IMDRF International Medical Device Regulators Forum

DRAFT DOCUMENT

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

Authoring Group: Medical Device Cybersecurity Working Group

Date: June 2022

Table of Contents

Preface

The document herein was produced by the International Medical Device Regulators Forum (IMDRF), a voluntary group of medical device regulators from around the world. The document has been subject to consultation throughout its development.

1.0 Introduction

Digital connectivity of medical devices has made patient care more efficient, data-driven, and effective. Utilization and reliance on third-party software components has made developing such medical devices more economical, more reliable, and increased the pace of innovation. However, while connectivity and utilization of third-party software components deliver 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. Increased information in communications from medical device manufacturers (MDMs) and regulators that identify third-party component vulnerabilities demonstrate these potential risks.

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 the generally low traceability of those common components within devices. To address this issue, the US National Telecommunications and Information Administration (NTIA) convened a multi-sector initiative of various stakeholders in 2018 to discuss software transparency. One of the outputs was the concept of a software bill of materials (SBOM), which NTIA defined as a list of one or more identified components and other associated information. SBOM may be leveraged across the total product life cycle (TPLC) in both premarket and post-market activities.

The benefits of an SBOM across the TPLC include (but are not limited to):

- an improved ability to identify software components contained in a device,
- more secure software development,
- increased software transparency among vendors, and
- better identification of suspicious software components.

Additional insights regarding SBOM benefits are found in NTIA's FAQ document and their "Roles and Benefits of SBOM Across the Supply Chain" document. To fully realize its benefits, the SBOM needs to be widely adopted by all stakeholders, while also recognizing that each stakeholder may have different roles and uses of SBOM, such as SBOM generation, management, distribution, ingestion, and utilization.

Building on the SBOM concept, Principles and Practices for Medical Device Cybersecurity (IMDRF/CYBER WG/N60FINAL:2020) included an SBOM as part of the customer security documentation to be prepared by the MDM and provided to the device user. Among a variety of benefits, using an SBOM for medical devices across the TPLC enables:

- Better management of End of Life of software components. If the MDMs know the software components and their respective end of life dates, it will allow them to be proactive and find alternative components or solutions. This is of benefit to device users since the cybersecurity of the medical device is increased as a result.
- Better pre-purchase and pre-installation planning- because having the SBOM allows healthcare providers to know which devices are potentially vulnerable or contain soon to be out of date software before purchasing. They can better assess if the benefits of getting the device will outweigh the security risks that come along with it.
  Regulators to have a better understanding of the product as a part of the benefit risk assessment undertaken in premarket reviews and informs their initial post-market

vulnerability impact assessments. This enhanced understanding provides insight into the number and types of products that may be impacted which can help to inform next steps.

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. For the purpose of this guidance, healthcare providers include healthcare delivery organizations.

2.0 Scope

This document is designed to provide recommendations applicable to responsible stakeholders including, but not limited to, MDMs, HCPs, users, regulators, and software vendors on the implementation of an SBOM and increased transparency in the use of software in medical devices, including in vitro diagnostic (IVD) medical devices. However, the document emphasizes the roles and responsibilities of MDMs and HCPs. This document is complementary to the preceding IMDRF cybersecurity guidance (IMDRF/CYBER WG/N60FINAL:2020), and the scope of relevant medical devices, as well as the focus on potential for patient harm remain unchanged.

Specifically, 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)). It is important to note that due to most regulators' authority over medical device safety and performance, the scope of this guidance is limited to consideration of the potential for patient harm related to the regulated medical device. For example, threats that could impact performance, negatively affect clinical operations, or result in diagnostic or therapeutic errors are considered in scope of this document. While other types of harm such as those associated with breaches of data privacy are important, they are not considered within the scope of this document.

This document also does not address cloud services. Cloud services that are a component of the regulated medical device may also present a risk to safety and effectiveness, especially availability. 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 document 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 are considered in future work.

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; and
- Demonstrate SBOM use cases for risk management, vulnerability management, and incident response from the perspective of medical device manufacturers and healthcare providers.

As was emphasized in the preceding IMDRF medical device cybersecurity guidance (IMDRF/CYBER WG/N60FINAL:2020), 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 focus on the cybersecurity concerns relevant to SBOM.

It is important to note that differences across medical device types and regulatory jurisdictions, may give rise to specific circumstances where different or additional considerations are required.

3.0 Definitions

For the purposes of this document, the terms and definitions given in IMDRF/GRRP WG/N47 FINAL:2018 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, labeling, or assembly that is intended to be included as part of the finished, packaged, and labeled device

3.9 *Credentialed scan:* a vulnerability scan performed with system credentials (e.g., username and password) to access the system and bypass certain security layers to collect more detailed system information.

Note: Per NIST SP-800-115, a vulnerability scan is a technique used to identify hosts/host attributes and associated vulnerabilities.

3.10 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)

3.11 Legacy Medical Device (syn. Legacy Device): Medical device that cannot be reasonably protected against current cybersecurity threats

3.12 *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)

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

3.14 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 and other associated information.

NOTE: The SBOM for a single component with no dependencies is just the list of that one component. “Software” can be interpreted as “software system,” thus hardware (true hardware, not firmware) and very low-level software (like CPU microcode) can be included. The primary focus of this effort is software components; however, hardware is not excluded. (NTIA Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM) 2019-11-12)

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

3.19 *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 1 to entry: Parties involved are usually supplier ("first party") and purchaser ("second party") interests.

3.20 *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)

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

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

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

4.0 Overview of SBOM Framework

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.

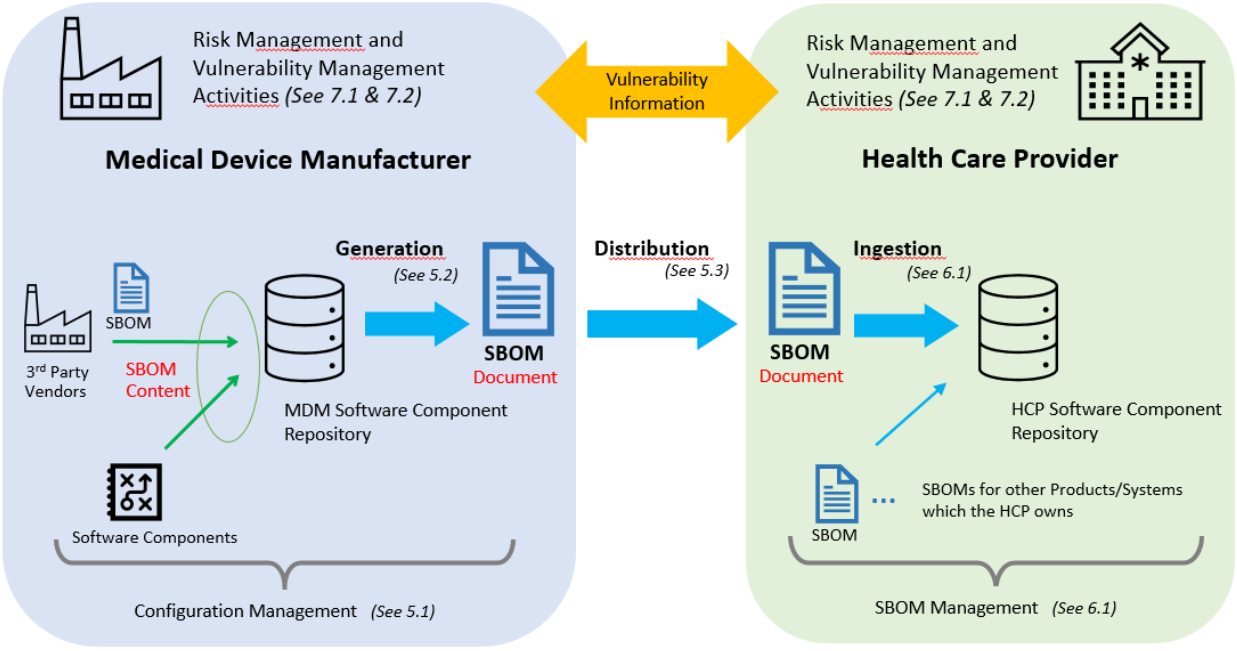

Figure 1 – Overall framework for SBOM

At a high level, SBOM content is collected by the MDM and is housed in a software component repository. The SBOM document is then 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.

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

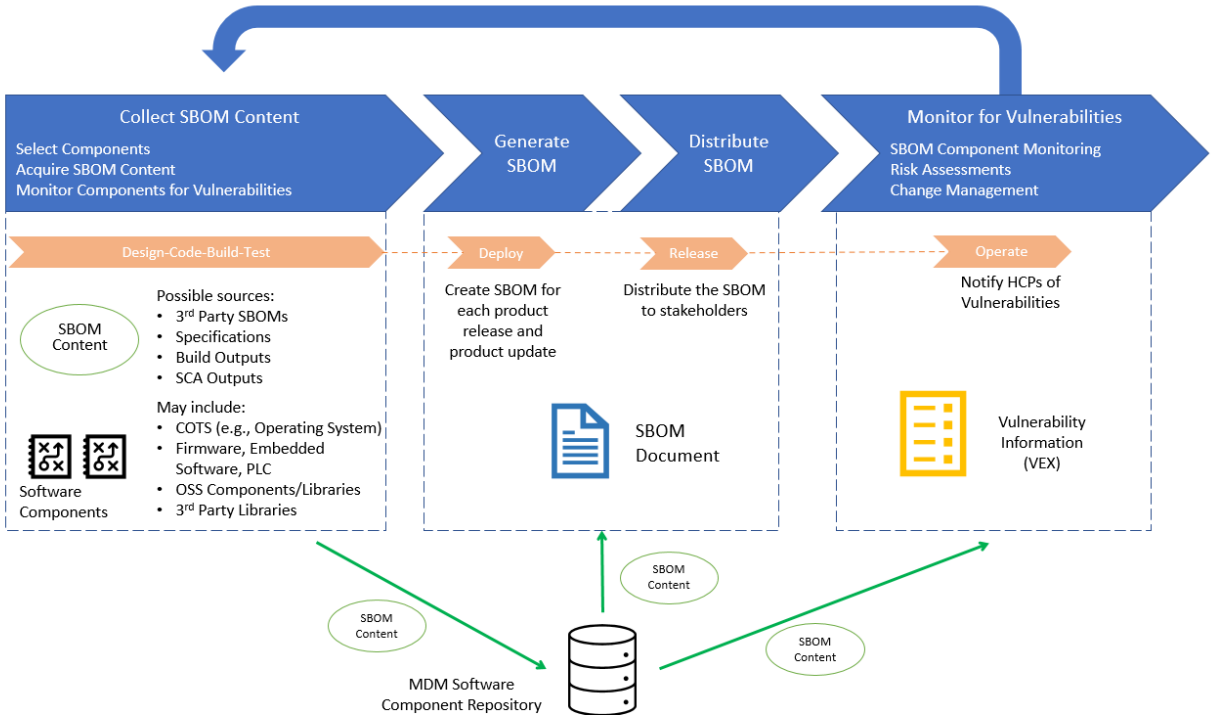

Figure 2: SBOM management across the software development life cycle (SDLC)

5.1 Collect SBOM Content

The design phase in the SDLC begins the collection of SBOM content. The content for generating an SBOM can come from a variety of sources. For example, SBOM content can be collected from the MDM's own development activity, via third-party provided SBOM or by software composition analysis (SCA) outputs. In addition, open-source software (OSS) may include a README that provides some, though perhaps not all, SBOM content. Within development activities, content may be collected from specifications (e.g., in design or version description documents) and build outputs (e.g., scripts). SCA tools may be used to scan the software to identify the included components, however it is important to keep in mind that the proprietary databases and code fingerprints which the tools rely upon may be incomplete or out of date.

SBOM content needs to be collected for the medical device platform (unless a software-only product) and the medical device application. This usually requires different sources and tooling. For example, a 3rd party commercial off the shelf (COTS) software would typically be found on the platform and specifications may be used to identify these. Upstream component vendors for components like firmware, embedded software, and program logic controllers (PLCs) can provide third-party SBOMs which the MDM can incorporate into their final finished devices. The MDM SBOM content repository is used to aggregate the collection of SBOM content. Additional details regarding the component types that may be included in the MDM SBOM content repository and tooling used to collect this content is found in Appendix 9.1.

5.2 Generate an SBOM

An SBOM is generated to assist MDM and HCP management of medical device cybersecurity, which may be influenced by the security of its software components. To generate the SBOM, the applicable SBOM content that was collected during design-code-build-test in the MDM SBOM content repository, is aggregated into an SBOM document for each product release and product update. Thus, the SBOM is updated and maintained throughout the life cycle of the device.

The final SBOM document that is distributed to SBOM stakeholders should follow a defined and established SBOM generation methodology to ensure consistent output. The following section will also describe 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 & Formats

The amount and type of information include in an SBOM may vary but in general SBOMs should be as complete as possible to enable stakeholders to manage risks more quickly, and effectively. For medical device cybersecurity, a baseline SBOM should include the following, NTIA consistent elements:

- Author name: author of the SBOM entry
- 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 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
- Component hash: Precise way to identify as-built component of SBOM
- Unique Identifier: Identifiers that are used to identify a component, or serve as a look-up key for relevant databases
- Relationship: Characterizing 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 at a deeper level, as needed. For example, considerations relevant to the life cycle of a device (e.g., a software component's end-of-support (EOS) date), would be of value 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 a limited number of standard, automated SBOM formats (Cyclone DX, SPDX, and 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

After SBOM generation, the must consider how best to advertise that it exists and how best to allow access to it. SBOMs should be initially provided to HCPs as part of the procurement process. The distribution of an SBOM is the process for how the SBOM information is exchanged from the manufacturer to the user. 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. 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 allow the SBOM to be distributed to or accessed by the HCP. As stated previously, there is no one way to best distribute an SBOM at this time, but 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, where a repository is 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 3rd 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 some considerations for some of the SBOM distribution categories descried above:

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 •
Accessible from an API on the medical device	• More control over SBOM access	• API standards remain undefined • Requires tooling

Method of Distribution	Advantages	Disadvantages
	• Can be used in an automated process	• 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 3rd 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

Table 1: Advantages and Disadvantages of Certain Methods of 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 keep the user's asset management system current by requiring a trigger to update it with the most up-to-date SBOM. In particular, a new SBOM shouldn't overwrite an old SBOM until all devices are updated, otherwise vulnerable software can be masked.

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 need to maintain internal security policies and practices to protect SBOM integrity, authenticity, and confidentiality

5.4 Monitor for Vulnerabilities

An SBOM does not contain vulnerability information. However, the SBOM may be used in conjunction with other resources (e.g., VEX) to monitor for medical device vulnerabilities. During the life cycle of the medical device, both the author (MDM) and the recipient (HCP) of the SBOM rely on accurate and up-to-date information about the third-party software components to identify and mitigate potential patient safety risks associated with possible third-party software vulnerabilities on the device or systems in which the devices operate.

Having up to date information on third-party components implies that MDMs have the capabilities to compose the third-party component list as part of pre-market activities and during post-market changes to the device and /or its software. This can be a challenging task and requires adequate internal processes and tools to be in place.

Leveraging existing change management controls (i.e., process used to identify, document, and authorize changes to an IT environment), is the first step in ensuring that any changes to the SBOM are captured and the appropriate follow-up actions are taken. Vulnerability monitoring can trigger change control to relevant software components and if software component selection is affected, then your medical device SBOM content can change. However, new vulnerability information does not always result in a software change and thus vulnerability information changes more frequently than the medical device software component information. Ultimately changes in SBOM content, result in an updated SBOM document that is generated and distributed when a medical device is updated.

5.4.1 SBOM & Change Management

While the Software Development Life Cycle (SDLC) has been well incorporated into the pre- and post-market change management processes of medical device development, third-party component change management is a new area for most manufacturers. Change control can be triggered through several events. Examples include but are not limited to:

- discovery of a vulnerability in a third-party component,
- changes during the medical device life cycle due to patching software bugs,
- addition of new functions to the medical device software,
- changes to third-party components that reside on the device hardware or within its operating system due to end of life (EOL) decisions, (security) patches, or new versions coming to the market.

In all scenarios, the software composition will change. For example, components might be exchanged for others, components may be added or removed, or new versions of components will become part of the composition.

Change control should not only apply to the overall SBOM itself, but also to the proprietary medical device software using third-party software libraries. For example, if a security fix has been implemented in the proprietary code to mitigate a potential vulnerability in a third-party software library, this should be tracked appropriately. This information is not only important for internal use, but also for informing 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. This section highlights some of the challenges in implementing SBOM across the SDLC.

a. **Legacy devices:** SBOM is a relatively recent concept and in generating an SBOM for legacy medical devices, an MDM may face difficulties obtaining granularity as even basic information may not be available for some elements. In this instance it is still desirable to build an SBOM which may be of reduced scope and depth, that captures major software components such as the Operating System, COTS software, and OSS as possible. Doing so allows this simple nucleus of the SBOM to be extended and improved for the next version of the device.
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
    i. Standards and tools continue to evolve and mature; MDMs should not wait for these to be "finalized"; rather they should generate initial SBOM documents 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)).
    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 SBOM documents are created for each product release or update. Defining the right depth of SBOM content to be included in the SBOM document will impact the quantity and type of resources needed to keep an SBOM document up to date.

6.0 Overview of Healthcare Provider Considerations

Healthcare has evolved over the last decade into a digital environment that permeates every facet of the industry. This digital transformation, which involves both business aspects and most critically patient care, has produced a dependence on secure software. This has coincided with a dramatic rise in cybersecurity breaches. Manufacturers should supply a software bill of materials (SBOM) with their products. The SBOM content needs to address many of the varied needs, resources, and capabilities of HCPs. The HCPs population is best described as a diverse – with large health systems, small rural facilities, and an increasingly important ambulatory component, including home care, that is now also digitally dependent and connected. SBOMs are applicable in these different use environments and advancements in tooling, services, and cybersecurity maturity will enable HCPs to leverage the SBOM to its fullest extent. Protection of the cyber healthcare environment is a shared responsibility of HCPs and MDMs with the SBOM being a common tool to support safety.

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

To be able to leverage an SBOM, organizations must first be able to ingest it. A complete and accurate asset inventory is critical. Once ingested, an SBOM is 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 an SBOM

An HCP needs to understand the hardware assets and the associated software running on its network. Establishing an inventory of off-the shelf or custom developed applications is typically handled through standard information technology processes. Establishing an inventory of software running on devices cannot be handled through these standard processes and requires input from the MDM. An SBOM is a method to transparently share this information between MDM and HCPs. Below are considerations related to an SBOM and a healthcare provider-managed SBOM repository.

A. A key time to obtain SBOM information is during the ***procurement*** process, this aligns with the timing of device information being shared between an MDM and HCP.

B. Delivery of the SBOM should be done through a ***standard, automated format*** to enable information to be efficiently ingested by an HCP. Three prominent formats to be considered are Cyclone Dx, SPDX, and SWID.

C. 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. However, the lack of standardized unique identifier for software and hardware components may result in manual mapping.

D. The level of SBOM completeness affects the extent to which it can be leveraged. At a minimum, SBOM component information should include: author name, timestamp, software component vendor (supplier), software component name, software component version, component hash, unique identifier, and relationship.

E. ***Communication*** between an MDM and HCP is highly recommended when an SBOM indicates a device has a known vulnerability, to ensure actions taken to address the vulnerability are validated by the MDM and if required, approved by the HCP's national/regional authority.

F. HCPs need the ability to create an internal SBOM repository, linking each device in their environment to the specific SBOM for ***enhanced enterprise device management***.

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

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

2. The repository needs to support *updating and maintaining* SBOM content throughout the device's life cycle to ensure accurate/current information.

    a. 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 SWID is one means of tagging software)

3. 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 used as a roadmap to attack a device or an HCP's network.

Note: Items A-E 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

With the scale and scope of devices in an HCP's environment, to be practically useful, an SBOM needs to be ingested in an automated way. Automation also aids in the management of the SBOM going forward as SBOMs may be updated over time. As a part of hospital operations, organizations may leverage a security information and event management (SIEM) software solution that can, among other things, collect, store, aggregate, and analyze 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 (e.g., whether they have the needed permissions to integrate the SBOMs into their systems).

While not an exhaustive list, the following table outlines some of the methods an HCP may use for ingesting and managing an SBOM and some corresponding considerations for each (i.e., advantages and disadvantages).

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	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 your unique needs	• May be time consuming or resource intensive to generate • Higher incidence of errors

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

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

7.0 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 a HCP may have multiple versions of the same device since the devices are not updated at the same time). 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.

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 organisations to take a more proactive security stance across the entire life cycle of a device.

This section provides some example use cases for an SBOM as an adjunct tool for:

- Risk management
- Vulnerability management
- Incident Management

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. Moreover, the forthcoming sections provide a high-level overview of these use cases.

7.1 Risk Management

7.1.1 Manufacturer's Perspective

Manufacturers need to consider the entire software supply chain when generating their SBOMs for risk-management purposes; this includes software and software dependencies that are developed internally or externally and included in the device.

Dependencies can include such things as libraries, operating systems, TCP/IP stacks, compilers, among other things. While not exhaustive, below is a list of some risk management activities that benefit from the use of an SBOM

A. **Hazard Analysis:** SBOM used to identify potential cyber security vulnerabilities associated with known software components.
B. **Risk Evaluation:** SBOM provides information about potential vulnerabilities that may exist, including their potential exploitability and impact. This can be used to estimate and evaluate the level of risk associated with a particular vulnerability
C. **Risk Control:** Monitoring and routinely updating an SBOM with known vulnerabilities helps to keep risks at an acceptable level (see also use case 7.2 vulnerability management).
D. **Assess and monitor:** Updating the SBOM as needed with new software releases (for example after identifying ineffective risk controls or to further reduce residual risks)
E. **Lifecycle risk management:** Provide an SBOM 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 Healthcare Provider's Perspective

SBOM's are used as a part of HCP's risk management starting at pre-procurement. Healthcare providers should request an SBOM from manufacturers for any devices that are integrated into their network infrastructure. SBOM provides greater transparency regarding what's 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. Though a regulator may use an SBOM to informs their initial post-market vulnerability impact assessment, this section focuses on the use of SBOM for this purpose from an MDM and HCP perspective.

7.2.1 Manufacturer's Perspective

Vulnerability management is 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 tool in supporting the timely identification of potential medical device vulnerabilities as they emerge and change over time. Using the SBOM, MDMs can more efficiently 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 enables the manufacturer to perform their risk assessment, communicate and remediate as needed. Complementary to the SBOM, a VEX[1,2] may be used to communicate to users additional information about device impacts and what actions (if any) they should take. 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 Healthcare Provider'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 the only 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 used to understand if and how their medical devices are impacted by a new vulnerability
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
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

[1] https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf
[2] https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.html#45-profile-5-vex

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 a 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[3] 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.

8.0 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:DRAFT:2022 (May 2022)

8.2 Standards

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

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

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

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

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

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

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

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

11. 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

12. 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

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

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

15. 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

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

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

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

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

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

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

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

23. 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

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

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

26. 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)

27. 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)

28. FDA (Draft): Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (April 2022)

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

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

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

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

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

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

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

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

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

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

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

8.4 Other Resources and References

40. NTIA FAQ
(https://www.ntia.gov/files/ntia/publications/sbom_faq_-_20201116.pdf)

41. 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)

42. NTIA Healthcare POC "How to Guide for SBOM Generation"
https://www.ntia.gov/files/ntia/publications/howto_guide_for_sbom_generation_v1.pdf

43. NTIA Vulnerability-Exploitability eXchange (VEX) Overview
https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf

44. 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

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

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

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

48. 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

49. NIST SP 800-115:2008, Technical Guide to Information Security Testing and Assessment
https://doi.org/10.6028/NIST.SP.800-115

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

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

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

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

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

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

56. National Telecommunications and Information Administration (NTIA) / US Department of Commerce, Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group
https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

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

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

9.0 Appendices

9.1 SBOM Component Types & 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 written 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 (SecDevOps).

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. **the software build**: 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. Some are free to use, making automation available to medical device manufacturers of every size.

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.

The number of components for virtual machines and the operating system will probably be less than the third-party software libraries discussed in the previous section, nonetheless automated discovery and management will be a prerequisite for efficient and cost-effective inventory.

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 components least prone to change on a medical device during its life cycle, unless known vulnerabilities are discovered. 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.

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 the section on 'Third-Party Software Libraries'.