



2.0

Healthcare SBOM Proof of Concept

UPDATE 2021-01-13

Overview

Goals

- Prove viability of Framing document's definition
- Expansion beyond initial PoC
 - Expanded use cases
 - Expanded participant list: HDOs, MDMs, vendors/suppliers
 - Tooling and automation
- "How-to" / playbooks for HDOs and MDMs

Approach

- Collaborate with other working groups on definition
- SBOMs produced for a predefined set of devices
- Execute proposed use cases including procurement
- Iterate to increasing complexity and speculative topics with published deliverables each iteration

Participants

HDOs

- Cedars-Sinai
- Christiana Care
- Cleveland Clinic
- Mayo Clinic
- New York Presbyterian
- Sutter Health

Vendors

- Medigate
- Censinet
- Nuvolo

MDMs

- Abbott
- Medtronic
- Philips
- Siemens Healthineers
- Thermo Fisher Scientific

Iteration 1 Objectives

Execute Naming-Focused Use Cases

- Use Case 1: A Supplier Creates an SBOM for a Primary Component
- Use Case 2: An SBOM Stakeholder Creates an SBOM

Confirm SPDX format supports content

- One format for this iteration
- Additional formats in following iterations

Confirm Baseline Elements

- Author Name
- Supplier Name
- Component Name
- Version String
- Unique Identifier
- Relationship
- Primary Component
- Included Components

Iteration 2 Objectives

Software Document Version

SBOM Component Completeness

Unique Identifier using **purl**

Software Identity

- List of common components
- Conventions to establish software identity
- Alignment across participant SBOMs for common components

SBOM Content for Included Components

- Include in the SBOM Document
- Reference an External SBOM Document

SBOM for Medical Device System-of-Systems

- Single Endpoint
- Multiple Endpoints

SBOM Registry

- List of POC SBOMs

Iteration 3 Objectives (Potential)

Exploring “VEX”

Unique Identifier

- purl
- CPE (or pseudo-CPE)

Additional Formats

- CycloneDX

Component Hash

Exploring MDM as Final Goods Assembler

- Ingestion of Component SBOM
- Naming Focused Use Case 5: An SBOM Consumer Uses a SBOM

Documents and Resources

HDO Quick Start Guide

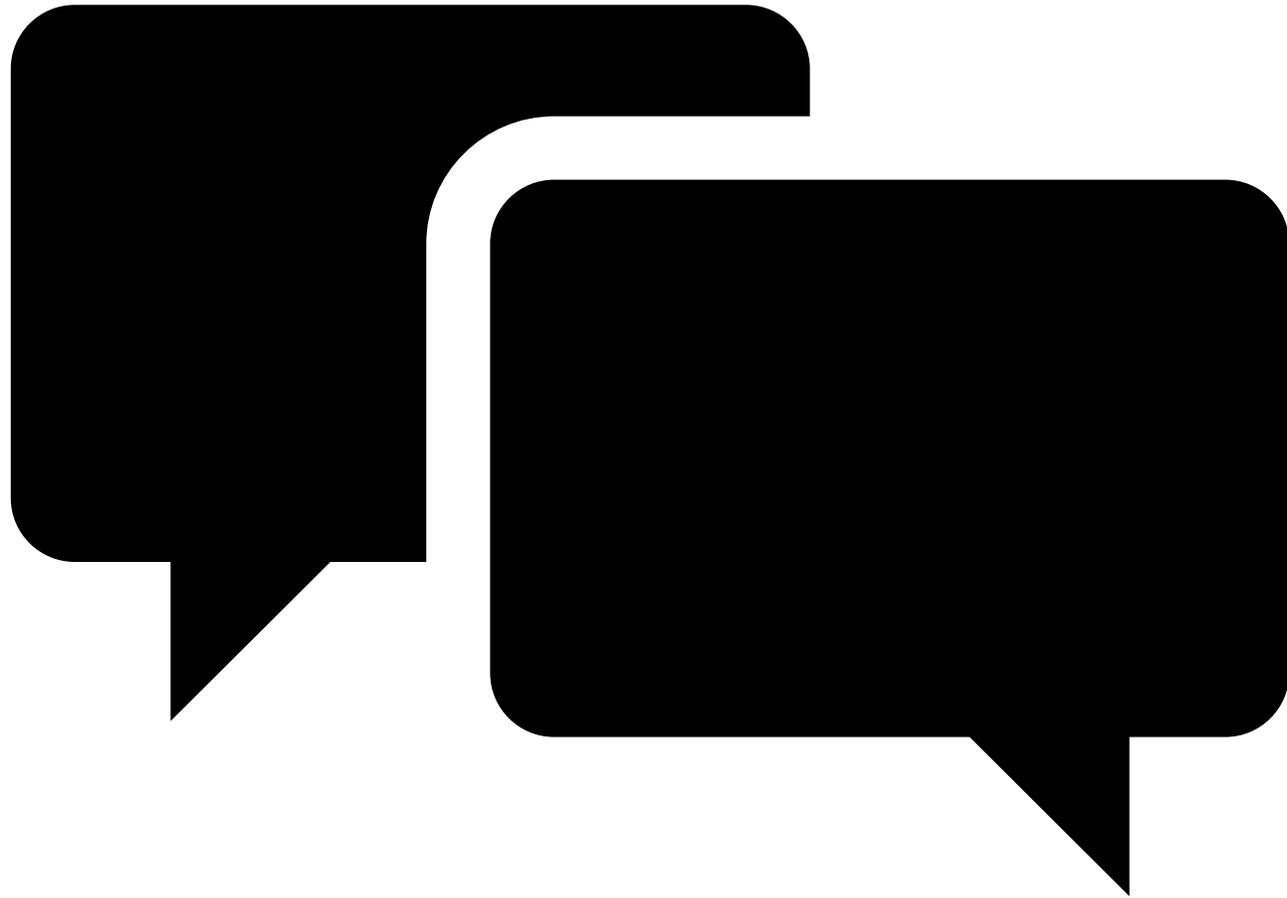
SBOM Generation How-to Document

- Guidance
- Actions for Iterations
- Examples

SBOM Medical Device System-of-Systems
Examples

Component Master List

- SBOM Examples
- SBOM Generation Tools
- SBOM Conformance Tools
- SBOM Registry



Discussion

Questions? Comments? Suggestions? Volunteers?