IMDRF International Medical Device Regulators Forum

MEDICAL DEVICE CYBERSECURITY WORKING GROUP UPDATE

Working Group Co-chairs:
Dr. Suzanne Schwartz, US Food and Drug Administration
Marc Lamoureux, Health Canada

GOALS

- To facilitate international regulatory convergence on medical device cybersecurity with open discussion and sharing best practices that are understandable and feasible for all stakeholders.

- Specifically, the WG goal is to produce a document providing medical device cybersecurity guidance for all responsible stakeholders, including manufacturers, healthcare providers, regulators, and users across the entire device lifecycle.

SCOPE

The document is intended to:

- Provide recommendations to aid in minimizing cybersecurity risks across the **total product lifecycle**;
- Recognize that cybersecurity is a **shared responsibility** among all stakeholders which are not only manufacturers but also healthcare providers, patients, regulators, and researchers;
- **Define terms** consistently and clarify the current understanding on medical device cybersecurity;
- Promote broad **information sharing policies** for cybersecurity incidents, threats, and vulnerabilities.

Linkages with Existing IMDRF Documents

- IMDRF/GRRP WG/N47 FINAL: 2018, in sections 5.5.2 and 5.8 describes information security, IT environment and cybersecurity.

- IMDRF/SaMD WG/N12 FINAL: 2014 describes the importance of information security with respect to safety considerations in Section 9.3.

- It was the intent of this WG to further elaborate on and provide additional clarity and granularity on these topics.

ACTIVITIES TO DATE

- Kick-off meeting was in **January 2019**
- Meetings occurred every 2 weeks
- Final guidance document outline complete: **February 2019**
- Guidance drafting and iterative review **February to April 2019**
- In-person WG working meeting: **June 10-13, 2019**, Medical Imaging & Technology Alliance (MITA) office in Arlington, Virginia
- Submitted draft Guidance to IMDRF Management Committee : **August 2019**

Key Highlights of Current Draft

- Document is structured into 4 main components:
  - Definitions
  - General Principles
  - Pre-market Considerations
  - Post-market Considerations

- All definitions add to N47 terms/definitions, generally align with internationally recognized standards, and include key terms such as: '*cybersecurity*', '*compensating control*', '*legacy device*', '*patch*', and '*privacy*', among others

KEY HIGHLIGHTS CONT'D

- **General Principles** section covers:
  - Requirement for total product life cycle approach
  - Concept of shared responsibility among stakeholders
  - Global harmonization and concept of information sharing

- **Pre-market** section covers:
  - Recommendations for manufacturers only
  - Recommendations include: good design, risk management, security testing, labelling, and regulatory submission requirements

KEY HIGHLIGHTS CONT'D

- **Post-market** section covers:
  - Recommendations for all stakeholders including manufacturers, healthcare providers and patients (users), regulators, and security researchers
  - Includes 'best practices' for healthcare providers to use medical devices in a secure manner
  - Provides guidance on information sharing and vulnerability disclosure along with remediation concepts and incident response best practices
  - Proposes level of regulatory oversight required for different categories of software maintenance
  - Recommends best practices for Legacy devices (devices that cannot be reasonably protected against current cybersecurity threats)

Future Work Plan and Milestones

1. Proposed document planned for Public Consultation: **October and November 2019**
2. Review and Organize Public Comments: **December 2019**
3. In-person meeting to produce a final guidance document: **mid/late January 2020** (tentatively Geneva, Switzerland)
4. Submit Final Guidance in **February 2020** for approval at Management Committee Meeting in **March 2020**

THANK YOU