



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

KMDIA Virtual Seminar

Thursday 29 July 2021

Introduction of DITTA Cybersecurity WG

Keiichiro Ozawa

Vice-chair of DITTA Cybersecurity WG



1. DITTA Activities of IMDRF

1. DITTA Activities of IMDRF

1-1 Promote and raise the global momentum of Cybersecurity

- IMDRF SaMD Guidance (IMDRF/SaMD WG/N12*) describes the importance of information security with respect to safety considerations in Sec. 9.3. (2014)

1. DITTA has recognized the worldwide importance of cybersecurity since then and promoting cybersecurity as the IMDRF work item.
2. DITTA held the **1st workshop** on cybersecurity in Brasilia (2016)
3. DITTA released the **1st white paper** on cybersecurity (2016)
 - FDA released “Post Market Management of Cybersecurity” (2016)

* <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-140918-samd-framework-risk-categorization-141013.pdf>

1. DITTA Activities of IMDRF

1-2 Development of New Work Item Proposal of IMDRF

4. DITTA held the **2nd workshop** on cybersecurity accompanying IMDRF meetings in Shanghai (March 2018).
 - Raising the cybersecurity awareness of both regulators and industries in the medical device field
 - Discussion on New Work Item Proposal among regulators.
5. DITTA Developed the **New Work Item Proposal** (March – May 2018)
6. Submission of NWIP to IMDRF Management Committee (June 2018)
 - **IMDRF MC approved the NWIP** (Beijing, Sep. 2018)
7. DITTA presented the importance of the global harmonization of cybersecurity in AHWP Annual Meeting(Kuala Lumpur, Nov. 2018)

1. DITTA Activities of IMDRF

1-3 Three important points in NWIP

Topic 1: Shared responsibility among stakeholders

Cybersecurity is a shared-responsibility among all stakeholders, including manufacturers, healthcare providers, regulators, patients, and others.

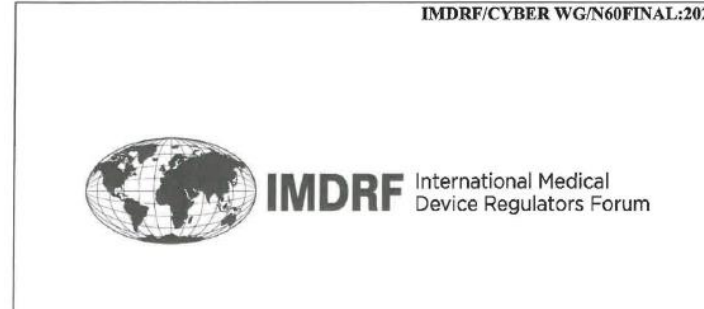
Topic 2: Information sharing

Broad information-sharing policies to have clearly established legal guardrails and create incentives for participation.

Topic 3: Definition

Define the terms and clarify the current understanding on medical device cybersecurity. It is necessary to clarify and define that medical device cybersecurity is different from information security which maintains confidentiality, integrity and availability.

1. DITTA Activities of IMDRF



And IMDRF WG activity started...
(Jan. 2019)

Title: Principles and Practices for Medical Device Cybersecurity
Authoring Group: Medical Device Cybersecurity Working Group
Date: 18 March 2020



Dr Choong May Ling, Mimi, IMDRF Chair

This document was produced by the International Medical Device Regulators Forum. There are no restrictions on the reproduction or use of this document; however, incorporation of this document, in part or in whole, into another document, or its translation into languages other than English, does not convey or represent an endorsement of any kind by the International Medical Device Regulators Forum.

Copyright © 2020 by the International Medical Device Regulators Forum.

1. DITTA Activities of IMDRF

1-4 Suggestion by DITTA in the IMDRF cybersecurity work item

a. DITTA is supporting the IMDRF activity

- DITTA organizes mirror groups and supports the activities in IMDRF!

b. Scope and definition

- The scope is well described in the Guidance Document. But DITTA would like to put more stress on the **difference between “medical device cybersecurity” and “information security”**.

c. Feasibility of the guidance document

- Currently the implementation of the Document attracts much attention from stakeholders. The key is the feasibility. DITTA would like to recommend each jurisdiction would consider one's own regulatory background and implement the document.



1. DITTA Activities of IMDRF

1-5 Publishment of N60 and DITTA Whitepaper

8. IMDRF published the guidance document (March 2020)
 - Principles and Practices for Medical Device Cybersecurity
<http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf>
9. IMDRF-DITTA Joint Workshop on cybersecurity (March 2020)
 - **The 3rd workshop on cybersecurity**
10. DITTA published **the 3rd whitepaper** (June 2021)



2. DITTA Whitepapers

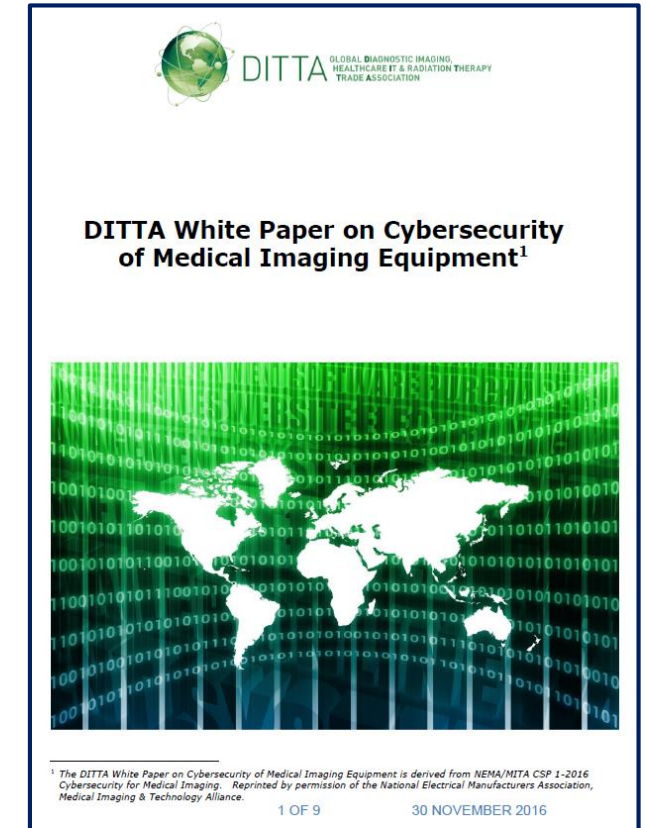
2. DITTA Whitepapers

2-1 DITTA White Paper on Cybersecurity of Medical Imaging Equipment

- Published in November 2016*
- Based on NEMA/MITA Cybersecurity for Medical Imaging
- Detailed cybersecurity best practices for manufacturers, suppliers and healthcare providers

*

http://www.globalditta.org/fileadmin/user_upload/Level_home/Press_releases/2016/DITTA_Cybersecurity_paper_29_Nov._2016_final_clean.pdf



2. DITTA Whitepapers

2-2 DITTA White Paper on Cybersecurity: *Best Practices in the Medical Technology Manufacturing Environment*

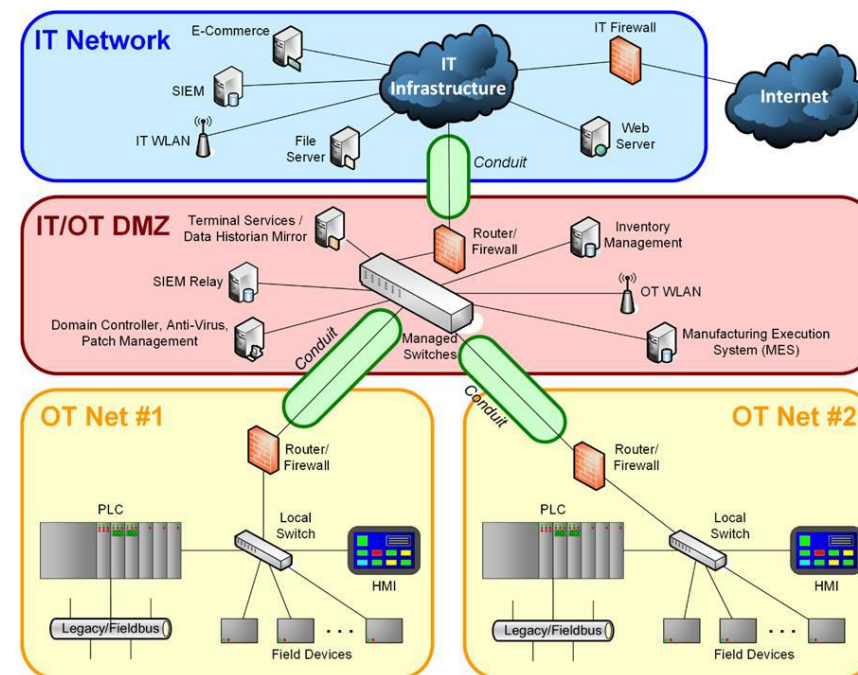
- Published in February 2019*
- Based on NEMA CPSP 2-2018 Cyber Hygiene Best Practices
- A set of industry best practices and guidelines within the medical technology manufacturing facility and engineering processes

*
https://www.globalditta.org/uploads/media/DITTA_White_paper_on_Cybersecurity_-_Feb._2019_-_Final.pdf



2. DITTA Whitepapers

1. Segmenting Networks
2. Understanding Data Types and Flows
3. Hardening Devices
4. Monitoring Devices and Systems
5. User Management
6. Updating Devices
7. Providing a recovery plan/escalation process



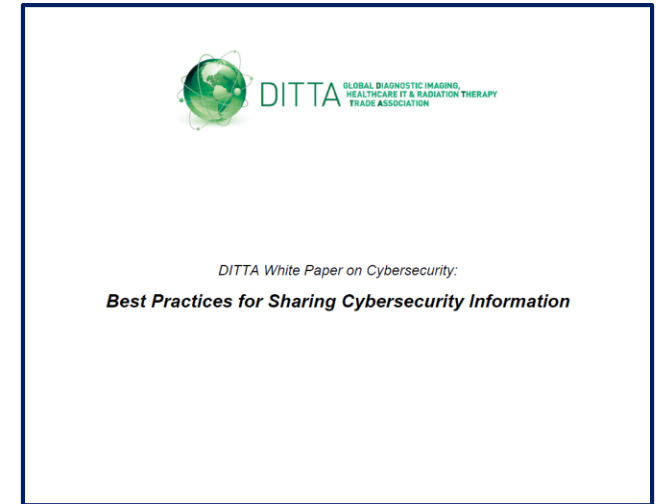
Segmenting networks

2. DITTA Whitepapers

2-3 DITTA White Paper on Cybersecurity: *Best Practices for Sharing Cybersecurity Information*

- Published in June 2021*
- Based on NEMA CPSP 3-2019 Cyber Hygiene Best Practices Part 2
- Industry best practices and guidelines that medical technology imaging manufacturers may consider when providing cybersecurity information to their customers
- It provides suggestions for how customers can work with their respective manufacturers.

* https://www.globalditta.org/fileadmin/Media_Centre/Media_Centre_2021/DITTA-Best_Practices_for_Sharing_Cybersecurity_Information_Final.pdf



3. DITTA Perspective on Cybersecurity



DITTA 3. DITTA Perspective on Cybersecurity

As an international trade association, we can contribute to medical device cybersecurity in terms of manufacturers by

1. Continuing development of **best practice documents** which are practical, feasible and promising quick effect
2. **Recognizing significant international standards**
3. Encouraging **information sharing** between manufacturers and healthcare providers by MDS2*

* SBoM and MDS2 will be discussed by the next speaker.



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

THANK YOU!

Keiichiro Ozawa

FUJIFILM Corporation

www.globalditta.org

Follow us on @DITTA_online

