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

AHWP Asian Harmonization Working Party
WORKING TOWARDS MEDICAL DEVICE HARMONIZATION IN ASIA

Asian Harmonization Working Party

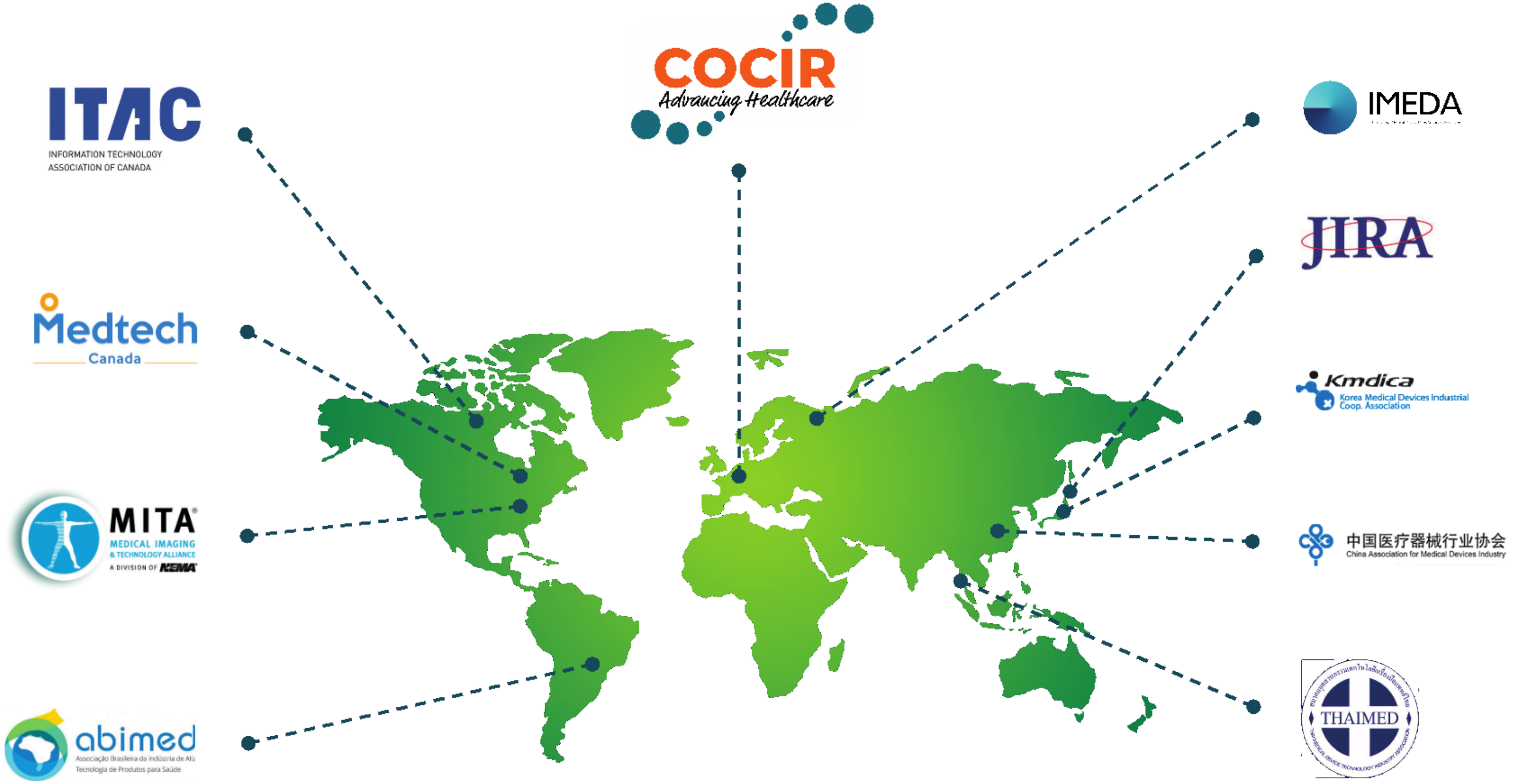
12 November 2019, Oman

General Overview on Cybersecurity trends around the Globe

Greg LeBlanc
DITTA

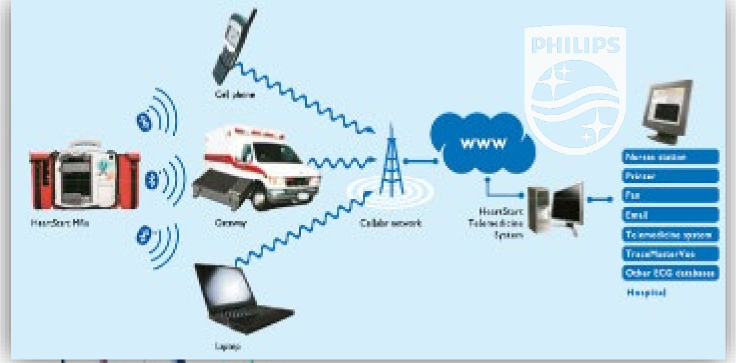
DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

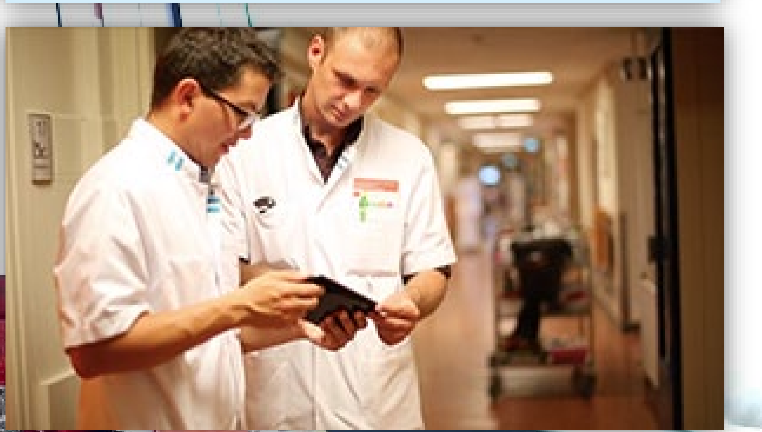
DITTA GLOBAL PRESENCE


COCIR
Advancing Healthcare
ITAC
INFORMATION TECHNOLOGY ASSOCIATION OF CANADA
IMEDA
JIRA
Medtech Canada
Kmdica
Korea Medical Devices Industrial Coop. Association
MITA
MEDICAL IMAGING & TECHNOLOGY ALLIANCE
A DIVISION OF NEMA
中国医疗器械行业协会
China Association for Medical Devices Industry
abimed
Associação Brasileira da Indústria de Alta Tecnologia de Produtos para Saúde
THAIMED

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA MEDICAL IMAGING & TECHNOLOGY ALLIANCE A DIVISION OF NEMA · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · ITAC INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

Healthcare is increasingly depended on ICT





Systems are increasingly connected

Systems are increasingly wireless

Systems become more ‘intelligent’

Shift from products to services

Safety versus Security

Exchange of security information is essential

Integration of networks and responsibilities?

Shared responsibility

RISKS → Mitigate

RISKS → Accept

RISKS → Reduce

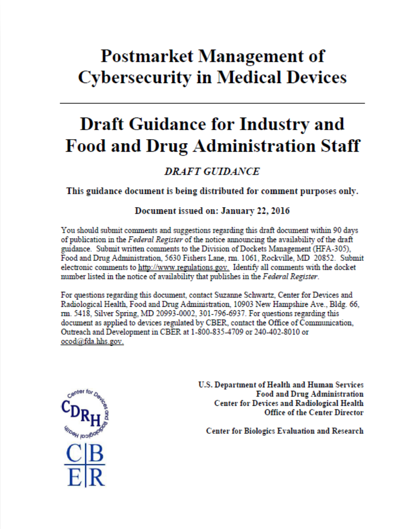
RISKS → Transfer

Digital transformation also increases security risks

Do we manage on Risk or Compliance?

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

THERE IS A LOT OF REGULATORY SECURITY GUIDANCE OUT THERE…



Postmarket Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

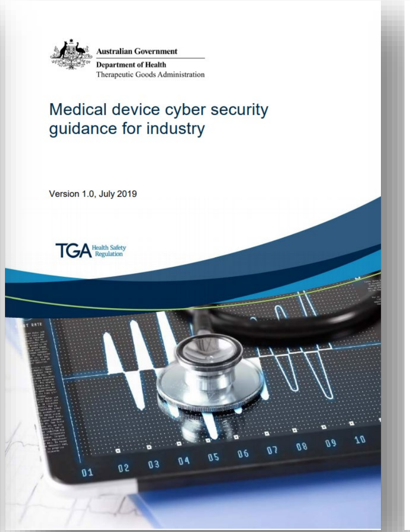
Document issued on: January 22, 2016

You should submit comments and suggestions regarding this draft document within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Submit electronic comments to http://www.regulations.gov. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5418, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director

Center for Biologics Evaluation and Research

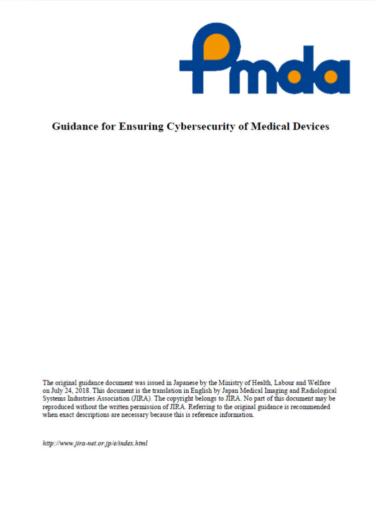


Australian Government
Department of Health
Therapeutic Goods Administration

Medical device cyber security guidance for industry

Version 1.0, July 2019

TGA Health Safety Regulation

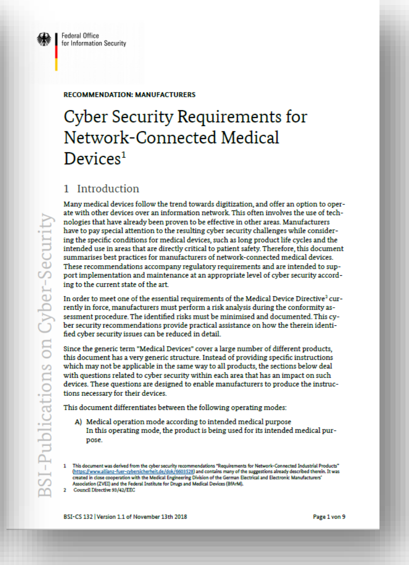


Pmda

Guidance for Ensuring Cybersecurity of Medical Devices

The original guidance document was issued in Japanese by the Ministry of Health, Labour and Welfare on July 24, 2018. This document is the translation in English by Japan Medical Imaging and Radiological Systems Industries Association (JIRA). The copyright belongs to JIRA. No part of this document may be reproduced without the written permission of JIRA. Referring to the original guidance is recommended when exact descriptions are necessary because this is reference information.

http://www.jira-net.or.jp/e/index.html



Federal Office for Information Security

BSI-Publications on Cyber-Security

RECOMMENDATION: MANUFACTURERS

Cyber Security Requirements for Network-Connected Medical Devices[1]

1 Introduction

Many medical devices follow the trend towards digitization, and offer an option to operate with other devices over an information network. This often involves the use of technologies that have already been proven to be effective in other areas. Manufacturers have to pay special attention to the resulting cyber security challenges while considering the specific conditions for medical devices, such as long product life cycles and the intended use in areas that are directly critical to patient safety. Therefore, this document summarises best practices for manufacturers of network-connected medical devices. These recommendations accompany regulatory requirements and are intended to support implementation and maintenance at an appropriate level of cyber security according to the current state of the art.

In order to meet one of the essential requirements of the Medical Device Directive[2] currently in force, manufacturers must perform a risk analysis during the conformity assessment procedure. The identified risks must be minimised and documented. This cyber security recommendations provide practical assistance on how the therein identified cyber security issues can be reduced in detail.

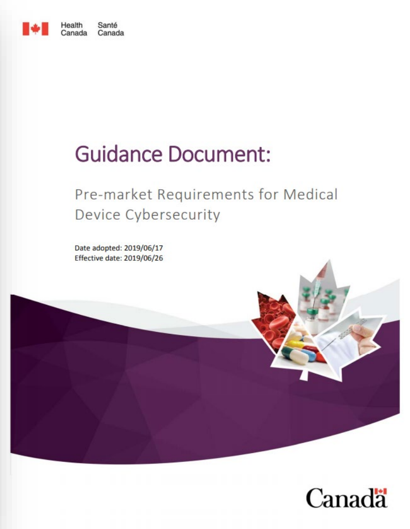
Since the generic term "Medical Devices" cover a large number of different products, this document has a very generic structure. Instead of providing specific instructions which may not be applicable in the same way to all products, the sections below deal with questions related to cyber security within each area that has an impact on such devices. These questions are designed to enable manufacturers to produce the instructions necessary for their devices.

This document differentiates between the following operating modes:

A) Medical operation mode according to intended medical purpose
In this operating mode, the product is being used for its intended medical purpose.

[1] This document was derived from the cyber security recommendations "Requirements for Network-Connected Industrial Products" (https://www.allianz-fuer-cybersicherheit.de/dok/6603528) and contains many of the suggestions already described therein. It was created in close cooperation with the Medical Engineering Division of the German Electrical and Electronic Manufacturers' Association (ZVEI) and the Federal Institute for Drugs and Medical Devices (BfArM).
[2] Council Directive 93/42/EEC

BSI-CS 132 | Version 1.1 of November 13th 2018 — Page 1 von 9



Health Canada Santé Canada

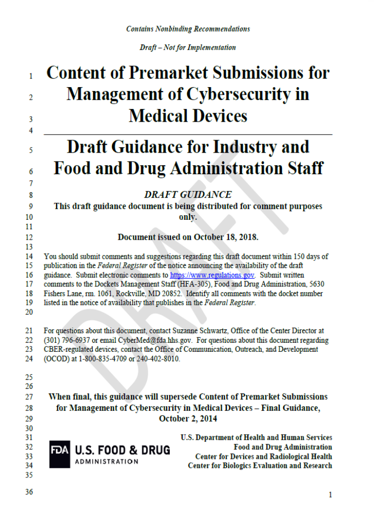
Guidance Document:

Pre-market Requirements for Medical Device Cybersecurity

Date adopted: 2019/06/17
Effective date: 2019/06/26

Canada

In development →



Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE
This draft guidance document is being distributed for comment purposes only.

Document issued on October 18, 2018.

You should submit comments and suggestions regarding this draft document within 150 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

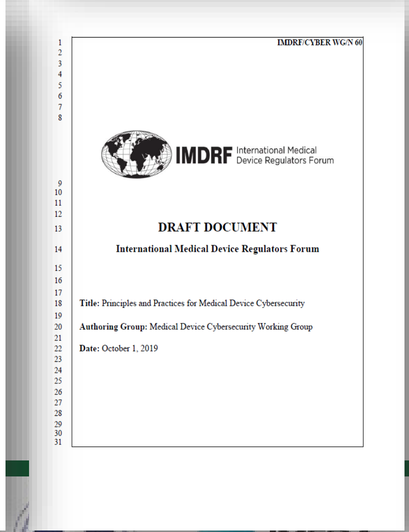
For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

1



IMDRF/CYBER WG/N 60

IMDRF International Medical Device Regulators Forum

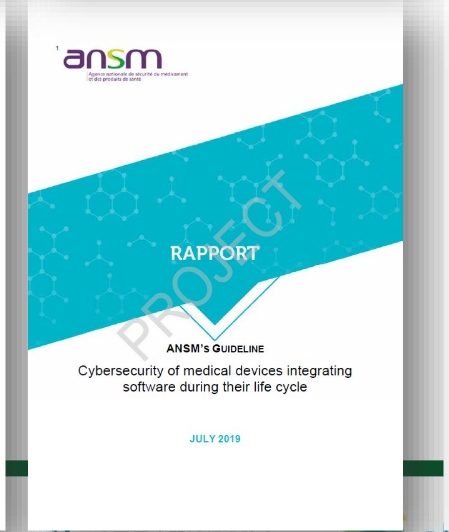
DRAFT DOCUMENT

International Medical Device Regulators Forum

Title: Principles and Practices for Medical Device Cybersecurity

Authoring Group: Medical Device Cybersecurity Working Group

Date: October 1, 2019



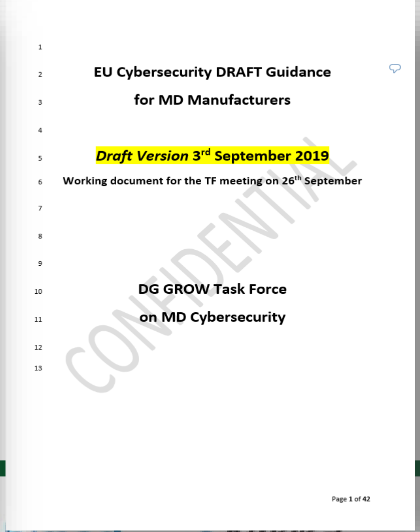
ansm
Agence nationale de sécurité du médicament et des produits de santé

RAPPORT

ANSM's GUIDELINE

Cybersecurity of medical devices integrating software during their life cycle

JULY 2019



EU Cybersecurity DRAFT Guidance

for MD Manufacturers

***Draft Version* 3rd September 2019**

Working document for the TF meeting on 26th September

DG GROW Task Force

on MD Cybersecurity

Page 1 of 42

AUSTRALIAN GUIDANCE

Medical device cyber security guidance for industry

Version 1.0, July 2019

TGA

- Total lifecycle approach (TPLC)
- References NIST Framework
- Recognizes AAMI TIR 57, UL 2900, ISO 27799, ISO/IEC 29147, ISO/IEC 30111, and others
- Stress on information sharing and vulnerability disclosure
- Stress on supply chain assessment
- References FDA guidance, NIST, IMDRF, but also South Korean and ECRI

CANADIAN GUIDANCE

Guidance Document:

Pre-market Requirements for Medical Device Cybersecurity

[illegible]

Canada

- Total lifecycle approach (TPLC)
- References NIST Framework
- Strong reference to TIR 57, NIST 800-30 and UL 2900
- Expect post market patching/monitoring plan in submission
- Expect a security risk management in parallel with safety risk management – in line with TIR 57, i.e. a dedicated security risk management process

JAPAN

Pmda

- Guidance for Ensuring Cybersecurity in Medical Devices (Notification No. 0724-1, July 24, 2018)
- Primary focus on risk management
  - Cybersecurity is now considered a foreseeable hazard
- Standards:
  - japanIEC 80001-2-2, IEC 80001-2-8 and NIST SP800-53
- Shared responsibility

EU MDR AND IVDR SECURITY GUIDANCE

- Being developed by DG Grow, Joint Research Center, European regulators, ENISA, notified bodies, hospitals and industry associations
- Details concepts around
  - Relation between safety and security risk management
  - Shared responsibility
  - State of the art
  - Documentation
  - Post market surveillance and vigilance
- Expected to be published in December 2019

EU Cybersecurity DRAFT Guidance
for MD Manufacturers

Draft Version 3rd September 2019
Working document for the TF meeting on 16th September

DG GROW Task Force
on MD Cybersecurity

IMDRF PRINCIPLES AND PRACTICES FOR MEDICAL DEVICE CYBERSECURITY

IMDRF

- Currently out for public consultation, closes on 2 Dec. http://www.imdrf.org/consultations/cons-ppmdc.asp
- Details concepts around
  - Total lifecycle approach (TPLC)
  - Shared responsibility
  - Information sharing
  - Documentation
  - Post market requirements
  - Coordinated vulnerability disclosure
- References to many standards and other guidance's

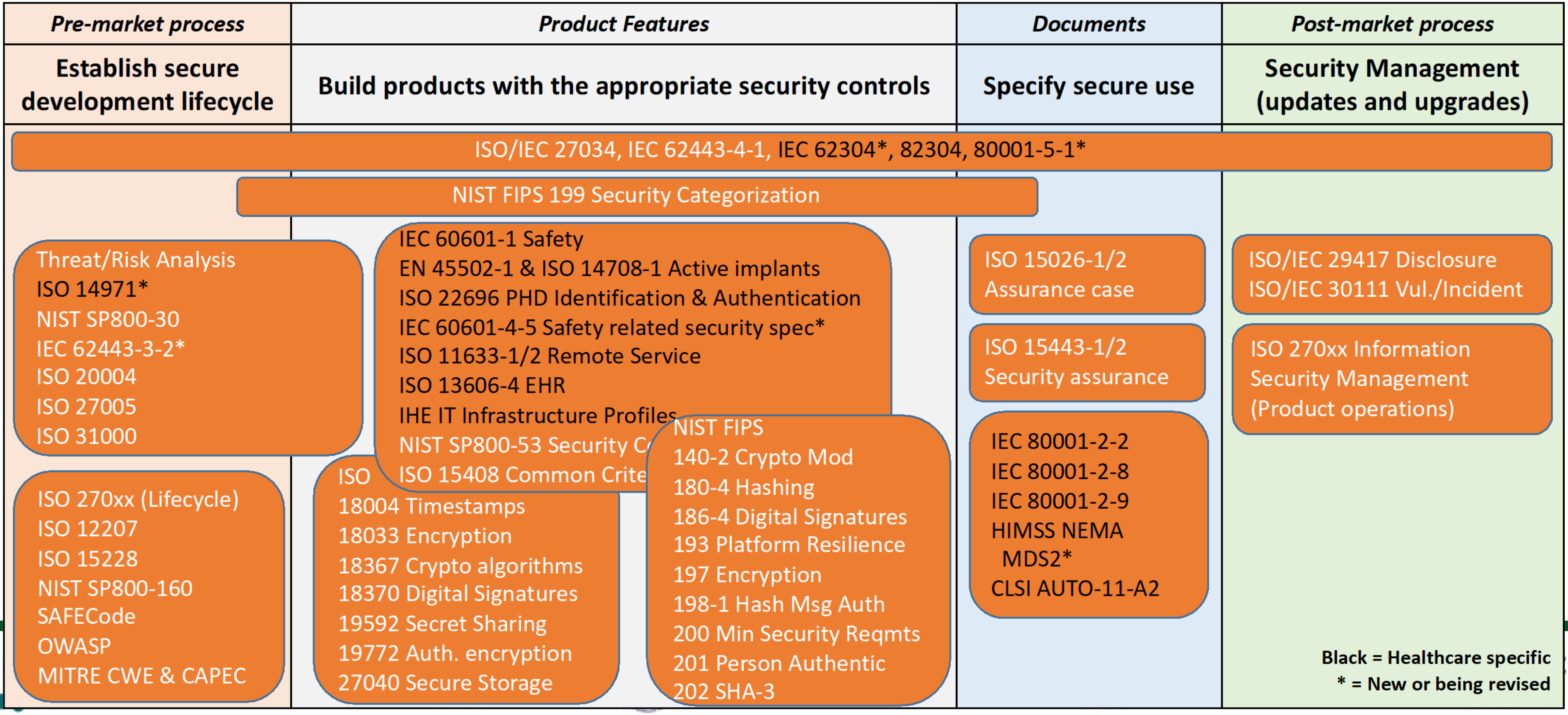
DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

CONSISTENT ELEMENTS ACROSS REGULATIONS

- **Security Risk Management**
- **Security by Design** (and by default)
- **Standards**
- **Documentation**
- **Total lifecycle with post market security requirements:**
  – Vulnerability and Patch management
  – Coordinated Vulnerability Disclosure

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

EXAMPLES OF SECURITY RELATED (HEALTHCARE) STANDARDS THAT CAN BE USED IN THE LIFE CYCLE OF MEDICAL DEVICES AND HEALTH SOFTWARE



Pre-market process	*Product Features*	*Documents*	*Post-market process*
Establish secure development lifecycle	**Build products with the appropriate security controls**	**Specify secure use**	**Security Management (updates and upgrades)**

ISO/IEC 27034, IEC 62443-4-1, IEC 62304*, 82304, 80001-5-1*

NIST FIPS 199 Security Categorization

Threat/Risk Analysis
ISO 14971*
NIST SP800-30
IEC 62443-3-2*
ISO 20004
ISO 27005
ISO 31000

ISO 270xx (Lifecycle)
ISO 12207
ISO 15228
NIST SP800-160
SAFECode
OWASP
MITRE CWE & CAPEC

IEC 60601-1 Safety
EN 45502-1 & ISO 14708-1 Active implants
ISO 22696 PHD Identification & Authentication
IEC 60601-4-5 Safety related security spec*
ISO 11633-1/2 Remote Service
ISO 13606-4 EHR
IHE IT Infrastructure Profiles
NIST SP800-53 Security C
ISO 15408 Common Crite

ISO
18004 Timestamps
18033 Encryption
18367 Crypto algorithms
18370 Digital Signatures
19592 Secret Sharing
19772 Auth. encryption
27040 Secure Storage

NIST FIPS
140-2 Crypto Mod
180-4 Hashing
186-4 Digital Signatures
193 Platform Resilience
197 Encryption
198-1 Hash Msg Auth
200 Min Security Reqmts
201 Person Authentic
202 SHA-3

ISO 15026-1/2
Assurance case

ISO 15443-1/2
Security assurance

IEC 80001-2-2
IEC 80001-2-8
IEC 80001-2-9
HIMSS NEMA
MDS2*
CLSI AUTO-11-A2

ISO/IEC 29417 Disclosure
ISO/IEC 30111 Vul./Incident

ISO 270xx Information
Security Management
(Product operations)

Black = Healthcare specific
* = New or being revised

ISO/TC215 AND IEC/TC62 DEVELOPMENT ACTIVITIES RELATED TO MEDICAL DEVICES/HEALTH-IT SECURITY

- Update* ISO/IEC 80001-1(:2020-Q1)
  Health informatics — Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 1: Application of risk management

- NWIP* ISO/IEC 80001-5-1(:2021-Q4)
  Health informatics — Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software – Part 5: Security – Sub-Part 5-1: Activities in the Product Lifecycle

- NWIP* IEC TR 60601-4-5(:2020-Q2)
  Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices

- NWIP* ISO/IEC 81001-1(:2020-Q4)
  Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms

Update* IEC 62304 ED2 (:2020-Q2)

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

THANK YOU!

www.globalditta.org

Follow us on @DITTA_online

COCIR Advancing Healthcare · JIRA · Medtech Canada · MITA · THAIMED · IMEDA · 中国医疗器械行业协会 China Association for Medical Devices Industry · abimed · Kmdica Korea Medical Devices Industrial Coop. Association · ITAC INFORMATION TECHNOLOGY ASSOCIATION OF CANADA