DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

IMDRF International Medical Device Regulators Forum

IMDRF/DITTA Joint Virtual Workshop

Monday 21 Sept. 2020

Cybersecurity - Where are we today?

Introduction to IMDRF Cybersecurity Guidance

Aftin Ross, PhD

Senior Science Health Advisor

FDA Center for Devices and Radiological Health

Presentation Outline

- IMDRF/CYBER WG/N60 Final Guidance, published March 2020
  - Purpose and Scope
  - General Principles
  - Context
  - Key Themes & Public Consultation Feedback integrated in Final Guidance
- Next Steps: New Work Item Extension Proposal

Guidance Purpose & Scope

Purpose:

- To provide fundamental concepts and considerations on the general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity

Scope:

- 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))
- Focused on consideration of the potential for patient harm

DITTA General Principles

Global Harmonization: Stakeholders are encouraged to harmonize their approaches across the entire life cycle of medical device cybersecurity

Total Product Life Cycle (TPLC): Risks associated with cybersecurity threats and vulnerabilities should be considered throughout all phases in the life cycle of a medical device

Information Sharing: Stakeholders are encouraged to engage in information sharing to increase transparency and collaboration to enable the safe and effective use of medical devices

Shared Responsibility: Medical device cybersecurity is a shared responsibility. All stakeholders must understand their responsibilities and work closely with other stakeholders to respond to potential cybersecurity risks and threats throughout TPLC

Context to Keep in Mind

- There are jurisdictional differences. The guidance explicitly states that jurisdictional requirements should be considered
- Manufacturers should:
  - Employ a *risk-based* approach to the design and development of medical devices with appropriate cybersecurity protections
  - Consider both the intended use environment and reasonably foreseeable misuse

Key Themes from Public Consultation

- Streamline the document & common terminology
- Clarify stakeholder roles and responsibilities
- Scope
- Definitions
- Cybersecurity risk management vs safety risk management
- Table 1: Medical device design considerations
- Labeling and customer security documentation
- Legacy

Streamlined the Document & Common Terminology

- Cut out text that was repetitive, did not add value, or was confusing
- Use consistent terminology (e.g. update vs patch and healthcare provider vs healthcare delivery organization)

Clarify Stakeholder Roles and Responsibilities

- More clearly articulated the action, the doer of the action, and indicated as appropriate the associated timing of the action
- Streamlined terminology for different stakeholders

Scope

- Clarified bounds of the device regulator, with emphasis on patient harm and patient safety
- Clarified scope to exclude information security and directly state scope includes medical device safety and performance
- Scope includes recommendations to all stakeholders, not just manufacturers

DITTA Definitions

- Added definition of:
  - Essential Performance
- Revised definitions of:
  - Cybersecurity
  - Legacy
  - End of Life
  - End of Support
  - Update
- Removed definitions of:
  - CVSS
  - Patch

Cybersecurity risk management vs safety risk management

- Collapsed content relating to risk management into a single section
- Acknowledged that security risk management may involve additional activities outside the scope of this IMDRF guidance (focused on the potential of patient harm)
- Clarified the acceptability of either:
  - an integrated risk management process inclusive of security risk and safety risk management or,
  - a separate, parallel security risk management process that feeds into general risk management
- Retained references to ISO 14971:2019, and pointed to AAMI TIR57, TIR97 and others as relevant standards for security risk management

Table 1 - Medical Device Design Considerations

- Added more technical examples (e.g. anti-malware, prevent replay of commands, secure hashes, unique signal of intent, etc.)
- Renamed table rows from “User Access” and “Physical Design” to "User Authentication" and "Physical Access" to better differentiate the terms
- Revised Table 1 language to accurately reflect safety-oriented scope (e.g. “data” became “safety-related data”)
- Revised row titles to reflect safety-oriented scope (e.g. “Data Confidentiality” and “Data Integrity” became “Data Protection” and “Device Integrity”)
- Differentiation of software updates between regular updates and in response to identified vulnerabilities

Labeling and Customer Security Documentation

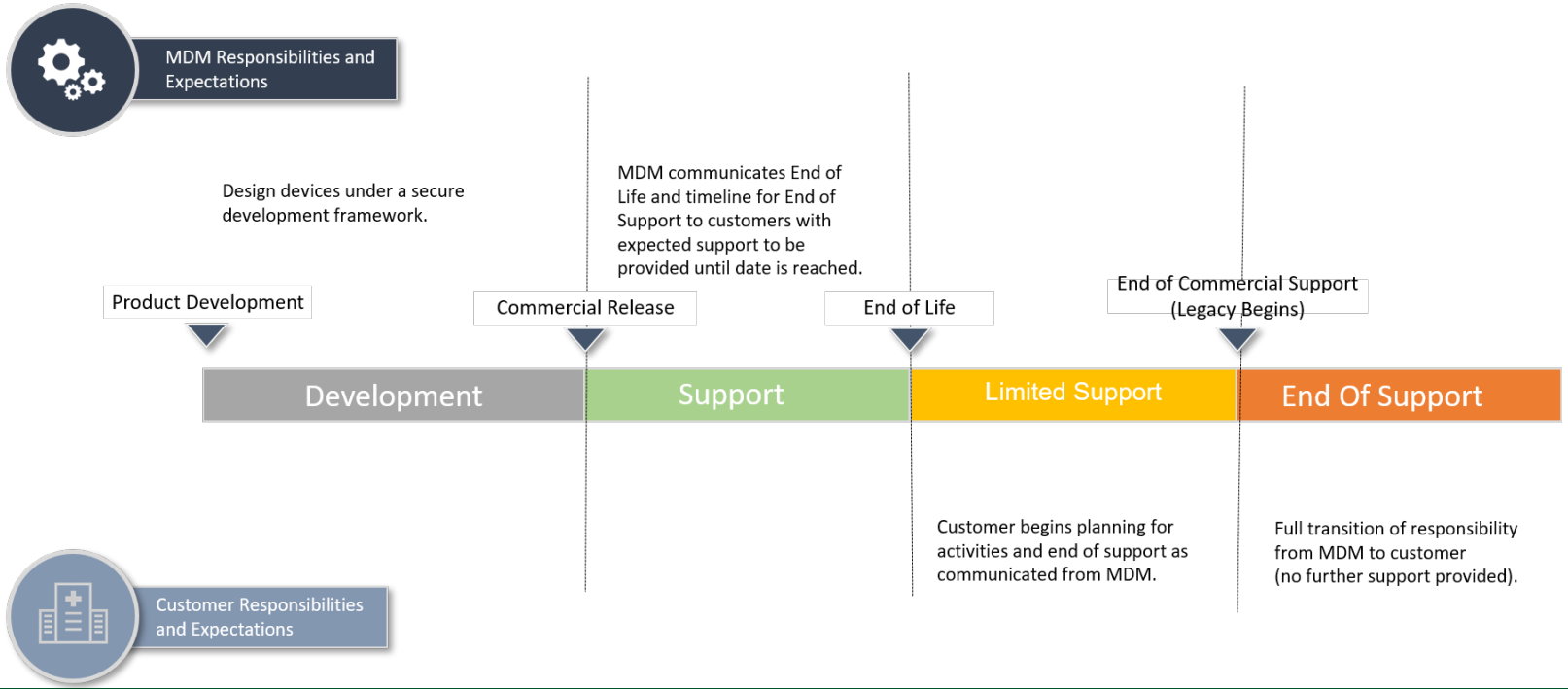
- Separated labeling and customer security documentation into distinct sections
- Clarified that SBOMs are considered under customer security documentation
- Clarified that are SBOMs are shared through trusted channels

Legacy

- Defined a conceptual framework taking us from present day to the future
- Defined legacy in terms of End of Support (EOS) vs End of Life (EOL)
- Added a figure to improve clarity
- Emphasized that device age is not a sole determinant of legacy
- Emphasized the planning and preparation for EOS for MDMs and healthcare providers
- Emphasized the transfer of responsibility
- Streamlined the document (Legacy Appendix was removed)

Legacy Device Conceptual Framework as a Function of TPLC

Cybersecurity and the Total Product Life Cycle



**Medical Device Manufacturer (MDM) follows regional guidance for medical device responsibilities, support levels may vary and as agreed upon with customers.*

New Work Item Extension Proposal

- **Focus** on Legacy Devices and Transparency of Software Components Including Use of Third-Party Software
- **Purpose:** Further underscores the link between safety & cybersecurity by:
  - Addressing implementation of SBOM, as well as, transparency in the use and support of third-party software;
    - Topics may include: lessons learned regarding construction, granularity, distribution, use, and support of third-party software including SBOM
  - Operationalizing the legacy device conceptual framework articulated in the 2020 IMDRF cybersecurity guidance in a related, but separate document.
    - Topics may include: additional definitions, legacy device best practices, postmarket vulnerability management, economic and regulatory incentives, etc.
- **Timeline:** 24-30 months

DITTA Thank you

IMDRF Cybersecurity WG
IMDRF Management Committee
IMDRF Secretariat
IMDRF Webmaster