Support: network-based security event detection; risk assessment and management; supply chain and inventory management (e.g., pre-procurement, procurement, asset identification).
    - Provide security information from external sources (e.g., recalls, advisories, vulnerability disclosures, MDS^2).
    - Integration with existing traditional systems (e.g., asset management (CMMS/CMDB), risk management, vulnerability scanners, IT security tools, network management).
    - Support security best practices (e.g., change management, traffic analysis, usage & network statistics, remediation best practices and prioritization).
- The associated contract must require that the capability exists and be made available to the HDO

- If appropriate tools or capabilities do not exist, HDOs should consider Request for Proposals (RFPs) or other similar vehicles that may enable the build-out and future acquisition of such capabilities.

E. Software Bill of Materials (SBOM)

Today, many modern technologies used in healthcare environments are built out of software and other technologies that enable their increasingly advanced functionality. These pieces of software and other technological components in turn contain other, smaller software "libraries" or programs. For example, MDMs or other technology providers frequently outsource development of OS subsystems or the entire OS; use a modified off-the-shelf or open-source OS, firmware, or application software; and source hardware parts or subassemblies with embedded code from suppliers, among other similar scenarios. Completed technologies ready for delivery and deployment are commonly composed of a combination of software with diverse origins, designers, and architecture.

Moreover, as discussed throughout this document, as technologies age, once-advanced security protocols become obsolete and support is gradually discontinued, and susceptibility to cyber threats increases drastically. Vulnerabilities may be isolated to individual segments of software within a technology, but a lack of supply chain visibility severely hinders locating exploitable components. This condition is exacerbated by the complexity of the healthcare ecosystem of interdependent HDOs, MDMs, other technology providers, and other organizations, of all sizes. As a result, tracking, understanding, and managing the cybersecurity risks introduced by the software components contained within technologies used in healthcare environments is a particularly challenging issue, and becomes more so within the context of legacy technologies. Clear delineation of component relationships and interconnections, and thorough documentation of supply chain lineage and attributes, is vital to mitigating the cybersecurity risk of legacy technologies. Achieving this critical supply chain transparency is the goal of software bills of materials, or SBOMs.

An SBOM is "a formal record containing the details and supply chain relationships of various components used in building software" [21]. It lists the software - and, potentially, other

21 https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf

technological details - that a product or technology uses or otherwise depends upon. This helps HDOs, MDMs, other technology providers, and others involved in the securing of technologies to track and manage their assets and inventory, and - most critically from a cybersecurity perspective - to track and manage vulnerabilities inherited from a technology's software supply chain.

While SBOM is still a relatively new concept in the healthcare sector, its use is growing. Moreover, executive and regulatory actions have encouraged or, in some cases, mandated SBOM use. [22]

The dominant challenge impeding SBOM adoption is the absence of a global standard for software component identification. Like any bill of materials, an SBOM is an evolving record that steadily consolidates its prior iterations as it moves upstream in the supply chain. As each organization performs a manufacturing step, the SBOMs of its suppliers are merged to reflect the production progress and software additions made to outgoing components. Efficiency and practicality constraints require the standard to be machine-readable so that downstream supplier data can be ingested and formatted into an updated SBOM.

A secondary challenge is that existing component identification standards are used inconsistently across suppliers and employ variable component attributes to the detriment of effective multi-organization transferability and data reliability.

This section provides recommendations and/or discusses current challenges related to SBOMs.

Subtopic #1: Incomplete or Missing Software Transparency Information

Legacy technologies often lack software transparency, including the third-party software that they contain. While current and future guidance documents are moving the industry towards solutions such as SBOMs, such efforts may not encompass legacy technologies already deployed in the healthcare environment, which lack associated SBOMs or other software transparency information. Without robust software transparency information through SBOMs or other methods, HDOs are forced to use less targeted, and sometimes less effective, mitigation strategies.

Recommendations for HDOs:

22 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; https://www.fda.gov/media/119933/download (SBOM referred to as "cybersecurity bills of material," or CBOM)

- HDOs should request from MDMs and other technology providers available SBOM information for current legacy technologies and technology versions in standardized and machine-readable formats. If legacy SBOM information is not available, HDOs should leverage the other recommendations in this subtopic.
- HDOs should collaborate with MDMs and other technology providers to maintain as current as possible versions of technology SBOMs.
- HDOs should leverage collaboration with industry, partners, and other parties who may have access to missing SBOM information.
- HDOs should leverage commercial tools (e.g., passive network monitoring solutions) that may be potentially accumulating missing SBOMs information.
- HDOs should cultivate processes (e.g., internally, through tools, and/or through contract services) that allow for regular importation and analysis of SBOMs to identify newly released vulnerabilities from private (e.g., manufacturer or industry organizations) or public (e.g., NVD or ICS-CERT) sources. These processes should allow for:
    - Identifying whether technologies in their inventory contains software components affected by identified vulnerabilities.
    - Identifying the actual physical technologies and technology versions affected via e.g., asset tracking number or location information.
    - Documenting and logging any decisions made and compensating measures applied.

Note Regarding SBOMs for Legacy Technologies

The recommendations detailed above relate to SBOMs generally, including SBOMs for current and future legacy technologies. However, there are recognized challenges with creating and maintaining SBOMs for legacy technologies that deserve special mention.

In particular, it can be difficult for an organization - including an MDM or other technology provider - to take an existing product that has not previously had an SBOM associated with it, and "reverse engineer" an SBOM for it. This may be because the technology predates the timeframe when the MDM or other technology provider tracked components for the purpose of vulnerability management. Tools and third-party services do exist, but they are not always capable of generating complete SBOMs. Another challenge is that many components do not provide their own SBOMs, so the subcomponents are opaque to the MDM or other technology

provider without additional work to identify these components, and then analyze them. These processes can be resource intensive and expensive to undertake.

Recommendations for MDMs

Because SBOMs are an important risk management tool, MDMs and other technology providers should develop and maintain SBOMs that are as complete as possible for their legacy technologies. With respect to current legacy technologies, SBOM expectations will change based on whether a device has or has not reached EOL/EOGS/EOS.

For current legacy technologies that have not reached EOS, MDMs and other technology providers should develop, maintain, and provide SBOMs to HDOs over the remaining supported life of the technology. Once a technology reaches EOS, MDMs and other technology providers should communicate this change of status to customers and provide a "last/final" SBOM with that communication, where it is clear that further SBOM updates will not be provided.

For current legacy technologies that have reached EOL/EOGS/EOS, MDMs and other technology providers should develop, maintain, and provide to HDOs current versions of legacy technology SBOMs to the best of their abilities. Recognizing resource limitations for both HDOs, MDMs, and other technology providers, organizations should communicate to prioritize SBOM creation.

Known Challenges/Future Work

As SBOMs are, at the time of this writing, still a maturing discipline, there are several recognized challenges:

- No standardized component and version naming conventions. Currently, there does not exist a recognized standard for naming and versioning components within SBOMs, nor for versioning SBOMs as they are updated. Consequently, different organizations may refer to the same components by different names, or use different versioning schemas, introducing confusion and limiting the use of available tools. In particular, it can make vulnerability matching (see below) more difficult.
- Multiple formats. There exist multiple accepted standards for SBOMs. While the flexibility allows organizations to choose the standard appropriate for their needs as SBOM formats continue to mature, it also introduces the potential for organizations to have to manage multiple different SBOM formats. Some tools have been introduced to

translate and/or normalize SBOM data between different formats, but best practices and robust tooling for managing multiple SBOM formats remain in development.

- Depth: To realize the full benefits of SBOMs, it is important that they be "complete," such that they provide full information on all transitive dependencies that a technology may contain. Additional development is needed to facilitate the creation and maintenance of "complete" SBOMs. While current practices and tools can generally create, ingest, and otherwise operate on SBOMs whose first level components are known, such incomplete SBOMs are insufficient for maintaining full situational awareness of an organization's software supply chain.
- Complexity and Size Requires Automation: SBOMs may range from several dozen to several thousand (if not more) lines, depending on the type of software and how many transitive dependencies exist. Organizations will need to be tracking, storing, and maintaining SBOMs for most, if not all, technologies in their environments, and doing so will quickly overwhelm manual processes and procedures.
- Exchanging, validating, and updating SBOMs: Organizations must be capable of routinely creating, ingesting, and maintaining SBOMs. However, mechanisms and best practices for exchanging, validating, and updating SBOMs are still being identified and matured.
- Rapidly changing information. Software typically iterates quickly, potentially leading to changes within SBOMs from one version to the next. Best practices for tracking, exchanging, receiving, and storing timely SBOM information are still being developed.
- Tooling: Tooling is critically necessary for managing SBOMs due to their size, their dynamic nature, and the amount of SBOMs each organization will likely need to manage. While SBOM tooling does exist, their capabilities are still maturing, and continue to iterate as the SBOM ecosystem itself matures.

In addition, a primary use case of SBOMs—for procurement, implementation, and vulnerability management purposes—is the evaluation of the components identified in an SBOM against known vulnerability information. By identifying whether components contain known vulnerabilities, and then assessing the risks presented by those vulnerabilities, organizations may make informed decisions about acquiring and implementing certain technologies (procurement and implementation) or responding to potential or actual risks (vulnerability management).

However, there remain several challenges with using SBOMs in this way:

- Incomplete vulnerability information. Accepted sources of vulnerability information, such as the NVD and private vulnerability databases, are known to be incomplete. For example, some vulnerabilities may not be reported to these sources, even if the vulnerabilities are mitigated with patches or otherwise fixed. In other cases, vendors may choose not to assign or report vulnerabilities for components or products that they may no longer be supporting. This missing vulnerability information may give a false sense of security that components are not vulnerable, when in fact they may be.
- Lack of context regarding exploitability. Software components may have few known vulnerabilities, or they may have hundreds to thousands. However, not all vulnerabilities are exploitable in all systems at all times. Comparing SBOMs to known vulnerability information, in the absence of additional context regarding whether the vulnerabilities are exploitable, may create inaccurate or incomplete impressions of how "vulnerable" or "insecure" a component (and the technology in which it sits) is. Moreover, it may distract or overwhelm organizations trying to manage risks to their technologies, as they may spend scarce resources addressing less risky or even non-exploitable vulnerabilities, or struggle to prioritize which vulnerabilities should be addressed first.
- Increased visibility of unmitigated vulnerabilities. SBOMs will create increased visibility of the vulnerabilities associated with the technologies used within healthcare environments. For various reasons, vulnerabilities revealed by SBOMs may be unmitigated. In particular, where vulnerabilities are associated with technologies that are past their EOGS/EOS dates, these vulnerabilities may remain perpetually unpatched. The additional visibility provided by SBOMs regarding unmitigated vulnerabilities will create additional risk management challenges, including the need for compensating controls or other risk management techniques.

To mitigate some of these challenges while SBOM practices continue to mature:

- MDMs and other technology providers should continue to monitor their current legacy technologies for cybersecurity signals and detect evidence of newly discovered or newly exploited vulnerabilities, and report discovered vulnerabilities. For legacy technologies for which support has ended, MDMs and other technology providers should act in compliance with applicable regulatory responsibilities.
- MDMs and other technology providers may need to communicate additional supplemental information to their customers, including vulnerability scoring

adjustments, information about exploitability based on the technology implementation, and/or known exploits.

- HDOs should monitor multiple vulnerability sources to assure best possible awareness of potential risks.
- HDOs should recognize that some vulnerability scoring systems were not intended to convey risk information beyond characterizing a vulnerability on the abstract level of the software component itself (e.g., CVSS), and HDOs may have to consult additional information sources or may have to engage in additional analysis to understand the risk to their environment.[23]
- HDOs, MDMs, and other technology providers can evaluate and use available tooling to help address these challenges.
- HDOs, MDMs, and other technology providers should join and actively participate in information sharing organizations to enable communication on critical issues, including vulnerability discovery, between industry peers.

Significant ongoing efforts are underway to address many of these challenges. Organizations wishing to learn more, or to get involved in these efforts, should examine the following resources and groups:

- NTIA SBOM Materials
- CISA SBOM effort
- IMDRF SBOM guidance/Working Group

F. Patching

Although software patching is a key practice in protecting technologies, patch management at HDOs is challenged by a diversity of equipment, lag time to patch availability, the accessibility and utility of patch information, ownership of patch installation, and the fact that patching

23 For example, the maintainers of one of the most recognized vulnerability scoring systems, CVSS, states that CVSS is "designed to measure the severity of a vulnerability and should not be used alone to assess risk." (emphasis added) As described in the authoritative guide to CVSS, "the CVSS Base Score represents only the intrinsic characteristics of a vulnerability [and] should be supplemented with a contextual analysis of the environment, and with attributes that may change over time[.] … [A] comprehensive risk assessment system should be employed that considers […] factors outside the scope of CVSS." https://www.first.org/cvss/user-guide

needs to be coordinated with care delivery to minimize patient impacts, creating complicated logistics.

Subtopic #1: Diversity of equipment

There are generally thousands of different makes and models of equipment within hospitals and systems. In both large and small organizations, the reality is that patching every technology remains a significant challenge. Aside from the sheer amount of resources required to monitor, retrieve, and deploy patches, tracking must be done at the asset-level to assure all patches are implemented routinely. Moreover, some equipment may not be capable of being patched due to design or to support status.

Recommendations for MDMs:

- Provide risk assessments for each vulnerability that applies to a technology as part of product security advisories or other vulnerability communications shared with HDOs.
- Collaborate with HDOs to identify the best mechanisms to provide awareness of update availability.

Recommendations for HDOs:

- Establish a full hardware and software inventory of technologies used in the HDO environment.
- Ensure documentation includes patch/support location information and support details, including specific patch installation requirements.
- Establish a comprehensive patching process that, to the greatest extent possible, makes patching routine and predictable. Section VII.C.3 provides additional detail and recommendations for doing so.
- Assess the priority of a given patch relative to the established patching schedule. This should inform whether the patch should be applied out of band, may be done during routine scheduled patching, or may be protected using compensating or other controls (for a limited time). Where appropriate and possible, it may be useful to consult with the MDM or other technology provider to inform the risk assessment and response actions.
    - The risk assessments, any direct actions taken (i.e., patching, compensating controls), and identified residual risks needs to be documented and kept current in relevant tools as it aids the HDO in ensuring they have the appropriate situational awareness. See Section VII.B for more details.

    - This should include any plans[24] to patch technologies at a later time, where compensating controls have been put in place to manage the risk temporarily or the risk (without compensating controls) has been determined to be acceptable for a limited time.
- If available from the MDM or other technology provider, any information regarding risks and vulnerabilities (including, e.g., Vulnerability Exploitability eXchange (VEX) information) can help assess the severity and exploitability of a vulnerability and be used to inform the priority of a patch.
- Assess the risk for technologies where the manufacturer is no longer actively providing patches (e.g., because the device is past EOGS/EOS), where patches aren't generally available or regularly implemented, and use alternate strategies for risk mitigation. See Section VII.C.4 for more detail and recommendations.

Subtopic #2: Lag time to patch availability

In healthcare environments, many devices and their associated vulnerabilities must be managed through the different stages of mitigation. A challenge HDOs face is when a vulnerability is known to be applicable to a device, but a patch is not yet available for installation on a device. MDMs need varying amounts of times to develop, test, and release patches, and they may further require verification and validation testing and documentation to qualify patches prior to release. This tends to result in delays in patch availability compared to enterprise infrastructure endpoints.

It is important to keep in mind that FDA has officially stated that MDMs may always update a medical device for cybersecurity, and that FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity.[25] For additional discussion summarizing FDA guidance on patching, see Page 45.

Recommendations for MDMs:

- Identify if a patch is needed
- Inform about patch timeframe and offer compensating controls in the meantime

[24] NIST SP 800-171 – POAM.

[25] https://www.fda.gov/files/medical%20devices/published/cybersecurity-fact-sheet.pdf

- Provide patches within a reasonable timeframe. To support this capability, ensure sufficient staff and other resources are available to develop, test, make available, and otherwise support patch availability.
- Design the patching process to simplify patch installation. See Section VII.C.3 for more details.
- Provide regular status updates on outstanding patches, e.g., through quarterly or other periodic updates

Recommendations for HDOs:

- Track the need for patches, including monitoring applicable patch feeds from MDMs and other third-parties
- Keep an up-to-date inventory of software on devices to facilitate matching patches
- Implement architectural protections to limit exploitability of end points, such as through micro-segmentation
- Solicit updates from MDM partners about the current status of outstanding patches
- When new, potentially urgent vulnerabilities (such as 0-days) are announced, prepare for patching; for example:
    - Identify devices that will need such patches
    - Deploy interim mitigations until final patch is available
    - Begin planning process for any applicable device downtime
    - Monitor vendor and community communication for changing guidance on response
    - Communicate with HDO staff about patch need
    - For known, exploited vulnerabilities, monitor for indicators of compromise
    - HDOs to provide annual training to their general staff, about 0-day vulnerabilities in addition to their annual training about phishing, etc.
- Consider developing a playbook that can be executed in such cases. HSCC is considering work to develop such a "0-Day Playbook."

Subtopic #3: Accessibility and usefulness of patch information

Although HDOs generally have an inventory of their equipment, specific cybersecurity information that permits more granular tracking and risk management (such as MAC address, IP address, or SBOM) are not always readily available. Moreover, it can be difficult to know what patches are available for devices within the installed base, based on the number of vendors, devices, and available customer information. HDOs must continually track and follow

up on patch status and mitigation strategies. Depending on the method of communication from the MDM, this may be as straightforward as waiting for formal written communication, or it can be as complex as continually checking the MDM's website waiting for that patch to be available.

Recommendations for MDMs and HDOs:

- Where possible, HDOs should request from MDMs their SBOMs, relevant hardware, and other identifying information (e.g., MAC address, serial numbers, any relevant unique identifiers, etc.) in standardized and machine-readable formats to facilitate patch tracking and deployment
- HDOs may consider leveraging commercial tools (e.g., passive network monitoring solutions) that can accumulate missing SBOM, hardware, and other identifying information
- HDOs should ensure that contracts and other agreements require and/or request that MDMs provide relevant information necessary to support patching processes. See Section VII.C.3 for more detail
- MDMs should ensure that their design and documentation process capture information relevant to patching processes, and this information should be provided to HDOs in a timely manner
- HDOs should collaborate with trusted industry partners, ISACs/ISAOs, and other parties who may provide missing SBOM, hardware, or other relevant identifying information
- HDOs should cultivate processes (e.g., internally, through tools, and/or through contract services) that allow for regular identification of software, hardware, and other information that should be monitored and documented to enable patch management.

For additional recommendations that may be useful, please see the SBOM and Inventory Management topics within the Challenges and Recommendations section.

Subtopic #4: Ownership of Patch Installation

Depending on the type of device and how it is managed, different parties may be responsible for installing patches. For example, certain patches and devices may require installation by the MDM due to validation and verification processes or other dependencies. Additionally, MDMs may not implement functionality, architecture, and processes that support direct customer patching.

HDOs, potentially through contracted ISOs, may be responsible for patching devices in other circumstances. However, HDOs should be aware that applying patches could have secondary consequences, such as when the patch is not yet verified and validated by the MDM, or when applying the patch could potentially raise remanufacturing considerations. [26]

In addition, especially with respect to current legacy devices, a device that has passed its EOS date may no longer be actively supported by the MDM, and the MDM is not releasing patches for it. However, in certain circumstances, vulnerabilities may be discovered that affect these legacy devices, and patching by the HDO may be necessary to protect them and the environment in which they operate.

For example, in certain cases where third-party software is implicated (such as operating systems), the third-party may be releasing patches that the MDM is not verifying and validating, due to the EOL/EOS status, or other reason. HDOs should carefully assess the risks of patching the third-party software, the potential consequences of doing so, including potential remanufacturing or other regulatory concerns, and any other relevant considerations, and act accordingly.

Recommendations for MDMs:

- Where possible and appropriate, MDMs should consider designing their devices and patching processes to support secure remote patching of fielded devices.
- Where possible and appropriate, MDMs should implement and support the capability for HDOs to apply patches that have been validated by the MDM.
    - For example, there may be circumstances where a device can indicate that there is a patch available, and the HDO may then decide whether to remotely retrieve and apply the patch according to their own processes and operational needs. Designing devices to support such capabilities may enable faster and more effective patching.
- MDM security documentation, labeling, and any other relevant materials should clearly indicate patch ownership responsibilities, capabilities, and—where appropriate - instructions.
- MDMs should provide detailed information related to patches, including what vulnerability or other issue it is meant to address.

[26] Please see the draft Remanufacturing Guidance for additional information.

Recommendations for HDOs:

- Determine and document patch ownership roles and responsibilities, as well as process, during device acquisition negotiations
- Document patching procedures in appropriate places and train appropriate staff in them
- Retain patching, remediation, and other change control documentation that is supplied, in case relevant at a later time
- Clearly document whether patches have been implemented for each device within the HDO environment
- Determine who can apply the patch (HDO, MDM, or 3rd party), and the process to patch. Some devices can accept remote patches allowing for a single deployment while others require a physical touch of every device

Subtopic #5: Coordinating Patching with Care Delivery

Patching typically requires that devices and other technologies be temporarily removed from service while the patch is downloaded, applied, tested, and verified. This downtime can last anywhere from several minutes to several hours, if not longer, and is contingent on the patch installing properly without issues, and further without affecting functionality in undesired or unanticipated ways. Where the patch does not install correctly, or where functionality is unexpectedly impacted, this downtime can last even longer.

In all cases, it is critically important that patching processes take into consideration potential patient care impacts either from the device being temporarily removed from service, or from patching occurring while the device is in use, if policies and procedures do not properly control for such activity being disallowed.

Consequently, coordinating patching with care delivery can be complex, and robust policies and procedures need to be established to manage it.

- See Section VII.C.3, specifically related to patch application

G. Third Party Component Risk Management

Subtopic #1: Designing Technologies with Secure and Securable Components

A fundamental challenge with many technologies used in healthcare environments is that the lifecycles between the software and hardware included in devices often don't align, introducing a functional and economic bifurcation in their management. This can occur because:

- The lifecycle events leading to a need for hardware replacements occur less frequently than the need for software updates, e.g., to address software vulnerabilities
- Software often can be updated more easily than hardware
- Software update requirements may surpass available hardware capabilities
- The cost and feasibility of updating can be limiting
- There may be limitations on the ability to affect clinical factors like workflow or training, since updating may require workflow changes.

In such situations, even if the technology is within the originally communicated support period, it could be considered as a legacy device from a cybersecurity perspective.

Expectations between technology usability and cybersecurity change as a result of this discrepancy. Technologies that still perform their intended function, even in the absence of software component support, may be difficult to retire or replace for fiscal or operational reasons.

Recommendations for MDMs:

- Provide clear information about the risks of a technology with unsupported components, and the potential upgrade pathways, so that the HDO can make an informed risk decision
- Where possible and appropriate, consider moving toward designs that better harmonize the lifecycles of software and hardware to mitigate some of this bifurcation
- Design technologies so that software, hardware, and other components can be updated or replaced during the technology's lifecycle. For example, MDMs may consider:
    - Forecasting for software, hardware, and other component end-of-life during device lifecycles and designing and executing plans to address end-of-life concerns. MDMs should communicate these plans to their customers as appropriate. Such forecasts should consider:
        - Shipping technologies with supported operating systems and other software components. This may require identifying end of life dates and ensuring development cycles account for necessary updates, as well as updating inventory before it is sent to customers.

        - Shifting development pipelines to use updated operating systems and other software as they become available, such that the software being included within finished technologies remain supported, or supported for longer.
        - Identifying and addressing potential cloud computing maintenance and end-of-life issues, such as the security and support status of microservices from the cloud service provider, and/or applicable Software as a Service (SaaS) and/or Platform as a Service (PaaS) functions. See Section VII.C.1.b)(1)(a) for specific recommendations on how to do this.
        - Identifying and addressing potential implantable device issues, recognizing that these devices are physically implanted within a patient's body, and therefore that special consideration needs to be given to how security, update, and other functional capabilities are designed and maintained over the lifecycle of the technology. Designs should be developed to minimize to the greatest degree possible any surgical intervention necessary to actually access the physical device to fix potential issues.
    - Designing technologies for modularity, such that software, hardware, and other components may be independently updated without forcing the obsolescence of other components or the technology itself.
- Where possible and applicable, consider how technologies can be designed to accommodate security features according to user specifications. Overall, technologies should be designed to be secure when released and securable over time.

Recommendations for HDOs:

- See Section VII.C.4 for discussion and recommendations.

Subtopic #2: Selecting Secure and Securable Third-Party Software Components

Because many medical technologies rely on software in order to safely and effectively perform their clinical functions, it is critical that MDMs carefully consider the software that they integrate into their designs.

This document has discussed in detail many types of legacy "pressures" that arise over the lifecycle of a given device, including end-of-life/end-of-support declarations, unknown software

supply chain and dependency issues, and a lack of updatability, among others. To anticipate and minimize these future legacy pressures, MDMs should prefer software suppliers that:

- Provide ongoing software support (e.g., security updates) and indicate support milestones, including end of life dates.
- Provide software supply chain information, including dependencies.
- Provide necessary documentation to support MDM risk management and regulatory compliance.
- Engage in collaborative exchanges regarding the MDM's design and secure architecture requirements, specifically so the software supplier understands the desired end use of the product in the healthcare ecosystem and may be able to advise and/or make targeted changes to their product to address any relevant considerations (such as extended anticipated lifetimes, certain security controls, etc.).

Legacy pressures also arise from more general risk management challenges. Devices that were not designed using secure development practices may be more prone to vulnerabilities or other security issues that may render them "legacy" unexpectedly, and organizations that lack robust cybersecurity risk management programs may not be able to address incidents or vulnerabilities that may impact their products, and that in turn impact MDMs, HDOs, and other healthcare stakeholders. Conversely, organizations with mature, sophisticated cyber risk management programs are more likely to be able to successfully address cybersecurity threats that could - in the absence of such capabilities - translate into drivers of legacy challenges.

Consequently, to further anticipate and minimize future legacy pressures to the greatest extent possible, MDMs should prefer software suppliers that proactively engage in cybersecurity risk management activities. See Section VII.D.2.a) for specific recommendations.

Subtopic #3: Identifying, Tracking, and Managing Third-Party Components

Today, many modern medical products are built out of software and other technologies that enable their increasingly advanced functionality. These pieces of software and other technological components in turn contain other, smaller software "libraries" or programs. For example, MDMs frequently outsource development of OS subsystems or the entire OS; use a modified off-the-shelf or open-source OS, firmware, or application software; and source hardware parts or subassemblies with embedded code from suppliers, among other similar scenarios. Completed devices ready for delivery and deployment are commonly composed of a combination of software with diverse origins, designers, and architecture.

Moreover, as discussed throughout this document, as technologies age, once-advanced security protocols become obsolete and support is gradually discontinued, and susceptibility to cyber threats increases drastically. Vulnerabilities may be isolated to individual segments of software within a technology, but a lack of supply chain visibility severely hinders locating exploitable components. This condition is exacerbated by the complexity of the healthcare ecosystem of interdependent HDOs, MDMs, and other organizations, of all sizes. As a result, tracking, understanding, and managing the cybersecurity risks introduced by the software components contained within medical products is a particularly challenging issue, and becomes more so within the context of legacy technologies. Clear delineation of component relationships and interconnections, and thorough documentation of supply chain lineage and attributes is vital to mitigating the cybersecurity risk of legacy devices. Achieving this critical supply chain transparency is the goal of software bill of materials, or SBOMs.

An SBOM is "a formal record containing the details and supply chain relationships of various components used in building software" [27]. It lists the software—and, potentially, other technological details—that a product or technology uses or otherwise depends upon. This helps MDMs, HDOs, and others involved in the securing of medical technologies to track and manage their assets and inventory, and—most critically, from a cybersecurity perspective—to track and manage vulnerabilities inherited from a technology's software supply chain.

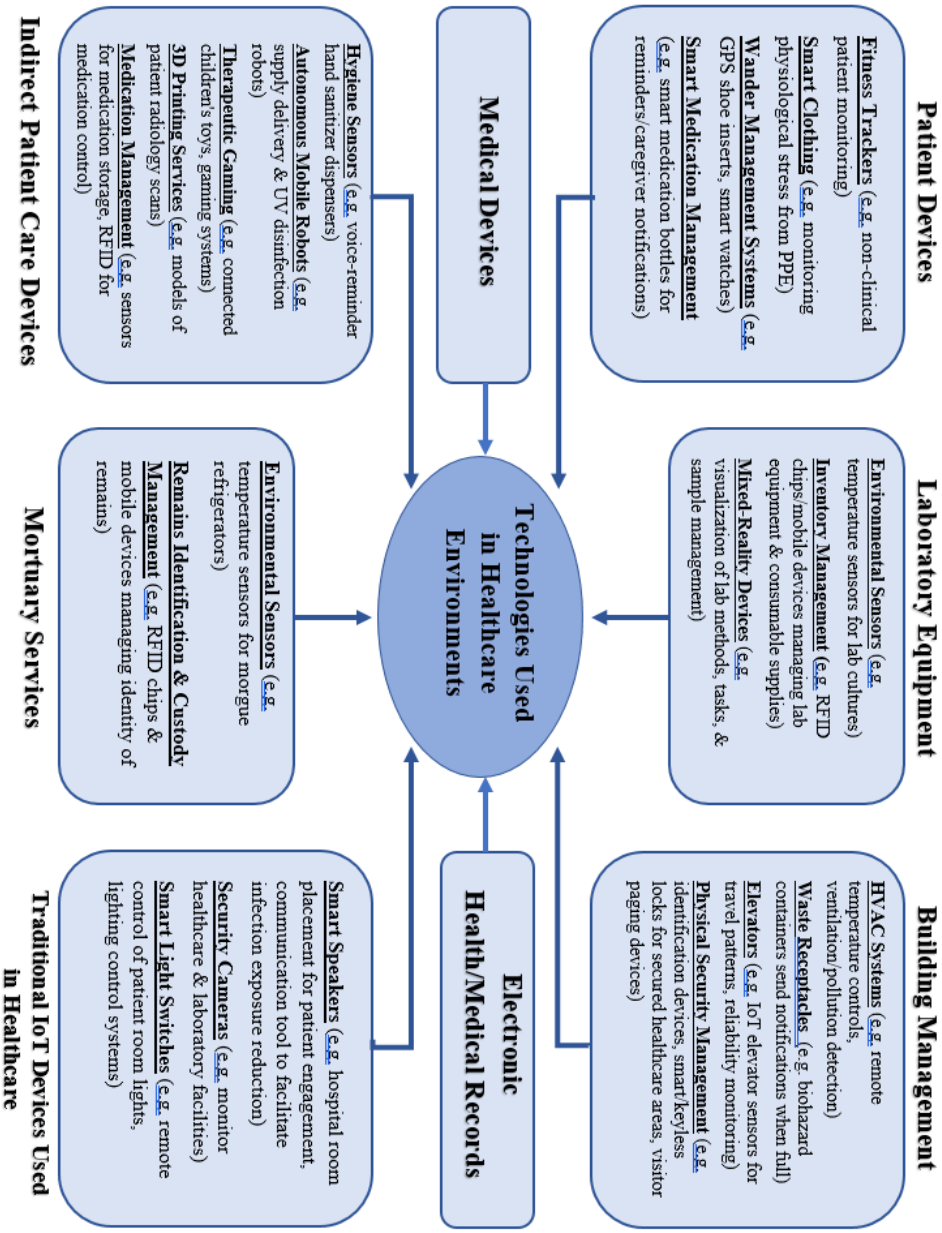
Recommendations for MDMs and HDOs:

- See Section VIII.E on SBOM

IX. Appendix 1 – Example Technologies Used in Healthcare Environments

This graphic contains a non-exhaustive list of the types of technologies that may be used in healthcare environments, and which likely should be included within a cyber risk management program.

27 https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf



X. Acknowledgements

The Health Sector Coordinating Council expresses its gratitude to the many member representatives who worked on the Legacy Task Group and contributed significant hours and thought leadership to the development of this resource.

In particular, we wish to thank:

Jessica Wilkerson (Co-Lead)

U.S. Food and Drug Administration (FDA)

Mike Powers (Co-Lead)

Intermountain Healthcare

Ramakrishnan Pillai (Co-Lead)

LivaNova (Formerly with Elekta)

Adam Brand

KPMG

Alex Kent

Capital One (Formerly with Medtronic)

Angelo Calvache

Accuray

Anura Fernando

UL

Ashley Mancuso

Johnson & Johnson

Audra Hatch

Thermo Fischer Scientific

Axel Wirth

MedCrypt

Bill Proffer

Leidos

Brindusa Curcaneanu

Nevro

Chad Williams

Bayer

Chris Bennett

Medical University of South Carolina

Chris Plummer

Dartmouth-Hitchcock Health

Colin Morgan (Sub-Lead)

Apracity

Darrell Hall

U.S. Department of Health & Human Services, Health Sector Cybersecurity Coordination Center (HC3)

Dave Rideout

Johnson & Johnson

Debra Bruemmer (Sub-Lead)

Mayo Clinic

Eddie Pena

Sentara Health

Eddie Myers

Crothall Healthcare Technology Solutions

Emily Mengel

WakeMed

Ezra Eisenberg

Sysmex

George Reed

WakeMed

Henry Sprafkin

Clearwater Compliance

Ian Glassman

Alcon

Inhel Rekik

Bracco Medical Technologies

Jason Kitchell

Uni-Med

Jeff Moore

Draeger Medical

Jessica Peterson

American Academy of Ophthalmology

Jim Jacobson

Siemens Healthineers

Jim McLean

Siemens Healthineers

Jim Adgate

University of Chicago Medicine

Jithesh Veetil

Medical Device Innovation Consortium (MDIC)

Joseph Burgoyne (Sub-Lead)

GE Healthcare

Jon Crosson

Health-ISAC

Jon Hunt

Medical Device Innovation Consortium (MDIC)

Jonathan Bagnall

Royal Philips

Justin Cooper

Sentara Healthcare

Katrina Jacobs

Kaiser Permanente

Kenneth Wilder

ClearDATA Networks, Inc.

Laura Robb Elan

Baxter Healthcare

Les Gray

Abbott

Linda Hillen

Abbott

Margie Zuk (Sub-Lead)

MITRE

Mark Shina

Absolute Imaging Solutions

Mark Sexton

Clearwater Compliance

Michael McNeil

McKesson

Michael Holt

Virta Labs

Michelle Jump (Sub-Lead)

MedSec

Nicholas Heesters

U.S. Department of Health & Human Services, OCR, HIPAA

Ojonimi Ocholi

Medtronic

Oleg Yusim

Edwards Lifesciences

Penny Chase

MITRE

Priyanka Upendra

Banner Health

Richard Flannery

International Association of Medical Equipment Remarketers and Services (IAMERS)

Rob Suarez

Becton, Dickinson, and Company (BD)

Robert Rajewski

CriTech Research, Inc.

Robert Kerwin

International Association of Medical Equipment Remarketers and Services (IAMERS)

Roberta Hansen

Abbott

Samantha Jacques (Sub-Lead)

McLaren Health

Sara Bohan

Mayo Clinic

Scott Nichols

Danaher

Scott Hanson

MedSec

Sheila O'Donnell

Crothall Healthcare Technology Solutions

Starke Moore

Ascensia Diabetes Care

Steve Abrahamson (Sub-Lead)

EY (Formerly with GE Healthcare)

Steven Hughes

Veterans Health Administration

Suraj Amasebail

GE Healthcare

Terrence Head

Becton, Dickinson, and Company (BD)

Terry Hutton

Sentara Healthcare

Thom Flloyd

Royal Philips

Ty Greenhalgh

Claroty

Tyrone Heggins

Becton, Dickinson, and Company (BD)

Uma Chandrashekhar

Alcon

Varun Verma

Royal Philips

Yoshiaki Cook

Canon Medical Systems USA

Zach Rothstein

Advanced Medical Technology Association (AMTA)

Zack Hornberger

Medical Imaging Technology Association (MITA)