IMDRF International Medical Device Regulators Forum

Final Document

IMDRF/CYBER WG/N73FINAL:2023

Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

AUTHORING GROUP

Medical Device Cybersecurity Working Group

Preface

Andrzej Rys, IMDRF Chair

Contents

1. Introduction

Digital connectivity of medical devices has made patient care more efficient, data-driven, and effective. Utilization of and reliance on third-party software components has made developing such medical devices more economical, more reliable, and increased the pace of innovation. While utilization of third-party software components provides many benefits, they may introduce cybersecurity risks with a potential to impact patient safety and the confidentiality, integrity, and availability of network-connectable medical devices.

Cybersecurity vulnerabilities are unique in that they may impact a diverse range of seemingly secured unrelated devices across various manufacturers due to the use of common software components. This problem is compounded by low traceability of those common components within devices. To address the global issue, the US National Telecommunications and Information Administration (NTIA) convened a multi-sector initiative of various stakeholders in 2018 to discuss software transparency. One output was the software bill of materials (SBOM) concept, which NTIA defined as a “list of one or more identified components, their relationships, and other associated information.” This initiative has informed SBOM development and adoption internationally.

The SBOM is a resource which can be leveraged to improve cybersecurity risk management processes in both pre-market and post-market activities (i.e., the Total Product Lifecycle or TPLC). For example, in the pre-market phase, medical device manufacturers (MDMs) can use SBOM resources during device development to track known software vulnerabilities and prevent release of devices with known cybersecurity risks. In the post-market, MDMs can use SBOM as a resource to supplement their vulnerability monitoring processes to identify at-risk devices released in the market.

An SBOM can support improved cybersecurity risk management processes throughout the TPLC as a primary or secondary resource. Benefits may include, but are not limited to:

- Faster and more comprehensive identification of software components in a device,
- more secure software development through better informed decision-making, and
- increased software transparency among vendors and stakeholders.

To gain the most benefit from SBOM, it should be used in conjunction with other cybersecurity risk management tools and procedures like those described in Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020), hereinafter also referred to as “IMDRF N60 guidance”. IMDRF N60 included an SBOM as part of the customer security documentation to be prepared by the MDM and provided to the device user. Medical device SBOMs benefit both MDMs and healthcare providers throughout the TPLC. For instance, SBOM is an effective management tool to track and prepare for software component End of Life (EOL). If an MDM knows the software components and their respective end of life dates, MDMs can better prepare themselves and their customers for any associated risks, which improves MDMs’ quality control capabilities. Device users benefit from increased transparency and cybersecurity information disclosure which allows them to implement cybersecurity activities based upon their individual risk profiles and cybersecurity capabilities. For example, an SBOM provided pre-purchase and pre-installation allows healthcare providers to know which devices can be deployed to meet their risk profile or might contain out-of-date software that can pose cybersecurity issues before purchasing. Manufacturers should supply a software bill of materials (SBOM) with their products. SBOM needs to support the varied needs, resources, and capabilities of all these HCPs. As SBOM adoption grows, advancements in tooling, services, and cybersecurity maturity will enable HCPs to leverage the SBOM to its fullest extent. Additionally, when provided with an SBOM, the customer (which can be HCPs or patients) can better assess the device cybersecurity risks.

An SBOM provided in pre-market submissions to a regulator is one indicator that the MDM has a mature cybersecurity program. An SBOM also allows the regulator a more complete benefit-risk assessment for the product. In the post-market, a more comprehensive understanding about which marketed devices have access to an SBOM can assist MDM, HCP (healthcare providers) and regulators with input from the MDM in estimating and addressing threat, vulnerability, and exploit impact.

As SBOM adoption grows within and across sectors, its value to organizations will increase. Stakeholders have different roles and uses of SBOM, such as SBOM generation, management, distribution, ingestion, and utilization.

This guidance provides a high-level description of an SBOM and best practices for the generation and use of an SBOM. The purpose of this document is to provide greater detail on the implementation of SBOM and software transparency as relevant to medical device stakeholders, including MDMs, healthcare providers (HCPs), and regulators. In this guidance, healthcare providers include healthcare delivery organizations (HDOs).

Additional insights regarding SBOM benefits are found in NTIA's FAQ document and their "Roles and Benefits of SBOM Across the Supply Chain" document.

2. Scope

This document considers cybersecurity in the context of medical devices that either contain software, including firmware and programmable logic controllers (e.g., pacemakers, infusion pumps) or exist as software only (e.g., Software as a Medical device (SaMD)). The document emphasizes the roles and responsibilities of MDMs and HCPs and provides recommendations on the implementation of an SBOM and increased transparency in the use of software in medical devices, including in vitro diagnostic (IVD) medical devices. While primarily focused on MDMs and HCPs, we believe that other stakeholders, including but not limited to medical device users, regulators, and software component vendors, may also find the concepts discussed in this document useful.

Protection of the cyber healthcare environment is a shared responsibility of HCPs and MDMs. The SBOM is a common tool to support safety as it can help to mitigate against the potential for patient harm. This document is intended to:

- Provide recommendations for medical device manufacturers in SBOM generation, management, and distribution.
- Provide recommendations to healthcare providers on ingestion and management of an SBOM.
- Demonstrate SBOM use cases for risk management, vulnerability management, and incident response from the perspective of medical device manufacturers and healthcare providers.

SBOMs are not a substitute for comprehensive security risk assessment, it takes knowledge of the device's intended use, the architecture and the design of the whole device to make a security risk assessment at the device level.

Due to most regulators' authority over medical device safety and performance, the scope of this guidance is limited to consideration of the potential for patient harm related to the regulated medical device. Differences across medical device types and regulatory jurisdictions may give rise to specific circumstances where different or additional considerations are required. For example, threats that could impact performance, negatively affect clinical operations, or result in diagnostic or therapeutic errors are considered in scope of this document. Other types of harm, such as those associated with breaches of data privacy, are not considered in the scope of this document; however, we acknowledge that these matters important, and SBOM may be a useful mitigation tool.

This document does not address SBOM-related issues and recommendations unique to cloud services that are provided in a remote computing environment (i.e., cloud services are on-demand internet access to computing (e.g., networks, servers, storage, applications) services). Cloud services that are a component of the regulated medical device system may also present a risk to safety and effectiveness. Manufacturers of regulated medical devices should be aware that cloud services and cloud software must also be reviewed in risk evaluations. Due to the complexities of cloud services which are further complicated when manufacturers leverage third-party clouds rather than manufacturer-controlled private clouds, this first IMDRF SBOM guidance does not yet include cloud technology explicitly within SBOMs. However, as technology evolves and understanding of the cloud increases from a regulatory perspective, it will be important to address the residual risk of cloud technology in the context of SBOM. It is anticipated that this and other risks will be considered in future work.

This document is complementary to the preceding IMDRF N60 guidance, and the scope of relevant medical devices, as well as the focus on potential for patient harm, remain unchanged. This document continues to recognize that cybersecurity is a shared responsibility among stakeholders.

While SBOM can address various software transparency issues including licensing and intellectual property, this document focuses on the cybersecurity concerns relevant to SBOM.

3. Definitions

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

3.1 *Application programming interface (API):* set of standard software interrupts, calls, functions, and data formats that can be used by an application program to access network services, devices, or operating systems (ISO 10303-1:2021)

3.2 *Asset:* physical or digital entity that has value to an individual, an organization or a government (ISO 81001-1:2021)

3.3 *Asset management:* coordinated activity of an organization to realize value from asset (ISO/IEC 9770-5:2015)

3.4 *Change management:* process for recording, coordination, approval and monitoring of all changes. (ISO 81001-1:2021)

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

3.6 *Cybersecurity:* a state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle. (ISO 81001-1:2021)

3.7 *Cybersecurity Incident*: A cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery. (National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.)

Note: A cybersecurity event is a cybersecurity change that may have an impact on organizational operations (including but not limited to mission, capabilities, or reputation)

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

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

3.9 *Hash, hash-value:* value calculated by a hash function, which is a computation method used to generate a random value of fixed length from the data of any optional length. (ISO 17090-4:2020)

3.10 *Legacy Medical Device (syn. Legacy Device):* Medical device that cannot be reasonably protected against current cybersecurity threats (IMDRF/CYBER WG/N60FINAL:2020)

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

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

3.13 *Releases and Update:* corrective, preventative, adaptive, or perfective modifications made to software of a medical device

NOTE 1: Derived from the software maintenance activities described in ISO/IEC 14764:2006.

NOTE 2: Updates may include patches and configuration changes.

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

3.14 *Repository:* organized and persistent data storage that allows data retrieval. (ISO/IEC/IEEE 26511:2018)

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

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

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

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

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

3.18 *Software composition analysis*: use of one or more tools for scanning a code base to identify what code – e.g., closed source software, free and open-source software, libraries, and packages – is included.

NOTE: These tools may also check for reported vulnerabilities pertaining to the code included. (https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf)

3.19 *Software transparency:* the schematic structure of the software that reviews all the frame, hierarchy, and components of the software.

3.20 *System*: the combination of interacting elements or assets organized to achieve one or more function (ISO/IEC/IEEE 12207:2017)

3.21 *Third-party software*: software provided by a person or body that is recognized as being independent of the parties involved. (Modified from ISO/IEC Guide 2)

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

3.22 *Use case*: specification of a sequence of actions, including variants, that a system (or other entity) can perform, interacting with actors of the system. (ISO/IEC 23643:2020)

3.23 *Vulnerability Exploitability eXchange (VEX):* Machine readable assertion about the status of a vulnerability in specific products

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

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

4. Overview of SBOM Framework

At a high level, SBOM content is collected by the MDM and is housed in a software component repository (see also NTIA "Software Suppliers Playbook: SBOM Production and Provision"). The device SBOM is then compiled and generated by the MDM and released for distribution so it can be leveraged by the HCP. The following sections provide more detailed information regarding the generation, distribution, and ingestion of an SBOM from both the MDM and HCP perspective.

Figure 1 shows a high-level framework where information sharing is enabled, and software transparency is enhanced via SBOM generation/ingestion between MDMs and HCPs. Under this framework, considerations both for MDMs and HCPs are addressed.

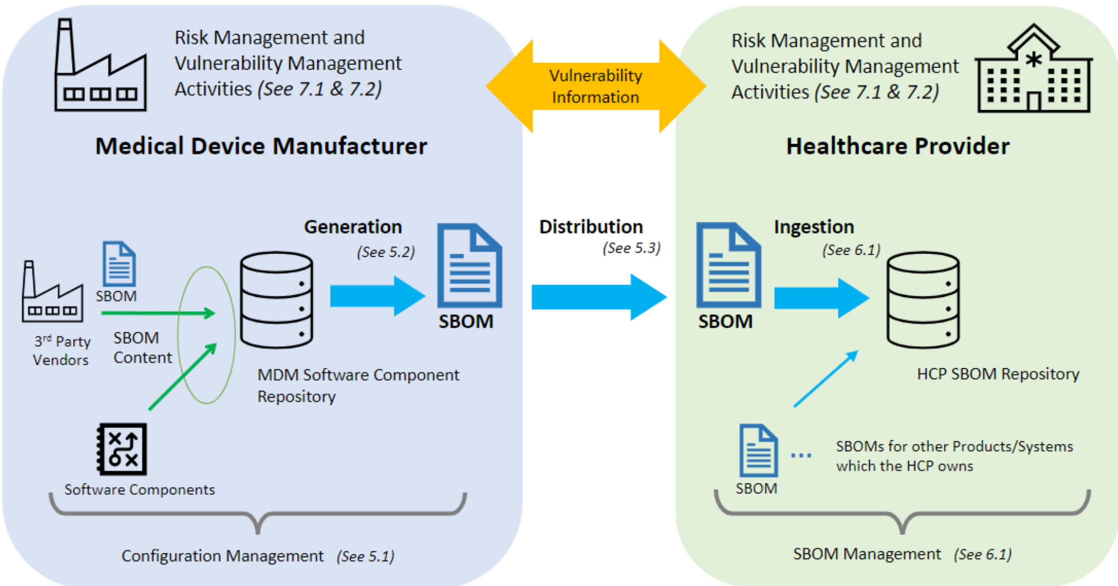

Figure 1: High-level framework for SBOM

5. Overview of Manufacturer Considerations

This section provides an overview of MDM considerations for SBOM including collecting SBOM content, generating an SBOM, distributing an SBOM, and maintaining the SBOM content (including vulnerability monitoring and change management). It is noted that a device SBOM itself is not maintained, since a new device SBOM is created and released with new product versions. However, from the perspective of the end user who receives the new device SBOM, it is an update to the previous device SBOM. The only way this update can be made is if the associated documentation and processes for the SBOM content are maintained. The terminology “maintain SBOM content” and the intent behind this description is further described in Figure 2.

During the software development life cycle (SDLC) stages of Design, Code-Build-Test, various types of software components are incorporated into the medical device. The SBOM content for these components should be collected and stored in the MDM software component repository with other related information as part of configuration management activities. The SBOM should be generated from this repository and distributed to HCPs as Deploy/Release phase activities. HCPs can get the SBOM during the procurement process or at the time of software release. After the SBOM is released, vulnerability monitoring can trigger change control to relevant software components and then feed back into SBOM content collection and the software component repository. Figure 2 provides additional granularity regarding SBOM management across the SDLC.

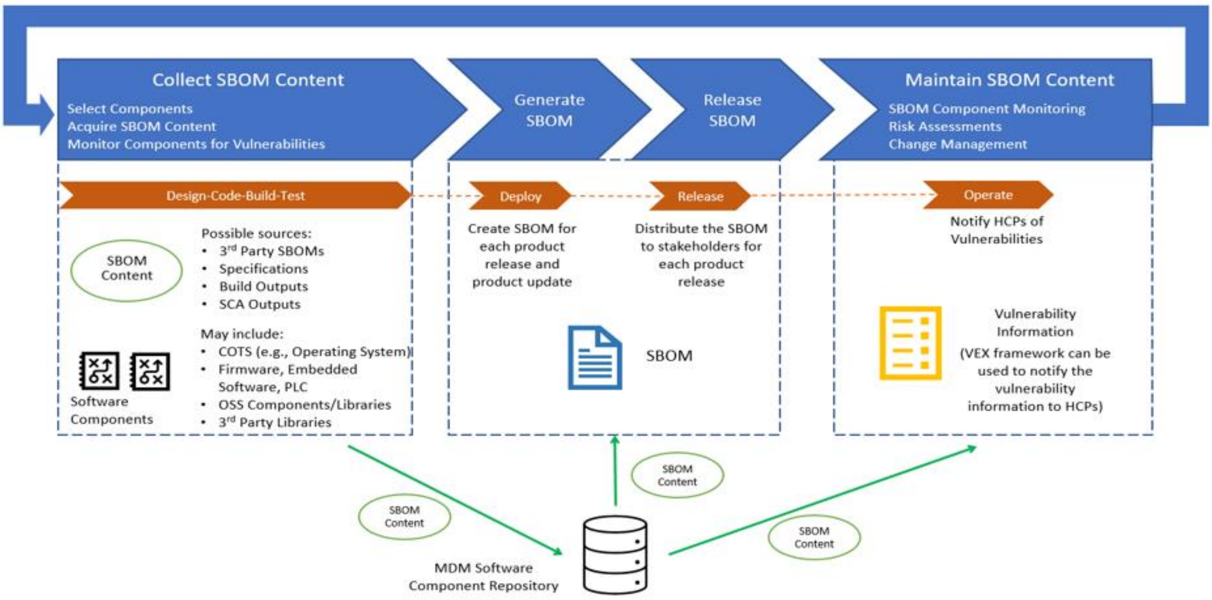

Figure 2: SBOM management across the software development life cycle (SDLC)

5.1. Collect SBOM Content

SBOM content collections begins in the SDLC design phase. SBOM content can come from a variety of sources, including:

- the proprietary software development documentation;
- third-party SBOM documentation provided by commercial software vendors;
- documentation provided with open-source software, or
- output generated by software composition analysis (SCA) tools.

Applicable SBOM content is collected during design-code-build-test and is then maintained in the MDM software component repository SBOM content needs to be collected for the medical device system, including components contained within peripherals which are part of the medical device system. This may require different sources and tooling. For example, relevant components may be identified with an SCA tool used to scan product. Alternatively, vendors for components like firmware, embedded software, and programmable logic controllers (PLCs) may provide SBOMs that the MDM can incorporate into their software component repository.

Additional details regarding the component types that may be included in the MDM software component repository and tooling used to collect this content is found in Appendix 9.1.

5.2. Generate an SBOM

For SBOM generation, manufacturers need to consider the entire software supply chain. To generate the SBOM, the applicable SBOM content should be aggregated into a device SBOM for each product release and product update. The final device SBOM for each product release and product update should be maintained and available for distribution. SBOM generation should follow a defined and established methodology to ensure consistent output. Thus, the SBOM is updated and maintained throughout the life cycle of the device.

The following section describes considerations for SBOM elements and format. Additional insights regarding SBOM generation and tooling may be found in NTIA's "How to Guide for SBOM Generation."

5.2.1. SBOM Elements and Formats

Each SBOM entry should contain information to identify each software component. The information available to include in an SBOM entry may vary, but in general, SBOMs should be as complete as possible as the depth of the SBOM impacts its utility. Access to more complete SBOM information enables faster vulnerability identification and assessment, which support improved device cybersecurity. Consistent with recommendations from NTIA, for medical device cybersecurity, a baseline SBOM should include the following elements:

- Author name: refers to the entity (i.e., an individual, organization, or similar) which produced the SBOM file.
- Timestamp: Record of the date and time of the SBOM data assembly.
- Software component vendor (supplier): The entity that creates, defines, and identifies components. Software component vendor name should generally refer to the legal business name for commercial software.
- Software component name: Designation assigned to a unit of software defined by the original supplier.
- Software component version: Identifier used by the supplier to specify a change in software from a previously identified version.
- Unique Identifier: Identifiers that are used to identify a component or serve as a look-up key for relevant databases.
- Relationship: Describes the relationship that an upstream component X is included in software Y".

The elements included in a SBOM are characterized by basic information that allows for their identification. Other information can be added to the SBOM as additional elements or as a supplement to the core SBOM, as needed. For example, a component hash is recommended because it can help map a component's existence to relevant data sources. In addition, considerations relevant to the life cycle of a device (e.g., a software component's end-of-support (EOS) date), could be provided as supplemental information, as it aids in medical device risk management across the TPLC.

In addition to thinking about the baseline elements to include, MDMs also need to consider the SBOM format. Currently, there are several automated SBOM formats: CycloneDX, Software Package Data Exchange (SPDX), and Software Identification (SWID). Additional information on these formats, including detailed medical device examples for SPDX and SWID, may be found in in NTIA's "How to Guide for SBOM Generation".

5.3. Distribute an SBOM

The distribution of an SBOM is the process for how the SBOM information is transferred from the manufacturer to the HCP or user. The MDM must consider how best to distribute their SBOM, including raising awareness, providing access, and pushing updates. This could be an electronic file or an application programming interface (API) on the product or on the manufacturer's website. While there is no one way to best distribute an SBOM at this time, the use of standardized automated discovery and exchange mechanisms are encouraged.

Firstly, HCPs need to be aware that an SBOM exists. SBOMs should be initially provided to HCPs as part of the procurement process. For example, this existence could be included in the product's customer security documentation (IMDRF/CYBER WG/N60FINAL:2020), the Manufacturer Disclosure Statement for Medical Device Security (MDS2, ANSI/NEMA HN 1-2019), a shared communication channel such as a publish/subscribe system, or a publishing interface on the medical device. As medical devices are updated frequently, a mechanism to easily identify a product and software version over the network in a standardized way should be encouraged to support automated updates.

Secondly, MDMs should enable the SBOM to be distributed to or accessed by the HCP. Existing methods generally fall into one of three categories:

- The SBOM is provided directly from the MDM to the HCP; or
- The SBOM resides on the medical device; or
- The SBOM is available to HCPs via a repository. An SBOM repository includes a collection of SBOMs from different products which may be from the same or different manufacturer.
    - A manufacturer-managed repository only contains SBOMs for devices from a single manufacturer while a centralized repository contains SBOMs for devices from multiple manufacturers.
    - Centralized repositories may be managed by third-party services or be healthcare provider-managed (i.e., HCPs may aggregate the device SBOMs they received from manufacturers into a centralized location for ease of use). For more information on considerations for a healthcare provider-managed repository, see Section 6.1.1.

While not an exhaustive list, the following table outlines advantages and disadvantages that MDMs should consider for SBOM distribution methods:

Table 1: Advantages and Disadvantages of Certain Methods of SBOM Generation

Method of Distribution	Advantages	Disadvantages
Included in the Customer Security Documentation from the manufacturer	• No specialized tools required	• Not automated • Documentation must be updated frequently and distributed to the user • There needs to be a way to link the document back to the device itself (strong asset management) • Less control over SBOM access
Provided by the manufacturer as a separate (electronic) document	• No specialized tools required • More control over SBOM access • Preferably machine readable	• Not automated • Documentation must be updated frequently and distributed to the user • There needs to be a way to link the document back to the device itself (strong asset management)
Accessible from the medical device through a display, reference (indirectly) or download	• Always the correct version • Under control of the user • More control over SBOM access	• Not automated • Requires access to the device to be able to access the information • The device might not have a means to extract the information (e.g., user interface, USB port, network connectivity) • Requires sufficient space on the device • May require the use of extra battery capacity (in battery operated medical devices)
Accessible from an API on the medical device	• More control over SBOM access • Can be used in an automated process	• API standards remain undefined • Requires tooling • Requires connectivity
Manufacturer-managed Repository	• More control over SBOM access • Can be used in an automated process	• Customers have to check multiple manufacturer sites/repositories for information
Centralized Repository	• More streamlined way for customers to access information (i.e., don't have to check as many individual manufacturer sites/repositories) • Can be used in an automated process	• Intellectual property, liability, and other considerations for the manufacturer when using a third-party service • Challenges with versioning as some organizations may have multiple versions of the same device with different update status and so will need to have access to all applicable SBOMs, not just the newest version

Another consideration in the distribution of SBOMs is the need to protect the SBOM information. Medical device SBOMs should be classified as sensitive/confidential information in alignment with industry best practice. Communication channels from the MDM to external recipients, regulators and HCPs need to support protection measures, to help reduce the chances of these documents being compromised and resulting in increased risk exposure. Furthermore, these external organizations (i.e., recipients of the device SBOM) need to maintain strict internal security policies and practices to protect SBOM integrity, authenticity, and confidentiality.

5.4. Maintain SBOM Content

An SBOM does not explicitly state whether a software component has a vulnerability. However, the SBOM may be used in conjunction with other resources to monitor for medical device vulnerabilities. One of the ways MDMs might notify HCPs vulnerability information is through the Vulnerability Exploitability Exchange (VEX).

During the life cycle of the medical device, each stakeholder relies on accurate and up-to-date information about the third-party software components. An MDM may use the SBOM to identify, assess, and mitigate potential patient safety risks associated with software vulnerabilities on the device. An HCP may use the SBOM to evaluate the device prior to purchase and during deployment so that they, and in collaboration with the manufacturer, can manage cybersecurity risk.

Vulnerability monitoring can trigger a change control event when it is determined that a change to the relevant software is necessary. MDMs should leverage existing change management controls (i.e., processes used to identify, document, and authorize changes to an IT environment) to ensure that any changes to device software are captured in the SBOM and that the appropriate follow-up actions are taken. Ultimately, any change in SBOM content should generate an updated device SBOM that is distributed to appropriate stakeholders, containing components that were changed.

5.4.1. SBOM and Change Management

While the Software Development Life Cycle (SDLC) has been incorporated into the pre- and post-market change management processes of medical device development in recent years, third-party component change management is still a new area for many manufacturers. It is important to understand that any event which causes the device software to change should result in a new SBOM. Such events include, but are not limited to:

- Remediation of a vulnerability through an upgrade, update, or patch,
- Addition of new functions to the medical device software,
- Exchange of one software component for another,
- Adding or removing a software component,
- Changes to third-party components that reside on the device hardware or within its operating system due to end of life (EOL) or end of support (EOS) decisions, (security) patches, or new versions coming to the market.

Change control should apply to the SBOM, which includes the proprietary medical device software and third-party software libraries. This information is not only important for internal version control, but also helps MDMs inform HCPs that a mitigation has been put in place.

Changes to the SBOM should be communicated to the HCPs on a regular basis and made available in an actionable and machine-readable format on an appropriate distribution platform.

5.5. Challenges

The SBOM has great promise for enhancing patient safety via software transparency. Generating, monitoring, and distributing a comprehensive SBOM as part of pre-market and post-market activities can be a challenge for the MDM. Adequate tools and internal processes are necessary.

This section highlights some of the challenges in implementing SBOM across the SDLC.

a. **SBOM for Currently Marketed/Legacy Devices:** SBOM is a relatively recent concept, and it is still being adopted. In general, generating an SBOM for older devices produced in the past may face difficulties obtaining an SBOM with even basic information and elements. MDMs should use their best judgement to incorporate SBOMs provided by third-party suppliers, including how composition analysis tools may be used to supplement those SBOMS when information from the third-party supplier is not available. It is still desirable to build an SBOM which may be of reduced scope and depth wherever possible, especially when it captures major software components such as the operating system, COTS software, and OSS. Doing so allows the core content of the SBOM to be extended and improved upon. This might be accomplished via the use of various tooling by HCP or other parties. MDMs should be careful to select tools with capabilities that best suit the organization's needs (e.g., providing optimal insight into the risks associated with the MDM's business). Certain SCA tools may generate SBOMs with the desired breadth and depth. SCAs can further confirm that compiler settings are set to promote security/hardening, determine whether the compiler avoided inclusion of code with vulnerabilities, the unexpected inclusion of system networking tools, and the inclusion of files containing debug information.

b. **Standards and Tools:** SBOM collection, generation, distribution, and use for vulnerability monitoring can be supported by standards and tools. High-level considerations regarding standards and tools are provided below and additional details regarding tooling used to collect SBOM content is found in Appendix 9.1. The stable, global identification of software and author need further clarification. International standards are a way that the state-of-the-art could be specified.

   i. Standards and tools continue to evolve and mature; MDMs should not wait for these to be "finalized." Rather, MDMs should generate initial SBOM applying basic/foundational SBOM concepts. For example, while tools may exist to identify the SBOM content, there may be challenges translating it to a machine-readable format and identifying those components that are vulnerable with centralized databases (such as the NIST National Vulnerability Database (NVD)). Vulnerability databases can change over time and may not be complete.

   ii. As many organizations continue working toward defining standards and tools, in the medium and long term, the MDM may be able to migrate the SBOM to newer platforms that become available.

c. **SBOM Depth:** SBOMs can be dynamic and change over time since SBOMs are created for each product release or update. Defining the right depth of SBOM content to be included in the SBOM will impact the quantity and type of resources needed to keep an SBOM up to date. Greater SBOM depth will generate higher quality SBOMs and provide higher value to the end user. However, with greater depth comes greater complexity and challenges in generating and analysing SBOMs.

d. **SBOM Distribution:** It is acknowledged that there are many challenges related to the distribution of SBOMs. These challenges include but are not limited to: (a) the frequency of software updates (b) the corresponding need to update the SBOM (c) the need to maintain distributed SBOMs in the user asset management system. An HCP may have multiple versions of the same device with different configurations and/or may update to the new software release at different times. The HCP needs to have the appropriate SBOM for each device.

6. Overview of Healthcare Provider Considerations

Healthcare environments have digitized over the last decade, and digital technology spreads across every part of the healthcare industry. This digital transformation has produced a reliance on software and software-driven devices to perform both administrative and clinical functions. Unfortunately, this digitalization has coincided with a dramatic rise in cybersecurity threats. Because the HCP landscape is increasingly digitally dependent and connected, this effects diverse HCP entities including large health systems, small rural facilities, and a growing ambulatory component, including home care.

Manufacturers should supply a software bill of materials (SBOM) with their products. This section provides an overview of healthcare organization considerations for SBOM including ingesting and intake of an SBOM and managing an SBOM. See Figure 1 for overall framework of SBOM.

6.1. SBOM Ingestion and Management

SBOMs are used as a part of HCP's risk management starting at procurement. Healthcare providers should request an SBOM from manufacturers for any devices that are intended to be integrated into their network infrastructure. To be able to leverage an SBOM, organizations should ensure they have capabilities to ingest the SBOM. It is critical for HCPs to have a complete and accurate asset inventory. The inventory should contain an up-to-date listing of medical devices with unique device identifiers, enabling correlation to other asset management systems and asset enrichment data sources such as SBOMs. An HCP needs to understand the hardware assets and the associated software running on its network. Once ingested, an SBOM should be managed to maximize organizational benefit.

This section provides an overview of healthcare organization considerations for SBOM including ingesting and managing an SBOM and specific considerations for healthcare provider-managed SBOM repositories.

6.1.1. Considerations for Ingesting and Managing and SBOM

An HCP needs to understand the hardware assets and the associated software, as well as Software as a Medical Device (SaMD) present and operating in the HCP network environment. HCPs can use established information technology and asset management practices to inventory software purchased directly from the developer or custom-developed software. However, software running on purchased devices cannot be easily inventoried through these established practices. An SBOM is a method to increase transparent sharing of this information between MDM and HCPs. Below are considerations related to an SBOM and a healthcare provider managed SBOM repository.

a. **Procurement**: An SBOM can be made available during the procurement process, which enables the HCP to review the device components. The HCP should be aware that an SBOM may change between procurement and delivery.

b. **Standard format and delivery**: Delivery of the SBOM should be done through a standard format and automated distribution and ingestion mechanism. This enables information to be efficiently ingested by an HCP and stored in a secured location to protect the integrity of the data. Three prominent formats to be considered are CycloneDx, SPDX, and SWID.

c. **Unique device identifier**: Device SBOMs are ideally mapped to a unique identifier to enable accurate correlation between an SBOM and each device due to the HCP likely having multiple models and versions. As described in the IMDRF UDI Application Guide, Unique

Device Identifier (UDI) should be referenced on a product level to ensure correct mapping to the device and manufacturer, but also include the version number of the medical device software or version number of the device itself, if applicable. The lack of standardized unique identifier for software and hardware components may result in manual mapping.

d. **Completeness**: The level of SBOM completeness affects the extent to which it can be leveraged. At a minimum, SBOM content information should include author name (company's name and/or person's name), timestamp, software component vendor (supplier), software component name, software component version, unique identifier, and relationship (See Section 5.2.1).

e. **Communication:** When a software component with a known vulnerability is discovered in a device SBOM, communication between an MDM and HCP is highly recommended to ensure actions taken to address the vulnerability are provided by the MDM and if required, approved by the HCP's national/regional authority.

f. **Enhanced device management**: HCPs need the ability to establish and manage an internal SBOM repository, linking each device in their environment to the specific SBOM for enhanced device management.

1. Search and Query Capabilities: The repository needs to have search and query capabilities to accurately identify and manage risk across the HCP's many devices, including known vulnerabilities.

   An HCP may even want to track the levels of nested software included in a purchased device, to learn that there are vulnerabilities

2. Updating and Maintaining: The repository needs to support updating and maintaining SBOM content throughout the device's life cycle to ensure accurate/current information. To ensure manageability, automated processes are needed.

   As formats and software identifiers are likely to change over the lifetime of devices and repositories, a generic capability to map between a device identifier and some document of any format used to document information on SBOM is the most important feature of such an SBOM repository (Per ISO/IEC 19770-2:2015 a SWID tag is one means of tagging software)

3. Secure Repository: The SBOM repository should be secure (e.g., role-based restricted access for those in the healthcare organization that need it) to prevent the information from being modified by malicious individuals or used as a roadmap to attack a device or an HCP's network.

Note: Items a-f above are general SBOM considerations and were also discussed in Section 5 as these considerations also apply to MDMs.

6.1.2. Methods for Ingesting and Managing an SBOM

SBOM can be ingested manually or through an automated process. However, since manual processes can quickly become cumbersome, automated processes are recommended for HCPs of all sizes to reduce administrative burden. Automation also aids in the management of the SBOM going forward, as SBOMs may be updated over time. As a part of healthcare provider operations, organizations may leverage a security information and event management (SIEM) software solution that can, among other things, collect, store, aggregate, and analyse data from networked devices, servers, etc. These SIEMs may be used to ingest an SBOM if the SIEM can read the SBOM format.

To maintain use of the SBOM over time, some healthcare organizations are exploring linking or integrating the SBOM within their Vendor Risk Management (VRM) system via their Configuration Management Database (CMDB) or Computerized Maintenance Management System (CMMS). In some cases, HCPs are exploring direct ingestion of the SBOM to these technologies. Custom developed software tools or scripts may also be used to ingest an SBOM. For direct ingestion and/or with the use of custom tools, HCPs will need to consider the proprietary nature of the electronic format of their data management systems

While not an exhaustive list, the following table outlines some of the advantages and disadvantages to methods an HCP may use for ingesting and managing an SBOM.

Table 2: Advantages and Disadvantages of Certain Methods of SBOM Ingestion and Management

Method for Ingesting or Managing an SBOM	Advantages	Disadvantages
SIEM	• Capable of directly ingesting	• Compatibility with SBOM formats • Ability to use with proprietary SBOMs • Reduced access for searching
CMDB/CMMS	• Highly searchable • Capable of directly ingesting (Some vendors are engaged in the NTIA pilot – Nuvolo and ServiceNow) • Direct correlation to individual assets	• Compatibility with SBOM formats • Ability to use with proprietary SBOMs
VRM	• Searchable, capable of directly ingesting	• Compatibility with SBOM formats • Ability to use with proprietary SBOMs • Lacks link to individual assets
Custom Scripts	• Can be tailored to HCP's unique needs	• May be time consuming or resource intensive to generate • Higher incidence of errors

Additional details regarding specific use cases related to the management of an SBOM can be found in Section 7.0 SBOM use cases.

7. SBOM Use Cases

SBOMs have a broad range of uses by stakeholders. For example, from an HCP's device life cycle perspective, SBOMs help during deployment, integration, configuration, use, maintenance, and device configuration management (e.g., because an HCP may have multiple versions of the same device since the devices are not updated at the same time).

SBOMs may also be used by MDM throughout the TPLC of a medical device from the design stage through end of support and decommissioning. Holistically, SBOMs can be used by organizations to take a more proactive security stance across the entire life cycle of a device.

This section provides examples of use cases for an SBOM as an adjunct tool for:

- Risk management
- Vulnerability management
- Incident Management

The following sections provide a high-level overview of these use cases. While the sections that follow primarily focus on perspectives from the MDM or the HCP, some of these use cases may have applicability for other stakeholder groups.

Asset management and procurement use cases are not included in this document. For additional information on these use cases, please refer to the NTIA Software Component transparency Healthcare Proof of Concept Report.

7.1. Risk Management

7.1.1. MDM's Perspective

Typical risk management activities are described in Section 5.2 of the IMDRF cybersecurity guidance (IMDRF/CYBER WG/N60FINAL:2020). For SBOM generation, manufacturers need to consider the entire software supply chain. This includes software components incorporated into the device. The SBOM can assist in identifying existing vulnerabilities in these software components by using external vulnerability information sources. When vulnerable software components are discovered, it will initiate the risk analyses process which also considers software dependencies.

Dependencies can include such things as libraries, operating systems, Transmission Control Protocol/Internet Protocol (TCP/IP) stacks, and other components required to run software and system. Below is a list of some risk management activities that benefit from the use of an SBOM:

a. **Risk Evaluation:** An SBOM, in conjunction with external vulnerability information sources, can be used to identify potential vulnerabilities. SBOM provides information about potential vulnerabilities that may exist, including their potential exploitability and impact. This vulnerability information can be used to estimate and evaluate the level of risk associated with a particular vulnerability.

b. **Risk Control:** Monitoring and routinely verifying whether vulnerabilities for components listed in the SBOM exist helps to keep risks at an acceptable level (see also use case 7.2 vulnerability management).

c. **Assess and monitor:** Updating the SBOM as needed with new software releases

d. **Lifecycle risk management:** Provide an SBOM in a machine-readable format as part of product security documentation to HCPs at purchase and update throughout the device's life cycle (with an up-to-date SBOM being provided to facilitate healthcare provider management as the device approaches EOS). See IMDRF/CYBER WG/N70DRAFT:2022) for additional details.

7.1.2. HCP’s Perspective

SBOM’s are used as a part of HCP’s risk management starting at procurement. SBOM provides transparency for what is included in the device software and thus the risks that may be associated with it. This will enable the HCP to better understand the benefits and risks of a device as it progresses through its TPLC, and how to apply risk control measures and mitigation strategies more effectively across the device life cycle.

7.2. Vulnerability Management

This section of the document discusses use cases and considerations to make effective use of a SBOM for medical device vulnerability management.

7.2.1. MDM’s Perspective

Vulnerability management is a critical aspect of the MDM’s post-market approach to ensure their medical devices maintain an acceptable risk profile. As a part of cybersecurity, manufacturers monitor threat and vulnerability information sources. The SBOM is an essential resource to leverage in supporting the timely identification of potential medical device vulnerabilities as they emerge and change over time. Using the SBOM, MDMs can identify medical devices that may be impacted by a vulnerability based on the impacted software components from the associated vulnerability information. Automation of the comparison of medical device SBOM information to impacted software component information from reported vulnerabilities can further improve the timeliness and accuracy of vulnerability identification. This improves the manufacturer’s ability to perform their risk assessment, communicate and remediate as needed. One possible outcome of the risk assessment could be that a vulnerable component is exchanged, which eventually leads to a revised SBOM.

7.2.2. HCP’s Perspective

Vulnerability management is an important process to allow healthcare institutions to continuously detect, evaluate, and remediate the vulnerabilities in the IT environment. As new vulnerabilities are being discovered daily, it is a way to effectively detect and remediate critical vulnerabilities in a timely manner. This section will explore the various SBOM use cases to assist the HCP in their vulnerability management process.

While not exhaustive, below is a list of some vulnerability management activities that benefit from the use of an SBOM

a. **Monitoring of healthcare organization’s assets against new vulnerabilities as they emerge:** SBOM can be used along with vulnerability information to understand if and how their medical devices are impacted by a new vulnerability. VEX may be a complimentary communication mechanism for vulnerabilities.

b. **Driving interim mitigations:** SBOM information enables the HCP to carry out interim mitigations as needed while the MDM/ supplier is still assessing the exact impact or developing updates to remediate the vulnerability.

   - It is still recommended that the HCP engage with the MDM regarding the interim mitigation as they may have a better understanding of how the interim mitigation could impact the intended use of the device. A manufacturer may provide interim mitigation guidance using vulnerability exploitability exchange (VEX).

c. **Lifecycle management:** SBOM aids in the understanding of current supported and unsupported software for new devices and those already in the field. It is helpful for MDMs to include a timeline for support that gives HCP’s enough time to assess risk (both to their enterprise as well as to patients) if they are unable to replace a device.

d. **Assisting healthcare provider with proactive security activities:** SBOM supplements vulnerability identification and security scanning activities when scanning is not feasible or appropriate (e.g., for embedded devices, SaMDs)

7.3. Incident Management

There are numerous ways that an MDM or an HCP might become aware of security incident which may impact medical devices. Irrespective of how they become aware, the SBOM is one of several resources that can help MDMs and HCP better manage cybersecurity incidents in the five stages of incident management[1] when used in conjunction with a robust incident response process. For an MDM, an SBOM repository can reduce the time it takes to identify and evaluate at-risk devices. For an HCP, an SBOM repository can help first-level-support teams and cybersecurity teams actions. Specifically, the repository improves the systematic collection, correlation, and evaluation of information to detect cybersecurity-relevant events which ultimately improves incident-handling. Collectively, this improved response can reduce risks posed by incomplete risk evaluations and data loss that leads to destruction of evidence.

[1] According to ISO/IEC 27035 five phases are:

- Plan and prepare
- Detection and reporting
- Assessment and decision
- Responses
- Lessons learnt

8. References

8.1. IMDRF Documents

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

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

3. Principles and Practices for Medical Device Cybersecurity IMDRF/CYBER WG/N60: FINAL:2020 (April 2020)

4. Principles and Practices for the Cybersecurity of Legacy Medical Devices IMDRF/ CYBER WG/N70 FINAL:2023 (April 2023)

8.2. Standards

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

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

7. ANSI/NEM HN 1-2019, Manufacturer Disclosure Statement for Medical Device Security

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

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

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

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

12. IEC TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

13. IEC TR 80001-2-8:2016, Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2

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

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

16. ISO/TR 80001-2-7:2015, Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

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

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

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

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

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

22. ISO/IEC 5962:2021 Information technology — SPDX® Specification V2.2.1

23. ISO/IEC 19770-2:2015 Information technology — IT asset management — Part 2: Software identification tag

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

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

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

8.3. Regulatory Guidance and Draft Guidance

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

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

29. European Commission: REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (May 2017)

30. European Commission: REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (May 2017)

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

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

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

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

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

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

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

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

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

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

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

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

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

8.4. Other Resources and References

44. NTIA FAQ

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

45. NTIA "Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)" Second Edition

https://www.ntia.gov/files/ntia/publications/ntia_sbom_framing_2nd_edition_20211021.pdf

46. NTIA "Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)"

https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

47. NTIA "Roles and Benefits of SBOM Across the Supply Chain"
https://www.ntia.gov/files/ntia/publications/ntia_sbom_use_cases_roles_benefits-nov2019.pdf

48. NTIA Software Component Transparency Healthcare Proof of Concept Report
https://www.ntia.gov/files/ntia/publications/ntia_sbom_healthcare_poc_report_2019_1001.pdf

49. NTIA Healthcare POC "How to Guide for SBOM Generation"

https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf

50. NTIA Vulnerability-Exploitability eXchange (VEX) Overview

https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf

51. NTIA Software Suppliers Playbook: SBOM Production and Provision

https://ntia.gov/files/ntia/publications/software_suppliers_sbom_production_and_provision_-_final.pdf

52. Dept of Commerce, Minimum Elements for a SBOM Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

53. OASIS Profile 5: VEX

https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.html#45-profile-5-vex

54. CERT® Guide to Coordinated Vulnerability Disclosure

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

55. The NIST Cybersecurity Framework

https://www.nist.gov/cyberframework

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

https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

57. NIST SP 800-115:2008, Technical Guide to Information Security Testing and Assessment

https://doi.org/10.6028/NIST.SP.800-115

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

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

59. MITRE medical device cybersecurity playbook (October 2018)

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

60. MITRE CVSS Healthcare Rubric

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

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

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

62. Open Web Application Security Project (OWASP)

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

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

64. National Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group

https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

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

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

9. Appendices

9.1. SBOM Component Types and Tools

SBOM content can come from a variety of sources. Examples of component types that may be included and tooling that may be used to generate the SBOM content are provided below.

a. Third-Party Software Component Types

The scope of component types incorporated in the SBOM might depend on several factors including but not limited to: capabilities of the MDM, expectations of the HCPs, maturity of SBOM software available, and potential or expected regulatory SBOM requirements.

However, when managing the SBOM, awareness of the different types of components is important as components might need different methods and tools for inventory and operational management. The following types can be distinguished:

i. Third-party software libraries that are linked to or embedded in the proprietary medical device software.

ii. Virtual machine, operating system, and third-party software components that reside on the operating system such as drivers, database software, management tools, and application frameworks.

iii. Third-party software components that come with vendor supplied hardware in use on the medical device: firmware, embedded software and programmable logic controller (PLC).

The next sections will elaborate on the SBOM inventory, operational management, and available tools for these different types of components.

b. Third-Party Software Libraries

In modern software development, it is not unusual to use significantly more code from third-party libraries compared to proprietary lines of code written by the manufacturer itself in a single piece of software. Composing and managing the SBOM containing these libraries can be done by ensuring the MDMs track and compose a list of all the libraries and update such lists for every software change that impacts the libraries used. Such manual tracking and updating of SBOMs can be considered a first, basic procedure for incorporating SBOM usage into their development processes. As organizations mature, they may begin adapting more advanced procedures like automation to make the process more efficient and accurate. An example of a more advanced procedure would be the leveraging of existing development platforms and the development and operations (DevOps) environments. Specifically, automated tools/plugins could be incorporated in one or more phases of the development pipeline (DevSecOps).

The advantage of SBOM is that it enables the identification of third-party libraries and known vulnerabilities in those libraries as early as possible. Early detection of any known vulnerabilities facilitates early remediation and will be more cost effective compared to late detection. Early replacement in the development process of a vulnerable component for a non-vulnerable component decreases costs because the procedural workload in early stages of a software development is far less than for example after the verification and validation phase. Coding rework will also be less extensive as code complexity and dependencies will increase as the code reaches final stages of the SDLC. In addition, early detection enables SBOM management throughout the SDLC, in general whenever changes to the software will alter the software composition of the SBOM.

Such tools or plugins analyze the software to detect embedded or linked open-source software, and some can detect commercial third-party software as well. They typically identify known vulnerabilities, such as out-of-date libraries that have available security patches. Monitoring for vulnerabilities feeds into SBOM content collection during:

i. **Coding**: for example, when executing Static Code Analyses (i.e., leveraging tools that attempt to highlight vulnerabilities in non-running source code).

ii. **Building**: for example, when the software is built for each end of sprint, where a sprint is a set time period by which specific work has to be completed and made ready for review.

iii. **Testing**: for example, when executing Static Application Security Testing (SAST).

These tools or plugins – usually referred to as Software Composition Analyses (SCA) software – do not need any manual input to generate the SBOM but will use available repositories to in general identify:

i. Software component name
ii. Software component vendor (supplier)
iii. Software component version
iv. Component hash
v. Relationship (One or more layers of dependencies)
vi. Component vulnerabilities
vii. Licensing model and compliance information

Note that apart from the larger SCA vendors, there are other tools and plugins available which can be used during code-build-test and produce similar outcomes. While some are free to use, making automation available to medical device manufacturers of every size, MDMs should be careful to select tools with capabilities that best suit the MDM's needs.

c. Operating System Components

Virtual machine(s) and the operating system in use by the medical device are essential components of the SBOM. There are existing third-party software components that rely upon the operating system on top of which the device software is built, including database software and application frameworks, as well as software components for other essential functions of the device such as security software, system management tools, remote support software, and networking components.

Several options exist to automate the discovery and management of third-party software components on the operating system. Some SCA vendors focus on both the components discussed in the previous section, as well as the other software components on the operating system that are not directly linked to or embedded in the proprietary software. But there are also vendors with a dedicated focus on Software Asset Management (SAM), a governance practice that manages the risks and value inherent in software.

If such tools are not an option for the medical device manufacturer, the software inventory on the operating system can be generated by executing purpose-built scripts (for example a PowerShell Script on Windows or Bash Script on Linux). Another option is to use a vulnerability management scanning tool. The advantage of the latter that it will also provide vulnerability information of the components discovered.

d. Firmware, Embedded Software and PLC

Third-party firmware, embedded software, and PLC are the components that are least prone to change on a medical device during its life cycle, unless vulnerabilities are discovered. Embedded software is built from board support packages, binary drivers, Software Development Kits (SDK), CPU microcodes, and other libraries. This may include a large dependency on open-source software. It is important to identify all software components included in the end-product.

As these types of software components are tied to the hardware of the device, they are part of the regular BOM for a medical device. A BOM is a comprehensive list of the materials and components needed to manufacture a device and thus includes much more than just software components. Hence, the BOM provides a good starting point for the inventory and management of these third-part software components. Like the SBOM, a regular BOM may be obtained from various sources, including an MDM's development activity or via third-party provided BOMs. A combination of source code management systems and binary software composition analysis can be used to automate or verify the generation of this information. It should be noted that any tools used should be compatible with the embedded system.

If the BOM is managed through Product Lifecycle Management (PLM) or Enterprise Resource Planning (ERP) software, export functions can be used to extract the software components. If available, the upstream SBOM of the firmware, software, or PLC vendor can be leveraged to add additional layers of depth for third-party components if that is required.

If these software components are proprietary, e.g., developed by the medical device manufacturer, the same approach applies as described in 'Third-Party Software Libraries' in Section 9.1.