Healthcare Proof of Concept Use Case Definitions

Objective: Determine what is meant by/what activities we want to take place under the healthcare delivery organization's procurement and operational use cases that have been put forward for consideration (asset management, vulnerability management, and risk management) in the healthcare proof of concept

General:

Activities SBOM is expected to enable*:

Provide relevant data elements to be used internally by the receiving organization to be used for the subsequent use cases

*Please note that throughout the document the activities SBOM is expected to enable are focused on those that occur after the SBOM has been transferred from the medical device manufacturer to the healthcare delivery organization (HDO)

Procurement Use Case:

Definition –

- **Procurement**: Procurement is a vital element of equitable access to health care. It can be defined as "the acquisition of property, equipment, goods, works or services through purchase, hire, lease, rental or exchange" and is taken to include "all actions from planning and forecasting, identification of needs, sourcing and solicitation of offers, evaluation of offers, review and award of contracts, contracting and all phases of contract administration until delivery of the goods, the end of a contract, or the useful life of an asset." It is inclusive of vendor selection

Procurement activities SBOM is expected to enable:

- A reduction of the number of questionnaires that have to be filled out as the SBOM can supplement the MDS2
- Awareness regarding the presence of interfaced or system conflicts with the health IT system, etc.
- Awareness regarding the introduction of customized software into the IT system
- Clarity regarding end of life for software components in the device (e.g. device has windows 7 which is known to end of life in XX time, allows for questions at time of procurement regarding transition schedule, security coverage for devices that have components that will be end of life (e.g. Do you have a plan for covering security?), etc.)
- Informs asset management via identification of potential cybersecurity concerns

- Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field
    - Identifies unsupported or vulnerable software so HDOs can initiate alternative mitigations or controls

Asset Management Use Case:

Definition –

- **Asset Management:** Provides principles, practices and techniques designed to assist users and managers in managing medical equipment assets. Asset management includes a list of all the devices and device components. It aims to ensure equipment meets clinical requirements, is effectively maintained, is replaced when and only when it needs to be, that equipment is decommissioned in a controlled manner, and that additional equipment is acquired when needed. All this is accomplished in a constrained environment for both capital and operating costs. The management of medical equipment is one of the main risk-critical issues to keep health services functioning because the unavailability of equipment or failure of equipment presents risks to patients, staff and service delivery.

Asset management activities SBOM is expected to enable:

- Assisting HDOs in standardizing risk assessment for asset management
- Reduction of the number of questionnaires that have to be filled out as the SBOM can supplement the MDS2
- Asset inventory when SBOM changes/updates are communicated to HDOs
- Awareness regarding the presence of interfaced or system conflicts with the health IT system, etc.
- Awareness regarding the introduction of customized software into the IT system
- Actions that can be taken to protect the asset by providing sufficient details for each component
- Providing insight into end of life and aid in end of life planning for software and devices

- Risk Management Use Case:
    - Definition –

        - **Risk**: Risk combination of the probability of occurrence of harm and the severity of that harm Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation and the possibility to avoid or limit the harm. [SOURCE: ISO/IEC Guide 51:2014, 3.9, modified — Note 1 to entry updated to remove the reference to hazardous event.]
        - **Hazard**: Potential source of harm [SOURCE: IEC Guide 51:2014

        - **Harm**: injury or damage to the health of people, or damage to property or the environment [SOURCE: IEC Guide 51:2014, 3.1]
        - **Risk management**: Risk management is an integral part of the medical device product development lifecycle. It is a systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk [SOURCE: ISO/IEC Guide 63, 20XX, 2.15] In other words, the main purpose of the risk management cycle is to reduce or mitigate the chances of failure in the product and enable the product to fail with minimal impact. Risk management helps identify interim measures until a permanent solution can be identified (e.g. things that can be done during an incident response (like unplug the device))

            - Risk Analysis: Systematic use of available information to identify hazards and to estimate the risk [SOURCE: ISO/IEC Guide 51:2014, 3.10]
            - Risk Evaluation: Process of comparing the estimated risk against given risk criteria to determine the acceptability of the risk [SOURCE: ISO/IEC Guide 63, 20XX, 2.14]
            - Risk Control: Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels [SOURCE: ISO/IEC Guide 63, 20XX, 2.12]

    - Risk management activities SBOM is expected to enable:
        - Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field
            - Identifies unsupported or vulnerable software so HDOs can initiate alternative mitigations or controls
        - Monitoring of HDO inventory against new vulnerabilities as they emerge
        - Assessment of a new product being added to the hospital network prior to integration (want to know how risky device is before adding to the network)
        - Assessment of the level of risk associated with a particular vulnerability (SBOM allows you to get to the point of looking at what vulnerabilities still exist on a product and then can go look up CVE, etc. to enable risk assessment)

- Vulnerability Management Use Case
    - Definition –

        - **Vulnerability management**: Vulnerability management is a pro-active approach to managing network security through reducing the likelihood that flaws in code or design compromise the security of an endpoint or network. Vulnerability management can also be used reactively during incident response. Actions include Identifying, Verifying, Mitigating and Patching vulnerabilities.

- Activities SBOM is expected to enable:
    - Monitoring of HDO inventory against new vulnerabilities as they emerge
    - Assessment of a new product being added to the hospital network prior to integration (want to know how risky device is before adding to the network)
    - Assessment of the level of risk associated with a particular vulnerability (SBOM allows you to get to the point of looking at what vulnerabilities still exist on product and then can go look up CVE, etc. to enable risk assessment)
    - Lifecycle management (understanding of current supported and unsupported software) for new devices and those already in the field
        - Identifying unsupported software so you can initiate alternative mitigations or controls
    - Assisting HDOs with proactive security activities such as supplemental network scanning and supplemental organizational penetration testing