Korea IMDRF Cybersecurity Working Group

2021.7.29.

Keunhee Han

khhan1@korea.ac.kr

KMDIA 사단법인 한국의료기기산업협회
Korea Medical Devices Industry Association

Ⅰ. Introduction of Korea Cybersecurity WG

1. Purpose of WG
2. Contributions and collaborations to IMDRF with MFDS

Ⅱ. Korea Status of Cybersecurity

1.1 Purpose of WG

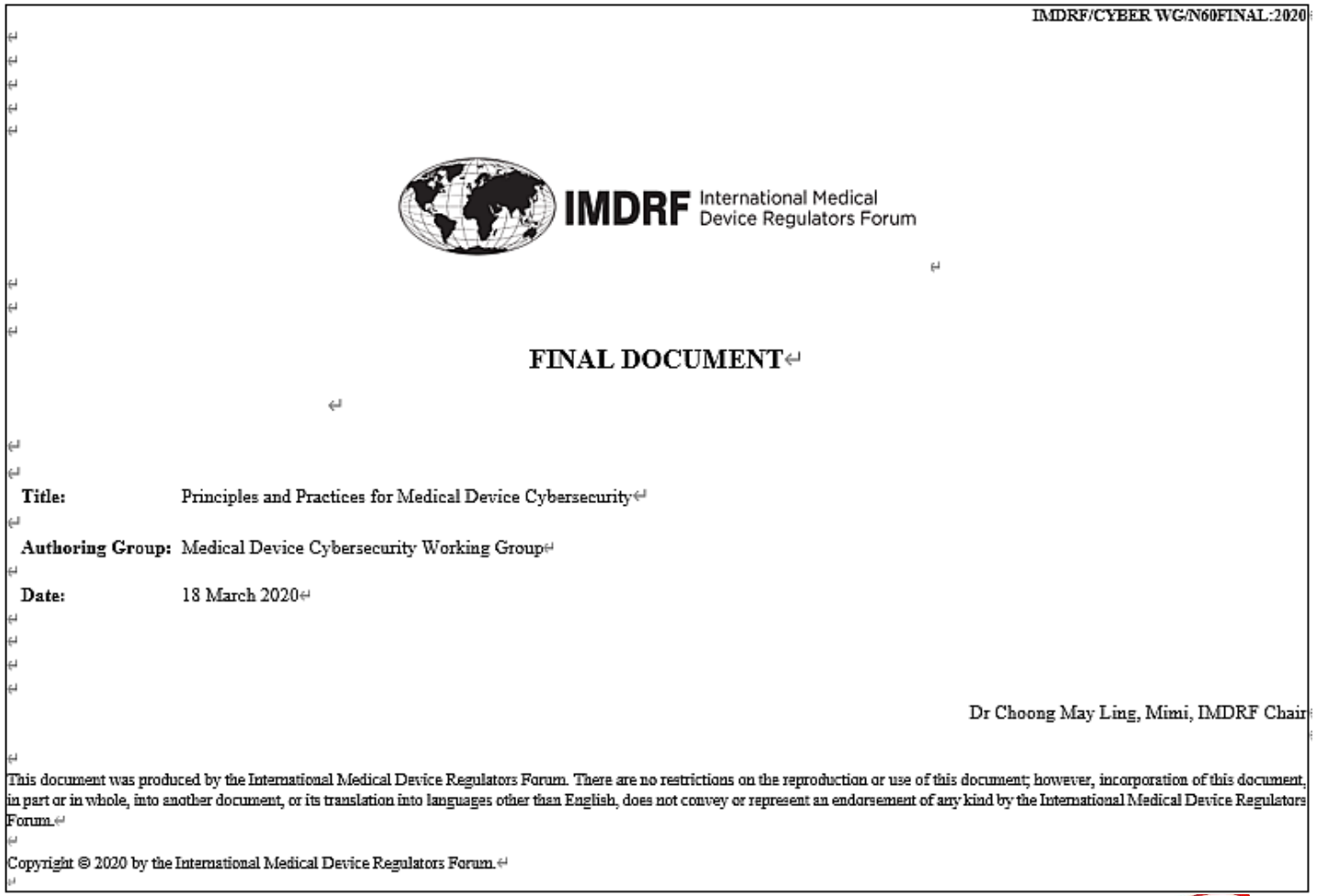
- WG Purpose
  - Sharing best practices among regulators on medical device cybersecurity and establishing common pre-market and post-market regulations.
- WG Configuration
  - A total of 14 academic/research/corporate experts chaired by Professor Keunhee Han of Korea University.
- WG Activity
  - Conduct regular/temporary meetings after committee formation
  - Support for creating a Medical Device Cybersecurity Guidelines organized by IMDRF
  - Support documents for "cyber security principles and utilization" by dividing the scope into pre- and post-market categories

1.1 Purpose of WG

No.	Name	Organization	Position	Role	Field
1	Keunhee Han	Korea University	Professor	Leader	Academy
2	이인혜	스마트의료보안포럼	사무국장		기관
3	이기태	삼성전자㈜	책임연구원		산업계
4	이성기	경북대학교 컴퓨터학부	교수		학계
5	권이석	한국산업기술시험원	주임연구원		시험연구
6	박정환	하이케어넷 주식회사	부장		산업계
7	방지호	한국기계전기전자시험연구원 정보보안센터	센터장		기관
8	조봉호	한국화학융합시험연구원	수석연구원		시험연구
9	장승진	LG 전자 CEO부문 디자인엔지니어링담당	책임연구원		산업계
10	이동학	㈜필립스코리아	차장		산업계
11	김민준	㈜에이치쓰리(H3)시스템	대표이사		산업계
12	김순석	한라대학교	교수		학계
13	백종현	한국인터넷진흥원	팀장		기관
14	권혁찬	한국전자통신연구원 정보보안연구본부	책임연구원		기관

1.2 Contributions and collaborations to IMDRF with MFDS(Ministry of Food and Drug Safety)

- "Principles and Practices for Medical Device Cybersecurity" published March.18.2020
- Members of the Cyber Security Working Group contributed to the IMDRF's guidelines and regulations through expert meetings.



IMDRF/CYBER WG/N60FINAL:2020

IMDRF International Medical Device Regulators Forum

FINAL DOCUMENT

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.

1.2 "Principles and Practices for Medical Device Cybersecurity"

- Purpose:
  - To provide fundamental concepts and considerations on the general p rinciples and best practices on medical device cybersecurity
- Scope:
  - Considers cybersecurity broadly in the context of medical devices that either contain or composed of software, and not just network connect ed devices
  - Excludes information security and directly state scope includes medic al device safety and performance
  - Includes recommendations to all stakeholders, not just manufacturers

1.2 "Principles and Practices for Medical Device Cybersecurity"

- General Principles:

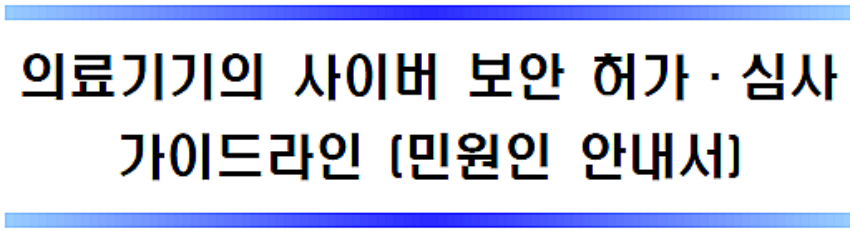
1. **Global Harmonization**: Stakeholders are encouraged to harmonize their cybersecurity approaches across the entire life cycle of the medical device.
2. **Total Product Life Cycle (TPLC)**: Risks associated with cybersecurity threats and vuln erabilities should be considered throughout all phases in the life cycle of a medical de vice.
3. **Information Sharing**: Stakeholders are encouraged to engage in information sharing to increase transparency and collaboration to enable the safe and effective use of medic al devices.
4. **Shared Responsibility**: All stakeholders must understand their responsibilities and wor k closely with other stakeholders to respond to potential cybersecurity risks and threa ts.

1.2 New Work Item Extension

- Progress and Planned MilestonesPurpose:
- **Goal:** To increase international alignment and improved safety and securit y
  - February 3, 2021: New Work Kickoff Meeting
  - April 2021: Final Document Outline
  - April–October 2021: WG Meetings every two weeks
  - October/November: 4-day WG Meeting
  - February 2022: Submission of draft to IMDRF MC(Management Committee)
  - April 2022: Public Consultation*
  - April–October 2022: WG Meetings
  - October/November 2022: 4-day WG Meeting
  - March 2023: Publish Final Document(s)*

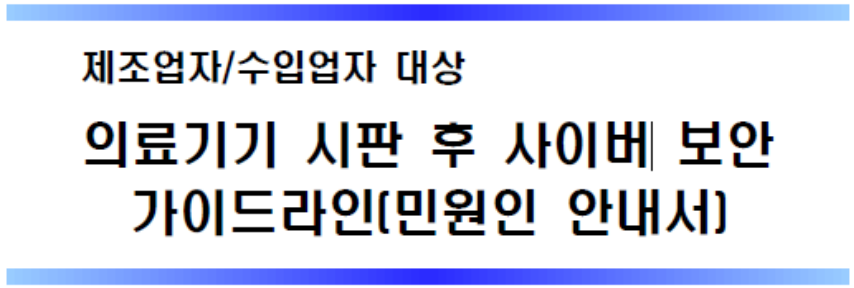
2 Korea Status of MD Cybersecurity

- Publication of "Guidelines for Cybersecurity Authorization and Examination of Medical Devices“ - Nov.2019
- Purpose
  - It is intended to secure safety management of medical devices that can communicate by clarifying the application of medical devices requiring cybersecurity and determining security requirements that can be applied according to the characteristics of the product and the scope of data to be submitted.
- Scope
  - 1) Medical devices that transmit and receive personal medical information such as biometric information of patients using wired and wireless communication
  - 2) Medical devices that can control devices using wired and wireless communication
  - 3) Medical devices that use wired and wireless communication to maintain firmware or software updates.



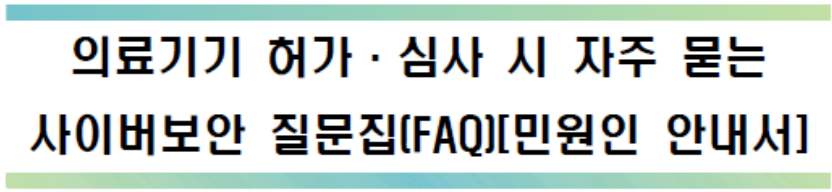
2 Korea Status of MD Cybersecurity

- Publication of " Guidelines for Medical Device Post-Market Cybersecurity" – Nov.2020
- Purpose
  - In order to respond to cybersecurity vulnerabilities after medical device marketing, it will present matters to be managed and observed by medical device manufacturers / importers, and reduce the risk of cybersecurity throughout the medical device lifecycle.
- Scope
  - 1) Medical devices that transmit and receive personal medical information such as biometric information of patients using wired and wireless communication
  - 2) Medical devices that can control devices using wired and wireless communication
  - 3) Medical devices that use wired and wireless communication to maintain firmware or software updates.



2 Korea Status of MD Cybersecurity

- Publication of "Cybersecurity FAQs Frequently Asked During Medical Device License Examination" – Apr.2021
- Part 1 Subject to submission of cybersecurity data: 19 items
  - A. Whether data are subject to submission for the purpose of communication.
  - B. Whether to submit data according to the composition of communication
  - C. Whether to submit data in the event of modification.
- Part2 Cybersecurity Required Principles Checklist: 7 items
  - A. What applies according to the communication configuration
  - B. Method of proof by checklist item
- Part 3 Cybersecurity Safety Proof Data: 9 Items
  - A. Requirements and types of data submitted
  - B. Matters to be included in the submitted materials.



2 Korea Status of MD Cybersecurity

- We will continue to reflect cybersecurity requirements in related laws and systems.
- We are going to benchmark cybersecurity issues of foreign regulators and push for system reform suitable for global trends.
- The Ministry of Science and ICT selects three universities in the metropolitan area and selects a convergence security graduate school that learns Healthcare security as its main major and fosters professional personnel.
- International standards for the security of IEC 62443 Series industrial control systems are being prepared in Asian countries such as Australia, EU, and US FDA to secure medical device products in the process of developing and producing them.
- So, We are lecturing on EMR/PACS/OCS Security, Medical Device Security, Risk Management, and Healthcare International Standards documents in graduate coursework.

Thanks