November 6th, 2018
All Hands Meeting

NTIA Software Component Transparency

Healthcare Proof of Concept AT A GLANCE

Leads: Jennings Aske, New York Presbyterian; Jim Jacobson, Siemens Healthineers

Objective: This is a collaborative effort between healthcare delivery organizations (HDOs) and medical device manufacturers (MDMs) to employ a provisional SBOM format 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.

Participating* Organizations: HDOs – NY Presbyterian, Cedars-Sinai, <others to be announced>. MDMs – Abbott, Bayer, Philips, Siemens.

Approach: Rapid prototyping. **Prior to the exercise:** Define the major HDO use cases in consultation with the "Use Cases and State of Practice" group. Select an existing data format that is machine readable, can satisfy the anticipated content required for the use cases and is feasible for the MDMs to produce in consultation with the "Standards and Formats" group. **During the exercise:** MDMs will generate/expose data based upon real products within the inventory of the HDOs. The HDO use cases will be exercised. As needed, and as blocking issues are encountered, the participants will iterate until reasonable options (or participant patience) are exhausted. Other members of the working group will function as observers.

Output: **Following the exercise:** The working group will create a report documenting the findings of the POC, with details captured as the exercise progresses. This report will be provided to the entire NTIA Software Component Transparency group. Following their review, the report will be available to the public and all interested parties. The working group will identify opportunities to present the results of the effort to other organizations and public forums.

HDO Use Cases: At a high level, two primary use cases will be considered: 1) Procurement and 2) Asset Management (risk management, vendor management, vulnerability management).

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.

The working group must establish a clearer definition of the roles of participants, as well as defining roles for those responsible for documenting the exercise and drafting the final 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).

*Participating means having active roles in the exercise (execution of the use cases). Many other individuals are members of the working group, collaborating on definition, direction, observing and documenting the exercise, as well as preparing the final report.