# Software Component Transparency

February 20, 2019


# Healthcare Proof of Concept

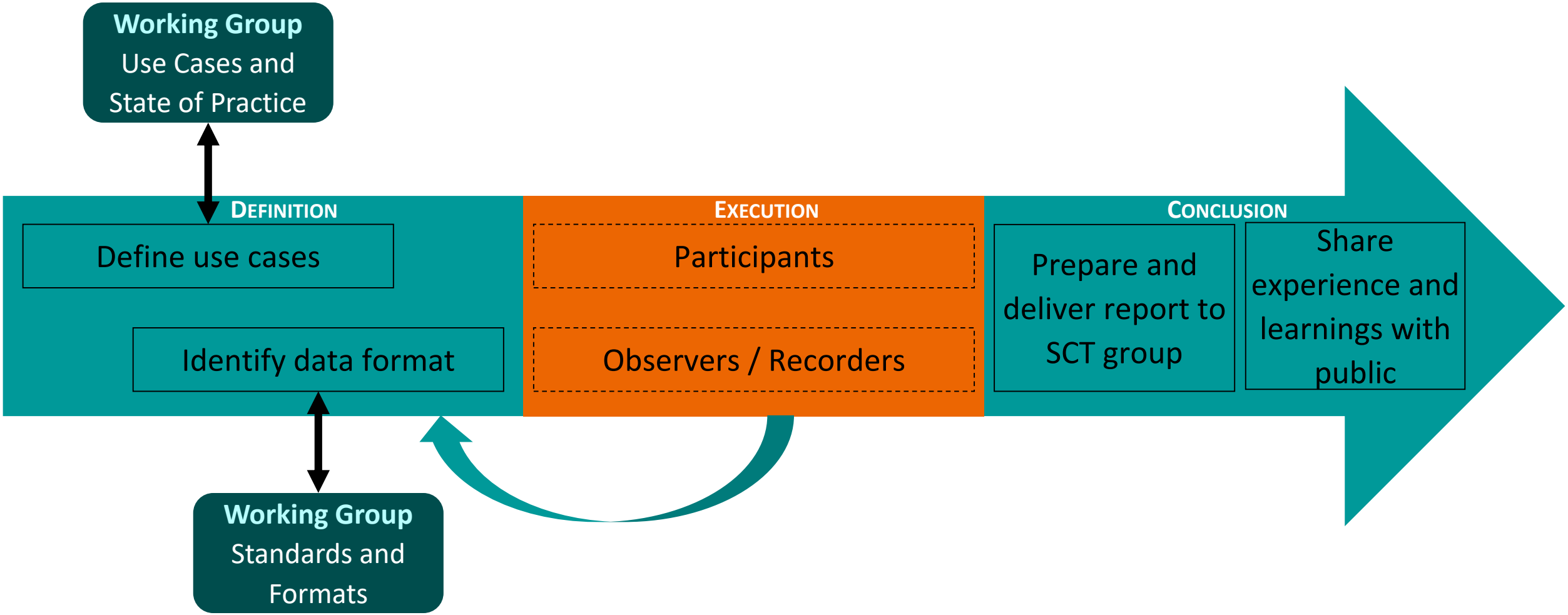
# 2019-02-20

# Objective

This is a collaborative effort between healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) to employ a provisional software bill of materials (SBOM) and exercise use cases for SBOM production and consumption.

The goal is to demonstrate successful use of SBOMs and relate to the overall cross-sector effort to establish standardized formats and processes.

# Overview


Working Group
Use Cases and
State of Practice
DEFINITION
Define use cases
Identify data format
Working Group
Standards and
Formats
EXECUTION
Participants
Observers / Recorders
CONCLUSION
Prepare and deliver report to SCT group
Share experience and learnings with public

# Currently Defined Details

## Use Cases

- Procurement
- Asset Management
  - Risk Management
  - Vulnerability Management

This is a very high level description. These use cases have been elaborated by a sub-group defining/detailing use cases and personas.

## Participants

- Healthcare Delivery Organizations
  - New York Presbyterian
  - Cedars-Sinai
  - Christiana Health
  - Mayo
  - Mass General
- Medical Device Manufacturers
  - Abbott
  - Bayer
  - Philips
  - Siemens

# Scope

| Item | In | Out | Comment |
|---|---|---|---|
| CBOM vs. SBOM (inclusion of hardware components) | | X | Minimum viable product, version 1, no clear line, let it be defined further outside the POC. Don't lose track of the issue. Parking lot. |
| Identifying a standard as the only acceptable format (canonization) | | X | No endorsement |
| Conforming to a standard (as opposed to defining a bespoke format) | X | | SWID and SPDX will both be used, but still not an endorsement |
| Inclusion of vulnerability information (front-end correlation) | | X | Gets stale, initiates long conversation, may need its own working group, could interfere with the execution of the POC, let's get the 1.0 version right and continue the conversation |
| Dependencies – level 1 | X | | Best effort/optional*, may not contribute to POC |
| Dependencies – level n | X | | Best effort/optional*, may not contribute to POC, can explode complexity |
| Globally unique & immutable component identifiers (one and only one) | | X | Not in version 1.0, hard problem |
| Vendor name | X | | |
| Version down to build number (as far as provided) | X | | |
| Context ("yeah it's in here, but don't worry about it because…") | ~~X~~ | X | May not avoid further questions, worth a try to determine benefit<br>Originally in scope, changed because of complexity |
| Delivery over the Internet (pull) | X | | Subscribe to information, manufacturers will not have the option to do so from their suppliers, at least for the POC |
| API for data access | X | | Could be a reference architecture/model for adoption |
| Machine readable format | X | | |

*Although not required for exercising the proof of concept, the final report should emphasize the importance of dependencies in the successful use of SBOMs.

# Use Case Details: Procurement

- SBOM is expected to enable HDO procurement activities such as:
  - 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
  - Identifying MDMs that incorporate security into their SDLC
  - Informs asset management via identification of potential cybersecurity concerns
  - Lifecycle management for new devices and those already in the field
    - Identifies unsupported or vulnerable software so HDOs can initiate alternative mitigations or controls

# Use Case Details: Asset Management

- SBOM is expected to enable HDO asset management use cases such as:
  - Assisting HDOs in standardizing risk assessment for asset management
  - 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

# Use Case Details: Vulnerability and Risk Management



- Lifecycle management 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 HDO can go look up CVE, etc. to enable risk assessment)

# What's New & Next Steps

- What's new since November update
  - Finalized use cases
  - Selected provisional SBOM data format
  - Completed HDO inventories
  - Finalized PoC roles and responsibilities

- Next steps
  - Finalizing sharing agreement
  - Identifying the products of which manufacturers will provide SBOMs
  - Deciding which SBOM use cases will be executed by which HDOs
  - HDOs - evaluation criteria for use cases
  - Standardizing a data collection format
  - Preparing the final report

# Potential Concerns

- The POC may be well advanced before consensus is reached and work finalized by the other directly related working groups, especially “Standards and Formats.” The intent of the POC is not to choose winners, but to find a workable path to confirming the utility of medical device SBOMs to HDOs. Still, whatever format chosen could lend weight to that format.

- Participants may expect some degree of confidentiality concerning details of the exercise which would need to be respected amongst members of the working group and resolved prior to creating a public report.

- This should be seen as just an exercise and not interfere with ongoing business relationships (e.g., no interaction with actual procurement or service activities).

# Questions????