NEXT STEPS TOWARD MANAGING LEGACY MEDICAL DEVICE CYBERSECURITY RISKS

November 2023

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

This white paper was prepared by The MITRE Corporation under contract with the U.S. Food and Drug Administration. The views, opinions, and findings contained in this playbook do not constitute agency guidance, policy, or recommendations or legally enforceable requirements. Utilizing the information presented in this document does not constitute compliance with any requirements of the Federal Food, Drug, and Cosmetic Act, or any other applicable law.

Acknowledgments

MITRE would like to thank the healthcare delivery organizations (HDOs), medical device manufacturers (MDMs), hospital trade associations, healthcare group purchasing organizations, deemed accrediting organizations, and government agencies that provided insights into the challenges of managing legacy medical devices through interviews and working group participation. The recommendations in this document are a direct result of lessons learned from these engagements.

Specific organizations participating in the working group included Abbott, BD, the Centers for Medicare & Medicaid Services (CMS), Christiana Care Health System, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Food and Drug Administration (FDA), Northwell Health, McKesson, McLaren Health, Medtronic, Siemens Healthineers, Smith and Nephew, The Joint Commission, University of California San Diego Health, and the Veterans Administration.

Table of Contents

List of Figures

1 Introduction

Legacy medical devices are those “that cannot be reasonably protected against current cybersecurity threats” [1]. These devices, which can include products that retain material useful life beyond declared “end of support” or “end of life,” may not have been designed to cope with current cyber risks. Because of the long lifetimes of medical devices and the lack of harmonization between medical device manufacturer (MDM) and healthcare delivery organization (HDO) practices for supporting and replacing devices, what may have been effective cybersecurity controls present at point of purchase may no longer adequately defend against current cyber threats. Additionally, in some cases medical devices being purchased today can already meet the definition of a legacy device as described in this paper. At the same time, legacy medical devices may still be broadly in use and providing needed healthcare, and simple removal of them may present risks to patient safety and clinical operations, as well as fiscal challenges. Since legacy risks likely cannot be mitigated sufficiently through patching and updating due to outdated technology and compatibility issues, other approaches to managing these risks may be required.

Over the past several years, the healthcare sector has worked on addressing the challenges posed by legacy medical devices. These challenges are described in the Background section below. The U.S. Food and Drug Administration (FDA) contracted with MITRE to develop a white paper that builds on this work, focusing on near-term solutions, providing advice on operationalizing key recommendations from the previous work, and including considerations for implementation by less-resourced HDOs, such as rural providers and safety-net hospitals.

MITRE initially interviewed a representative group of stakeholders, including those from HDOs, MDMs, and healthcare cybersecurity experts, to develop an initial landscape analysis to define the scope and parameters for the white paper. MITRE then convened a small working group drawn from HDOs, group purchasing organizations (GPOs), MDMs, distributors, federal agencies, and hospital accrediting organizations to collaboratively develop the white paper.

Based on the stakeholder interviews and the working group discussions, MITRE identified challenges in adopting the processes described in the previous work on managing the risk of legacy medical devices. In the Recommendations section below, studies and pilots are proposed to drive adoption. Additionally, the creation of templates, standardized information, and processes are suggested to assist less-resourced HDOs.

The remainder of the paper presents findings from the interviews and working group discussions. This includes a discussion of previous work on legacy medical devices, challenges in operationalizing those efforts, and several recommendations to address those challenges, including:

- Shared responsibility over the medical device lifecycle
- Vulnerability management
- Workforce development
- Mutual aid

Appendix A summarizes the recommendations in tabular form.

2 Findings

2.1 Background

Connected medical device technology has revolutionized patient care. Devices range from infusion pumps that help ensure the safe delivery of medications to patients to implantable medical devices such as implantable defibrillators, that save patient lives. The ability to utilize data obtained from these devices is supported by a robust but vulnerable information technology system, including multiple electronic health record systems. The challenge of managing the interrelated use of data between different network applications and devices, many of which require data transfer between products from different manufacturers, adds to this complex environment. In addition, the explosion of available technologies used in healthcare environments has supported the shift from inpatient care delivery to the home and outpatient facilities.

These improvements to care come at a cost: the need to keep these devices safe from cyber risks. The critical nature of these risks was emphasized in the 2017 Healthcare Industry Cybersecurity Task Force Report ("the Report"), in which the importance of protecting medical devices was recognized by it being one of the six key imperatives stated in the report. The Task Force noted the tremendous diversity in the healthcare system in the U.S., recognizing that there are large, medium, and small health systems, as well as very small rural or critical access hospitals. That diversity has only grown, and the healthcare ecosystem itself has grown more complex since the Report's publication.

Medical devices are acquired and implemented in the context of these complex organizations and their strategic processes, financial resources, and organizational governance. As medical devices are substantial investments for HDOs, devices are procured on set timeframes to maximize the value and life of a device. Consequently, medical devices are frequently utilized beyond their ability to keep up with evolving cyber threats. For under resourced HDOs, there may be a choice between not offering a medical device or service to patients or using a potentially insecure legacy device that can provide that service to patients. Additionally, beyond consideration of financial resources, the replacement of legacy devices occurs in the context of organizational and people-focused factors. For example, the implementation of new devices or technologies to replace legacy device may require changes to internal business process and procedures and retraining of clinicians/other personnel.

This environment has resulted in a glut of legacy medical devices, which still perform their primary function, but may be vulnerable to cyber risks. In their report, the Task Force highlighted specific risks associated with networked medical devices and interconnected IT networks:

- Failure to provide timely security software updates and patches to medical devices and failure to address legacy devices.
- Malware that alters data on diagnostic and treatment devices.
- Firmware/software updates that alter device function(s).

- Denial of service attacks that make a device unavailable.
- Exfiltration of personal identification information and/or personal health information.

The Task Force had several recommendations for protecting medical devices including:

- Securing legacy medical devices by implementing regular software updates, establishing firewalls, and ensuring compatibility with modern security protocols, among other controls.
- Improving manufacturing and developing transparency among developers and users.
- Improving the turnaround time for security updates and patches.
- Increasing adoption and rigor of the secure development lifecycle in the development of medical devices.
- Requiring strong authentication to improve identity and access to medical devices.
- Employing strategic and architectural approaches to reduce attack surfaces.

The International Medical Device Regulators Forum (IMDRF) published in 2020 the *Principles and Practices for Medical Device Cybersecurity* (IMDRF/Cyber WG/N60 Final:2020) [2]. The guidance proposed foundational cybersecurity principles and best practices for the total product life cycle (TPLC) of medical devices. In 2023, the IMDRF published *Principles and Practices for the Cybersecurity of Legacy Devices* (IMDRF/Cyber WG/N70 Final:2023) [1]. The document:

- Explains legacy medical device cybersecurity within the context of the TPLC Framework with clearly defined responsibilities for MDMs and healthcare providers (HCPs).
- Provides recommendations for MDMs and HCPs in communication, risk management, and transfer of responsibility to the HCP.
- Provides recommendations regarding compensating controls after the End of Support lifecycle phase.
- Provides implementation considerations for MDMs and HCPs in addressing risks to existing legacy devices that were developed prior to the TPLC Framework for medical device cybersecurity and are still in use.

The N70 guidance emphasizes the shared responsibility of all stakeholders, including MDMs, HCPs, users, regulators, and software vendors. It focuses on devices typically found in hospitals and other clinical settings, and excludes implantable devices and home-use devices, although some of the recommendations may be applicable for manufacturers of those types of devices.

In 2023 the Healthcare Sector Coordinating Council (HSCC) published *Health Industry Cybersecurity Managing Legacy Technology Security* (HIC-MaLTS) [3]. This document was the product of three years of work by the HSCC Cyber Working Group, which consists of industry and government member organizations, including MDMs, HCPs, trade groups, government representatives, health information technology companies,

and others. The HIC-MaLTS identifies the respective and shared responsibilities recommended to healthcare stakeholders in the cybersecurity management of legacy medical devices and technologies, and provides current industry best practices, recommendations, and references for optimizing clinical security, resiliency, and patient safety. It reflects the wide variety of medical devices and other products in the healthcare environment, their diverse locations of use, and their unique risks. It also addresses the issue of the technologies used in healthcare environments and device software functions. A key element in the HIC-MaLTS is the responsibility transfer framework, which details the factors HDOs should assess to make informed decisions about continuing to use unsupported legacy technologies.

Both the HIC-MaLTS and the IMDRF/Cyber WG/N70 Final:2023 clearly define terms and emphasize the criticality of the Software Bill of Materials (SBOM). The latter is the main tool that both MDMs and HCPs need to agree on to ensure that cybersecurity is maintained even beyond the declared end of support timeframe.

2.2 Challenges

The Task Force, HSCC, and IMDRF working groups have done valuable work in identifying the challenges posed by legacy medical devices and providing recommendations, frameworks, and processes to address them. Nonetheless, some challenges and gaps remain in implementing those recommendations:

- Data is needed to inform decisions that will be made by individual HDOs and MDMs as they implement the risk management frameworks, as well as to potentially inform future policies and regulations.
- Managing the cyber risk of legacy medical devices is dependent upon clearly defining medical device lifetimes and lifecycle phases, permitting the development of shared responsibility models between HDOs and MDMs, where specific roles and responsibilities may change as devices move through the different lifecycle phases. This collaborative effort requires transparency, clear expectations, and better understanding of the design process, the security posture of the devices, and the clinical and operational environment in which they operate.
- Frameworks, such as the HIC-MaLTS responsibility transfer framework, offer valuable recommendations, however, HDOs, particularly those in less-resourced rural and safety-net facilities may struggle to implement them on their own. Therefore, it is essential to identify resources to assist them and MDMs are encouraged to adopt standardized processes.

3 Recommendations

The following recommendations address the above challenges and gaps. Some recommendations call for collecting and analyzing data, while others call for improving information sharing and transparency. To ensure that these recommendations are effectively carried out with involvement by all relevant stakeholders and that the data collected is reliable, valid, and useful, stakeholders are advised to follow governance and data collection principles discussed in section 3.1.

The remaining sections focus on recommendations to:

- Further shared responsibility of managing legacy medical devices.
- Improve vulnerability management of legacy medical devices through information sharing.
- Develop a skilled workforce.
- Establish mutual aid relationships to help less resourced HDOs.

3.1 Cross-Cutting Principles

3.1.1 Governance

This section summarizes the governance principles in the HSCC's HIC-MaLTS [3]. Please refer to the HIC-MaLTS document for the full content.

> 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.
>
> It is recommended that governance within HDOs oversee the medical technology lifecycle from procurement to decommissioning, with an emphasis on cybersecurity. This includes defining a risk management strategy, establishing a model, defining the organization's risk management tolerance level, and developing a lifecycle management plan. While each organization's strategy, model, risk tolerance, and plan may differ, the determination and implementation of these steps are essential for effective enterprise risk management.
>
> Governance within MDMs is responsible for identifying risks and hazards, including cybersecurity risks and hazards, throughout the

TPLC of the medical devices that they place into the market. “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 all devices and/or technologies.”

Governance within both HDOs and MDMs requires the appropriate staffing and structure to assure roles and responsibilities are clearly identified and delineated. It is a best practice to build cross functional teams to oversee and manage cyber risk, with ultimate oversight at the board level. It is recommended to identify a senior management member as the leader for enterprise risk management and be responsible for reporting the work to the board, as board accountability for cybersecurity is critical. Open and clear communication between parties is also essential to identify, remediate, and/or mitigate risks.

3.1.2 Data Collection

Although the Task Force and working groups have identified the challenges of legacy devices, there is a lack of valid and reliable data to provide HDOs and regulatory agencies an accurate and usable assessment of the status of legacy device usage in the United States. Obtaining this data can enable more informed policy and decision making, and it can also be used to measure improvement and trends as performance standards are instituted.

To be effective, it is a best practice that this data be based on predetermined definitions so that benchmarks across organizations can be established. The data collected would have definable value, rather than simply being collected to show that an inventory was done. Critically, a best practice is to streamline data collection, since most HDOs are already stressed by multiple surveys and reporting requirements.

These latter considerations will involve both quantitative as well as qualitative data to present an accurate picture for each HDO. Finally, it is recommended that the data be used in a non-punitive manner. The data may then be turned into clear, actionable steps, so that even the smallest organizations, especially those most at risk, can easily comprehend and utilize it for enhancement. This type of data gathering will require participation by the MDMs, distributors, resellers, and other stakeholders to be effective.

3.2 Shared Responsibility Over the Medical Device Lifecycle

There is misalignment between the economic useful life of clinical equipment as measured by the buying patterns of HDOs and the supported useful life of the same equipment as defined by MDMs. Ideally, HDOs would replace legacy medical devices when they reach an MDM’s declared end of support, but these devices may still be able to provide useful clinical functionality, even if they can no longer be reasonably secured against cyber threats. Further, when HDOs decide to replace these devices, they may be sold on the secondary market (which includes the MDMs) to smaller HDOs less able to manage the risks.

HIC-MaLTS recognizes this gap and provides the responsibility transfer framework to support decision making and best practices for managing the cybersecurity of legacy devices that HDOs intend to continue using.

Previous work on legacy devices has suggested adopting new business models, such as leasing, or incentives, such as "cash for clunkers,"[1] to encourage replacement of legacy devices, but these new models and incentives have not yet been widely adopted. HDOs prefer purchasing medical devices to leasing because they want greater control over managing the devices; leasing is often more expensive than capital purchase and there are limited incentives for the lessors to upgrade the hardware. Leasing and cost per procedure also typically includes the use of MDM service organizations, which can increase costs. Additionally, there is a significant gap of additional variable HDO cost drivers that are not accounted for at an asset level, including but not limited to IT network and application management, design and construction costs, and technical and clinical training. Incentives may not fully account for ongoing costs and may be insufficient for replacing devices outside an HDO's planned procurement cycle.

The following recommendations suggest collecting data to better understand the misalignment between HDO and MDM notions of the useful life of devices, increasing transparency between HDOs and MDMs to ensure security expectations are shared, and developing generic or standardized security architectures to better share responsibilities for managing risk and moving toward more modular and resilient design.

Recommendation 1: Pilot data collection to support decision making for legacy device risk management

There is a lack of both quantitative and qualitative data to enable HDOs and MDMs to make informed decisions about the risks and costs of replacement versus the continued use of legacy devices. Many decisions are driven by costs, and HDOs and MDMs need to better understand each other's constraints. In addition, aggregated sets of data could better quantify the risks across the healthcare sector and result in improved alignment within the business operations of the MDMs and HDOs. Finally, this aggregated data, if developed and made publicly available, could potentially inform policies, regulations, and the development of incentives for replacing legacy devices, such as:

- Seeking opportunities to drive replacement of legacy devices by exploring reimbursement and payment distributions based on End of Life (EOL) inventory and reporting.[2]
- Defined useful life for all major components for all network connectable equipment.
- Conditions of participation, in-network agreements, and state licensure, which all set minimum standards for health, safety, and program participation.
- Cyber insurance premiums could differ based on EOL reporting and status.

[1] Action item 2.1.4 in the Task Force report referred to the "cash for clunkers" program for cars (Department of Transportation – National Highway Traffic Safety Administration. [2016]. Car Allowance Rebate System [CARS])

[2] Reimbursement typically reflects some sort of charge-based or cost-plus based payment methodology. Payment reflects a preset amount (negotiated or otherwise) that may or may not reflect the costs of the provision of service.

- Expectations and requirements set by accrediting organizations, such as The Joint Commission and DNV.
- FDA regulation or guidance.
- Federal, state, or private foundation grant programs for safety net providers and facilities.
- Manufacturer product pricing.
- Facility/provider inventory management.
- Accounting standards (e.g., depreciation schedules).
- Financial margins (excess revenue to purchase capital) for both MDMs and HDOs.

It is recommended that the pilot collect a snapshot of data to be used by the individual participants. The aggregated results could then be used by non-participants to provide some measurable baseline that they can use in their decision-making, as well as informing future work. It is recommended that the pilot develop processes, data standards, etc., leveraging existing reporting and data collections that can be reused by HDOs and MDMs in ongoing collection and analysis activities.

It is recommended that the pilot:

- Identify the questions to be answered, including:
  - Lifecycle management
    - What devices, both legacy and non-legacy, are being used?
    - Where are the devices in their lifecycle when purchased, and at survey time (based on MDM product roadmaps and defined lifecycle dates)?
    - Are the devices at EOL?
    - Are any components within the device at EOL?
    - Are there observable patterns, correlations, and trends in the data? (e.g., does lifecycle misalignment or different patching cadences correlate with device type, HDO size, or device management approach?)
    - Are the devices inventoried and tracked?
  - Vulnerability management
    - Are the devices patched? Who patches the devices (MDM, HDO, or third-party service provider)? What is the patching cadence?
    - Can the device be patched?
    - Does the MDM have a dedicated team for patch development for each device or a single team for all devices?
    - Will the MDM share data with the HDO to allow support after end of life so risk transfer can occur?
  - Cost structures and implications

        - What are the costs to MDMs continuing to provide service for a supported device? For a device no longer supported?
        - What are the costs to HDOs in maintaining the device (e.g., additional security controls, equipment maintenance contracts, training clinical engineering staff on maintenance)?
        - What is the cost of replacement versus the cost of additional controls?
        - What is the impact on quality of care and patient safety by using the legacy medical devices?[3]
- Explore data collection challenges and develop solutions
    - Identify data sources that can be used to answer the questions. Ideally, it is recommended that the pilot identify existing data sources to reduce the burden on collecting data such as existing asset inventories, information that devices may report to electronic health record (e.g., laboratory information systems), data from healthcare passive monitoring tools, financial data from HDOs and MDMs, and MDM SBOMs. The recently published *Hospital Cyber Resiliency Initiative Landscape Analysis* [4] contains some high-level data on cybersecurity costs, which can serve as a starting point for measuring the total cost of ownership of legacy medical devices.
    - Define standards for the data to facilitate analysis and correlation across data sources.
    - Define a representative sample to include small, medium, and large HDOs and MDMs.
    - Develop tools for importing, cleaning, and analyzing data.

Recommendation 2: Develop information sharing agreement templates to increase transparency

Information sharing agreements (ISAs) are commonly used to describe expectations for cybersecurity design and practices between MDMs and HDOs. These agreements are typically initiated by HDOs and may take the form of or be included within Business Associate Agreements (BAAs), Health Insurance Portability and Accountability Act (HIPAA) security agreements, Authority to Operate rules, Non-Disclosure Agreements (NDAs), and HDO specific information sharing agreements created by its legal and security representatives as a blanket to apply to all medical devices regardless of expected product use and/or connected status. A broad range of HDO and MDM stakeholders are involved throughout the review and implementation of the ISAs, along with post-agreement management often requiring extensive resource engagement.

Given the complexity and diversity of these agreements, it would be beneficial for HDOs and MDMs to have template ISAs to be used as models to streamline the process and ensure that appropriate expectations are included for managing legacy medical device

[3] The Responsibility Transfer Framework in HIC-MaLTS offers guidance on assessing the risk of using these devices.

cybersecurity risks. When developing these templates, the HSCC *Model-Contract Language for MedTech Cybersecurity* document [5] can be used as a starting point, but ISAs are typically more detailed and granular.

It is recommended that ISAs include expectations for security controls, device access (e.g., credentials), identification and timely management of product security vulnerabilities for products sold and supported by the vendor for the product life, and potential requirements for support after useful life period has expired for some legacy capital devices. HDOs and GPOs have developed questionnaires used during procurement to identify secure configuration management practices used by MDMs to strengthen the security and resilience of the devices; controls used by MDMs to reduce and manage risks throughout the lifecycle; agreements on support for incident response, recovery, and repair; and processes used by MDMs to securely develop and manage devices. It is recommended that a sample of these questionnaires are analyzed to identify a common set of expectations to be used in developing the template ISAs.

It is recommended that ISAs have clear definitions for what is defined as a connected medical device or system, including expectations for limited connectivity to support cybersecurity updates and system updates as mandated by the ISA. For example, it may be important for devices that do not require always-on connectivity to allow connected or physical access to support updateability per contractual expectations. It is recommended that ISAs contain consistent vulnerability management identification, classification, and remediation timelines.

Recommendation 3: Establish security architecture working group

Managing the risk of legacy medical devices is a shared responsibility. However, there is a lack of visibility into medical device security architectures on the part of HDOs, and a lack of visibility into HDOs' network and security environments on the part of MDMs. In part, this is due to concerns about potential loss of intellectual property, as well as exposing sensitive information to third parties and malicious actors. Developing baseline security architectures based on security controls and an understanding of generic information flows and functional components could enable HDOs and MDMs to work together to better manage cyber risks of legacy medical devices within clinical and other healthcare environments.

Establishing a security architecture working group that includes a broad range of stakeholders is recommended, in order to:

- Identify and prioritize security controls that may be implemented within devices and within an HDO's network infrastructure to improve cyber risk management.
    - It is recommended that these efforts use standards such as National Institute of Standards and Technology (NIST) Cybersecurity Framework [6], Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 r5) [7], and *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide (NIST 800-66 r2)* [8].
    - It is recommended that these efforts leverage work on developing security baselines, such as the U.S. Department of Health and Human Services

(HHS) 405d HSCC Cybersecurity Working Group's *Health Industry Cybersecurity Practices* [9] and the HSCC Cybersecurity Working Group's *Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry* [10].

  - It is recommended that these efforts analyze a sample of the questionnaires used by HDOs and GPOs during procurement to identify common types of controls for protecting devices against cyber incidents, controlling access to the device, protecting data at rest and in transit, and monitoring and alerting, etc.

- Identify generic functional and network components that can be used in a high-level architectural description. Both MDMs and HDOs could use these to develop threat models to identify threat boundaries and responsibility for securing different parts of the architecture. See *Playbook for Threat Modeling Medical Devices* [11].
- Develop a standardized way of describing controls, functional and network components, and information flows. This includes defining necessary attributes, such as the owner of a security control (i.e., MDM, HDO), protocols, sensitivity of data, encryption algorithms, authentication methods, etc.
- Develop example generic architectural descriptions. These descriptions can be tailored by MDMs and HDOs for two main purposes:
  - Sharing security information during procurement.
  - Fostering design collaboration in new product development.

Recommendation 4: Develop research program in modular design for medical devices

If medical devices were designed to be more modular, (e.g., isolating the software platform and clinical software, and splitting hardware components across multiple circuit boards), legacy software and hardware could be replaced, and an HDO could have the option to upgrade those components instead of a total replacement of the device or adding expensive network controls to manage legacy risk.

A research program funded by agencies, such as Advanced Research Projects Agency for Health (ARPA-H), National Science Foundation, or Department of Homeland Security (DHS) Science and Technology Directorate, is recommended to explore both modular design techniques for medical devices and efficient ways to verify and validate that upgrading modules does not impact the essential performance of medical devices (to speed up the regulatory approval process, when required). The results of this research program could be adopted by manufacturers in their designs. In addition, students and other researchers would learn about modular design, and could then bring that knowledge to MDMs and other stakeholders.

There are economic considerations in the adoption of modular design, and the data recommended to be gathered during the collection pilot may be able to contribute to the discussion about the tradeoffs.

3.3 Vulnerability Management

Legacy devices, by definition, cannot be reasonably protected against current cybersecurity threats. Thus, it is important to develop approaches to vulnerability risk management that reduce the risks posed by legacy devices to acceptable levels.

Vulnerability management is a complex process. HDOs may be notified of vulnerabilities through various channels: MDMs (MDMs may push out notifications to HDOs or HDOs may visit MDMs' websites), government alerts (e.g., Cybersecurity and Infrastructure Security Agency [CISA] alerts, FDA Safety Communications), Health Information Sharing and Analysis Center (H-ISAC) alerts, third-party service providers, and public disclosures, among others. Once an HDO learns of a vulnerability, it needs to determine which devices in its environment are at risk from the vulnerability. For vulnerabilities in widely used third-party components, this may require communication with MDMs and possibly conducting risk assessments for hundreds or thousands of devices. Development of patches by affected MDMs and determination of how the patch(es) can be delivered (i.e., installed by MDM on-site, installed by MDM remotely, installed by HDO, installed by third-party service provider) by affected HDOs then takes place. If a vulnerability is disclosed prior to a patch being available to fix it (i.e., zero-day vulnerability), HDOs may need to install additional compensating controls and mitigating configurations, generally provided by the MDM, to manage the risk prior to receiving, deploying, and testing the patch.

Recommendation 5: Conduct study on vulnerability management coordination

The current vulnerability management process is resource-intensive and time-consuming for HDOs, MDMs, and other stakeholders/entities. A study could explore approaches to streamlining and improving the process. It is recommended that the study include:

- Determination of the feasibility of a centralized or federated repository for vulnerability and patch notifications. A benefit of a federated repository is that existing information sharing organizations, such as the H-ISAC or the HHS Health Sector Cybersecurity Coordination Center, could participate and augment this repository without standing up an entirely new governance structure.
- Protection of MDM proprietary information.
- Ensuring information is actionable and is directed to the appropriate individuals within the affected organizations. For example, if an HDO third-party service provider is involved, they and the HDO both need to be informed about vulnerabilities. In this case, while the service provider implements the patch or mitigations, the HDO remains responsible for managing the overall risk.
- Identifying areas for automation.
- Leveraging SBOMs and government databases (e.g., National Vulnerability Database and Known Exploited Vulnerabilities database) to determine affected devices and assess risk.
- Establishing clear expectations, aligned with existing laws and regulations, including for example FDA, between HDOs and MDMs on timing and delivery of

patches. For example, the exploration of preferences and defining criteria for out-of-band patching versus bundled with features (this can be included in ISA templates).

- Exploring timely development of controls, with responsibility shared between MDMs (device configuration changes) and HDOs (additional/modified network controls). The generic architectural descriptions recommended above may facilitate this process.
- Defining processes for implantable devices and home-use devices where the patient is required to be more involved.

If the study determines that a repository is feasible, it will be important to consider the governance structure. A voluntary public-private partnership could be established. Oversight might be through a Critical Infrastructure Partnership Advisory Council recognized mechanism that allows for sharing of information between the U.S. government and the private sector through protected communications. Since it is critical to support less-resourced HDOs, it will be important to consider different business models, such as free membership/services for less-resourced HDOs (absorbed by the partnership or subsidized by government, insurance, etc.), or a tiered fee structure.

It is recommended that the study review other information-sharing public-private partnerships, both within the healthcare sector and other industries (e.g., the Federal Aviation Administration's Aviation Safety Information Analysis and Sharing System). Some of the issues considered in the study may benefit from piloting activities, such as approaches for automation and developing actionable information. The study should also consider the potential synergy between this repository and on-going data collection activities proposed in Recommendation 1.

3.4 Workforce Development

Managing the risks of legacy devices and minimizing the impact of devices becoming unsupported requires a skilled workforce. Competency Models[4] can be used by an organization to determine what skills and knowledge are required for different roles supporting critical functions that directly or indirectly manage legacy risk. The Competency Model is intended to underscore the necessary professional development needs each organization may benefit from focusing on. It can be used to communicate and understand expectations for current and future organizational needs. It can also be used to consider career moves and the preparation required for those moves, which ultimately will serve to make a more effective and unified function. The Competency Model can identify skill gaps, which can be filled organically through training programs or through third-party service providers.

[4] Competency models consist of "a collection of knowledge, skills, abilities and other characteristics (KSA&Os) that are required for effective job performance." (https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Competency%20Modeling%20Documentation.pdf). Organizations create their own competency models to help employees in their professional development.

Figure 1. HDO Competency Model Template

Recommendation 6: Development of competency models for roles related to legacy cyber risk management

Figure 1 depicts a template for a competency model appropriate for HDOs:

- *Cybersecurity core competencies:* Skills that are needed in core areas depending on how the role within a function supports the organization.
    - There are different skill levels:
        - Core (basic skills, such as communicating with cross-functional teams)
        - Advanced (technical skills, such as enterprise architecture, for identifying solutions)
        - Operational (operational management skills, such as strategic planning)
- *Critical areas and functions:* The role's responsibility within the organization that influences legacy cyber risk management (note that a single individual might have multiple roles). For an HDO, these include: IT infrastructure, biomedical engineering, clinicians, cybersecurity/information security, and management. For each area, specific competencies may be defined. For example, the NIST National Initiative for Cybersecurity Education (NICE) Framework [12] defines competencies for cybersecurity workforces and the HCSS *Health Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent* [13] contains useful information specific to healthcare.
- *Support and services:* Available resources, tooling, etc., to help develop the organization's workforce such as resources from FDA, CISA, the HSCC Cybersecurity Working Group, IMDRF, the American Hospital Association, and

NIST. These resources may include materials for implementing cybersecurity competencies, as well as instructional courses, workshops, and webinars.

- *Timing*: How to prioritize and push out workforce development programs or initiatives.

Recommendation 7: Identify resources for workforce development

Less-resourced HDOs may have limited resources for workforce development initiatives, and therefore, it will be important to identify resources to support workforce training. Example resources include:

- CISA provides a collection of cybersecurity training resources (https://www.cisa.gov/cybersecurity-training-exercises), including the *Workforce Training Guide* and *Cyber Career Pathway Tool* to help cybersecurity professionals expand their skills, as well as resources for organizations to conduct cybersecurity exercises and other training.
- The Federal Virtual Training Environment (https://fedvte.usalearning.gov/public_fedvte.php) offers free cybersecurity courses to the public, including courses on securing networks and cloud infrastructure, managing cyber risk, and defending against cyber incidents.

3.5 Mutual Aid

Maintaining a secure and resilient healthcare delivery organization is challenging for well-resourced hospitals, and extremely challenging for the less resourced safety net and rural hospitals. Legacy devices are a risk that is faced by all. Collaboration and mutual aid across HDOs, particularly between well-resourced and less resourced HDOs, can be beneficial as these organizations confront growing cyber risks and require assistance in managing impacted legacy devices.

Recommendation 8: Participation in mutual aid partnerships

There are different models for mutual aid including ad-hoc relationships, private sector partnerships, and state/local government partnerships. Recommendations for potential mutual aid partnerships are as follows:

- HDOs that already have existing clinical relationships may engage in ad-hoc, informal cybersecurity mutual aid. Because of these clinical relationships, larger HDOs in a region may already be familiar with the clinical environment of smaller, less-resourced HDOs and could provide best practices and technical assistance. This is facilitated by November 2020 Centers for Medicare & Medicaid Services (CMS) and the HHS Office of Inspector General final rules amending the Stark Law and Anti-Kickback Statute,[5] which created the Cybersecurity Exception and

[5] The Anti-Kickback Statute "prohibits offering, paying, soliciting or receiving anything of value to induce or reward referrals or generate Federal health care program business" and the Stark Law "prohibits a physician from referring Medicare patients for designated health services to an entity with which the physician (or immediate family

Safe Harbor to protect the donation of certain cybersecurity technology and services to address increasing cyber threats. To facilitate this sharing of information and expertise, it is recommended that the participating entities arrange preliminary NDA and BAA agreements, establishing expectations and understandings of the ability to freely share data and resources, and potential limitations. These mutual aid plans between HDOs can mirror or leverage all-hazard mutual aid agreements, such as those for in times or natural disaster or mass casualty events, that may already exist.

- Regional healthcare organizations may form private sector partnerships to collaborate and share on topics and challenges around cybersecurity. These partnerships may hold regular meetings or telephone calls to discusses a variety of topics and allow members to ask questions about how others are solving problems/challenges, technologies that members employ, how controls are implemented, and exchange ideas and best practices. These groups may also conduct tabletop exercises for their membership. An example partnership is the Mid-Atlantic Cybersecurity Alliance, which was founded by BeeBee Health and Christiana Care Health System; members include hospitals, clinics, the Delaware Information Exchange, Delaware Medical Society, and other organizations in New Jersey and Maryland.
- State and local government may organize regional partnerships. These partnerships may include local agencies, such as law enforcement, fusion centers, and offices for emergency management and public safety. In addition to healthcare organizations such as hospitals, clinics, nursing homes, and state health information exchanges, some activities may include other critical infrastructure entities that service HDOs and related entities (e.g., water and wastewater systems and energy sectors). These partnerships may have regular meetings or calls to share current threat information and cybersecurity topics of interest to the membership. The partnership may conduct exercises, both sector-specific and cross-sector, and involve local government authorities in addition to the private sector organizations. The MassCyberCenter and the Massachusetts eHealth Initiative (MeHI) have organized a state cybersecurity partnership focused on healthcare, which holds monthly cyber calls for healthcare providers and partner organizations and conducts regional resiliency exercises for healthcare and other critical infrastructure sectors.[6]

The *Medical Device Cybersecurity Incident Regional Preparedness and Response Playbook* [14] provides information on regional partnerships and cybersecurity resources that are freely available from CISA, HHS, and other sources.

CISA has a state and local cybersecurity grant program, which could provide funding to a state or local government to set up a regional partnership (see: https://www.cisa.gov/state-and-local-cybersecurity-grant-program).

member) has a financial relationship, unless an exception applies" (https://oig.hhs.gov/documents/provider-compliance-training/939/StarkandAKSChartHandout508.pdf). The 2020 final rules created an exception for cybersecurity technology and services.

[6] MassCyberCenter and MeHI are divisions of the Massachusetts Technology Collaborative (https://masstech.org/about-masstech).

4 Conclusion

This paper has identified several approaches to address legacy challenges based on previous work:

- First, managing the risk of legacy medical devices is a shared responsibility over the lifecycle of a medical device. It will be important to collect data to understand the magnitude of the problem and the economics from both the MDM and HDO perspectives, which will enable informed decision making by HDOs and MDMs as well as developing new policies and incentives. In addition, it will be important to develop tools for increasing transparency, both to convey security expectations and to share technical information to support managing legacy medical device cybersecurity risks.
- Second, vulnerability management is complex, and it will be important to investigate approaches to streamline coordination of vulnerability notification and patching/mitigations.
- Third, managing legacy medical device cybersecurity risks requires a skilled workforce defined with a competency model.
- Finally, it will be important for less-resourced HDOs to manage legacy medical devices, and regional mutual aid approaches may be able to help.

By addressing legacy medical device risk, medical device cybersecurity can be improved, and patient safety safeguarded from growing cyber risks.

5 References

[1] IMDRF, "Principles and Practices of Cybersecurity for Legacy Medical Devices (IMDRF/Cyber WG/N70Final:2023)," 11 April 2023. [Online]. Available: https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices.

[2] IMDRF, "Principles and Practices for Medical Device Cybersecurity (IMDRF/Cyber WG/N60Final:2020)," 18 March 2020. [Online]. Available: https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity.

[3] HSCC Cybersecurity Working Group, "Health Industry Cybersecurity: Managing Legacy Technology Security (HIC-MaLTS)," March 2023. [Online]. Available: https://healthsectorcouncil.org/wp-content/uploads/2023/03/Health-Industry-Cybersecurity-Managing-Legacy-Technology-Security-HIC-MaLTS.pdf.

[4] U.S. Department of Health and Human Services and HSCC Cybersecurity Working Group, "Hospital Cyber Resiliency Initiative Landscape Analysis," April 2023. [Online]. Available: https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf.

[5] HSCC Cybersecurity Working Group, "Model Contract Language for MedTech Cybersecurity (MC2)," March 2022. [Online]. Available: https://healthsectorcouncil.org/model-contract-language-for-medtech-cybersecurity-mc2/.

[6] NIST, "NIST Cybersecurity Framework," [Online]. Available: https://www.nist.gov/cyberframework.

[7] NIST, "Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 r5)," July 2023. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[8] NIST, "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: NIST SP 800-66r2 ipd," July 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.ipd.pdf.

[9] U.S. Department of Health and Human Services and HSCC Cybersecurity Working Group, "Health Industry Cybersecurity Practices," 2023. [Online].

[10] HSCC Cybersecurity Working Group, "Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry," May 2023. [Online]. Available: https://healthsectorcouncil.org/wp-content/uploads/2023/06/Considerations-for-Prioritized-Recognized-Cybersecurity-Practices.pdf.

[11] The MITRE Corporation, "Playbook for Threat Modeling Medical Devices," November 2021. [Online]. Available: https://www.mitre.org/news-insights/publication/playbook-threat-modeling-medical-devices.

[12] NIST, "Workforce Framework for Cybersecurity (NICE Framework). NIST SP 800-181 r1," November 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

[13] HSCC Cybersecurity Working Group, "Health Industry Cybersecurity Workforce Guide: Recruiting and Retaining Skilled Cybersecurity Talent," June 2019. [Online]. Available: https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-Workforce-Updated-Format.pdf.

[14] The MITRE Corporation, "Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook," November 2022. [Online]. Available: https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response.

Appendix A Summary of Recommendations

	Shared Responsibility Over the Medical Device Lifecycle
Recommendation 1	Pilot data collection to support decision making for legacy device risk management
Recommendation 2	Develop information sharing agreement templates to increase transparency
Recommendation 3	Establish security architecture working group
Recommendation 4	Develop research program in modular design for medical devices
	Vulnerability Management
Recommendation 5	Conduct study on vulnerability management coordination
	Workforce Development
Recommendation 6	Development of competency models for roles related to legacy cyber risk
Recommendation 7	Identify resources for workforce development
	Mutual Aid
Recommendation 8	Participation in mutual aid partnerships

Appendix B Abbreviations and Acronyms

Term	Definition
BAA	Business Associate Agreement
CIO	Chief Information Officer
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CMS	Centers for Medicare & Medicaid Services
DHS	Department of Homeland Security
EOL	End of Life
EOS	End of Support
FDA	U.S. Food and Drug Administration
GPO	Group Purchasing Organization
H-ISAC	Health Information Sharing and Analysis Center
HCP	Healthcare Provider
HSCC	Healthcare and Public Health Sector Coordinating Council
HDO	Healthcare Delivery Organization
HHS	U.S. Department of Health and Human Services
HIC-MaLTS	Health Industry Cybersecurity – Managing Legacy Technology Security
HIPAA	Health Insurance Portability and Accountability Act
IMDRF	International Medical Device Regulators Forum
ISA	Information Sharing Agreement
MeHI	Massachusetts eHealth Initiative
MDM	Medical Device Manufacturer
NDA	Non-disclosure Agreement
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
SBOM	Software Bill of Materials
TPLC	Total Product Lifecycle