IMDRF - DITTA Joint Virtual Workshop

Cybersecurity: Where are we today?

Taking place during the 16th meeting of IMDRF

Monday 21 Sept. 2020
13:00 to 16:00 CEST – 7:00 to 10pm SGT – 7:00 to 10:00am EST

Preamble:
Cybersecurity is a high priority for physicians, hospitals, and manufacturers of all internet-connected devices, and even more so when patient safety and health information are at stake. DITTA continues to be pro-active and lead efforts to strengthen cybersecurity for medical technologies. Cybersecurity is a shared responsibility. Collaboration between regulators, healthcare providers and industry is thus essential to safeguard the patients' health information and their physical safety. As IMDRF has recently adopted its guidance on cybersecurity of medical devices, the workshop takes place at the right time to discuss its implementation in the different jurisdictions.

Workshop Objectives:
- Follow-up on the publication of the IMDRF cybersecurity guidance
- Better understand how regulatory frameworks are evolving and provide an overview on evolution in various jurisdictions
- Understand current developments of cybersecurity international standards in healthcare
- Learn from healthcare providers on steps towards ensuring their facility is cyber secure
- Understand ways to avoid cyber-attacks utilizing advanced risk frameworks
- Learn what the medical device industry is doing to make devices more cyber secure and preventing from cyber attacks

Moderation:
- IMDRF moderator from Singapore for part 1, 2 and 5
- DITTA moderation for part 3 and 4

Proposed structure

- Welcome Introduction by DITTA Chair (5 mins)
- Keynote Opening from IMDRF Chair (5 mins)
- Latest Update from IMDRF Cybersecurity WG Convenor (10 mins)

Part 1: Regulations – status in IMDRF jurisdictions (40 min)

Purpose: Provide latest developments in regulatory frameworks in 5 regions
Principle: panel of 5 regulators from Singapore, USA, Europe, Japan and Canada (5 max countries), having 5 mins pitch each followed by 15 mins open discussions on global regulatory convergence
Part 2: What healthcare providers are doing on cybersecurity (20 mins)

**Purpose:** better understand initiatives/actions taken by hospital providers

**Proposal:** 2 speakers – 1 from Singapore, 1 from Europe

Virtual Break (5 mins)

Part 3: International standards on cybersecurity (30 mins)

**Purpose:** Share latest developments in standardization on cybersecurity

**Principle:** panel of 2 Standard organizations IEC and ISO, having 10 mins pitch each followed by 10 mins open discussions on how those standards are complementing and provide support to regulatory framework

Part 4: What Industry is doing to prevent cyber-attacks (40 mins)

**Purpose:** Share initiatives, best practices and actions taken by manufacturers

**Principle:** panel of 4 manufacturers (2 from DITTA, 2 from GMTA) having 5 mins pitch each followed by 20 mins open discussions on their visions and actions

Part 5: Multi-stakeholder panel discussions (20 mins)

**Purpose:** Exchange between regulators, industries, standard bodies and healthcare providers on how to maximize collaboration

**Principle:** panel including 2 regulators, 1 DITTA rep., 1 rep for standardization, 1 rep. for hospital provider

Conclusions by IMDRF Lead and DITTA Chair (5 mins)