

PHILIPS

www.philips.com

Developments of eHealth security in standards and regulations

Ben Kokx

Director Product Security, Philips

Normkonferansen 2019

innovation  you





Healthcare is increasingly depended on ICT



Systems are increasingly connected



Increase in Health-IT services



Digital transformation also increases security risks



Safety versus Security



Security
related risk

Security risk
with safety
impact

Safety
related risk

Safety versus Security



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Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE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 is for use by industry and FDA staff in connection with the guidance.

December 12, 2019

You should consult the guidance and supporting information regarding the guidance within 90 days of publication in the Federal Register for the most current information for the guidance. The guidance is available on the Center for Devices and Radiological Health (CDRH) website at <https://www.fda.gov/oc/ohrt/ohrt-guidance>. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>.

For questions regarding the guidance, contact the Center for Devices and Radiological Health (CDRH), Food and Drug Administration, 1085 North Mountain Ave., 303g, 28th St., N.E., Atlanta, Georgia 30329. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>.

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 Regulatory Evaluation and Research

Government of Canada
Ministère de la Santé
Health Canada

Medical device cyber security guidance for industry

Version 1.0, July 2019

TGA

Fda

Guidance for Industry: Cybersecurity of Medical Devices

This guidance is for use by industry and FDA staff in connection with the guidance.

December 12, 2019

For questions regarding the guidance, contact the Center for Devices and Radiological Health (CDRH), Food and Drug Administration, 1085 North Mountain Ave., 303g, 28th St., N.E., Atlanta, Georgia 30329. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>.

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 Regulatory Evaluation and Research

ANSM

Cyber Security Requirements for Network Connected Medical Devices

This guidance is for use by industry and FDA staff in connection with the guidance.

December 12, 2019

For questions regarding the guidance, contact the Center for Devices and Radiological Health (CDRH), Food and Drug Administration, 1085 North Mountain Ave., 303g, 28th St., N.E., Atlanta, Georgia 30329. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>.

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 Regulatory Evaluation and Research

Guidance Document:

Pre-market Requirements for Medical Device Cybersecurity

July 2019

Canada

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This guidance is for use by industry and FDA staff in connection with the guidance.

December 12, 2019

For questions regarding the guidance, contact the Center for Devices and Radiological Health (CDRH), Food and Drug Administration, 1085 North Mountain Ave., 303g, 28th St., N.E., Atlanta, Georgia 30329. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>.

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 Regulatory Evaluation and Research

IMDRF

DRAFT DOCUMENT

Intermarket Stock of Medical Device Cybersecurity

This document is for use by industry and FDA staff in connection with the guidance.

December 12, 2019

For questions regarding the guidance, contact the Center for Devices and Radiological Health (CDRH), Food and Drug Administration, 1085 North Mountain Ave., 303g, 28th St., N.E., Atlanta, Georgia 30329. For more information, see the [CDRH website](https://www.fda.gov/oc/ohrt/ohrt-guidance) at <https://www.fda.gov/oc/ohrt/ohrt-guidance>.

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 Regulatory Evaluation and Research

ANSM

RAPPORT

ANSM's Guidance

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 T1 meeting on 20th September

DG GROW Task Force on MD Cybersecurity

Page 2 of 6

In development →

Australian Guidance

- 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



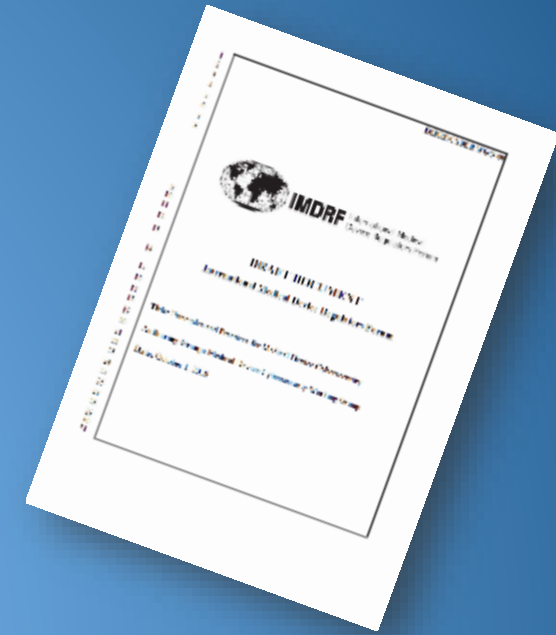
Canadian Guidance

- 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

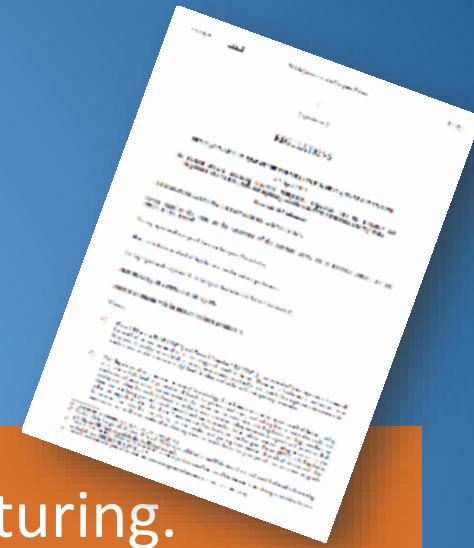


DRAFT IMDRF Principles and Practices for Medical Device Cybersecurity

- 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, e.g. ISO 80001



European Medical Device Regulation Security specific requirements



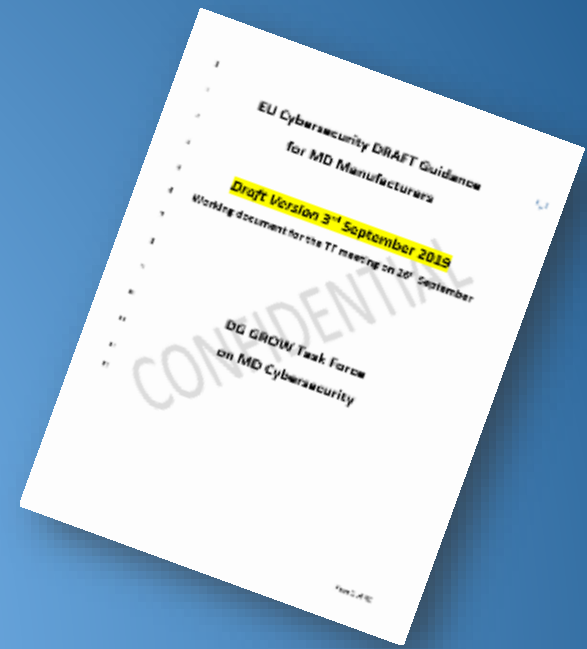
Organization: State of the art information security manufacturing.

Annex I.17.2

Device: Environment Annex I.14.2.(d)	Device: Repeatability Annex I.17.1	Device: Reliability Annex I.17.1	Device: Performance Annex I.17.1	Device: Access Control Annex I.17.4 Annex I.18.8	Labeling: security measures network characteristics Annex I.17.4 Annex I.23.4(ab)
--	--	--	--	---	--

DRAFT MDR & 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
 - Security requirements for the operating environment
 - Documentation
 - Post market surveillance and vigilance
- References to ISO 80001 series, IEC 62443, 27001, 14971 and 31000
- Expected to be approved during the MDCG meeting, December 13



Consistent items across regulations

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





Do we manage on Risk or on Compliance?

Product compliance to which security standard? A view on the various European requirements

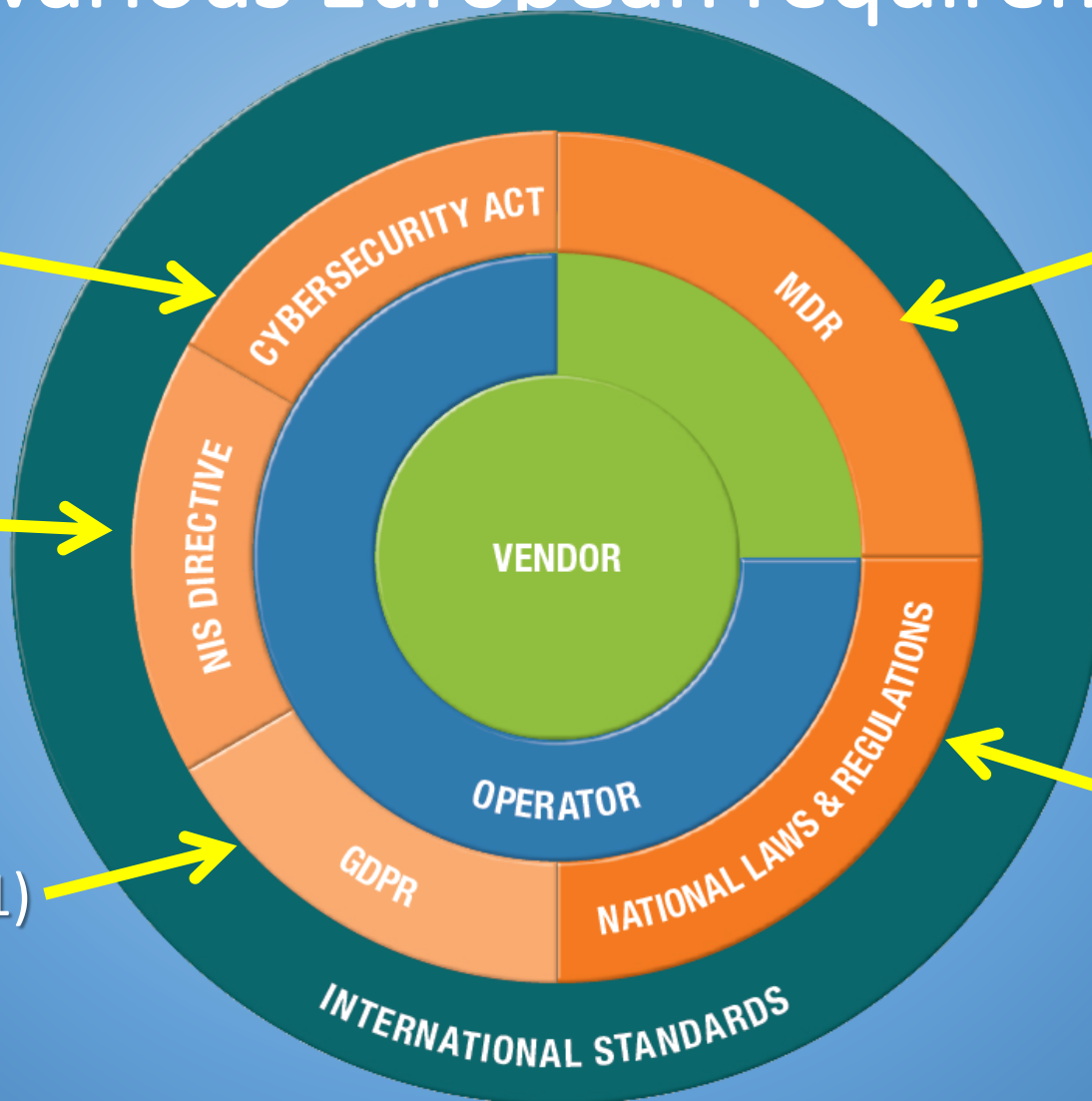
ISO 27000 series,
ISO 15408, and... ?

ISO 15408, IEC 62433,
ISO 27000 series, and... ?

ISO 27000 series (new 27701)

.....?
(IEC 80001-2-8,
IEC 62443 ?)

National standards,
ISO 27000 series,
and... ?





Security requirements for the operating environment



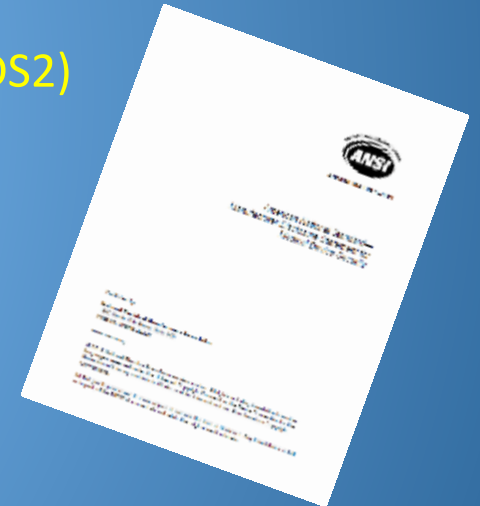
Shared responsibility

Healthcare specific security standards

- There are security elements in several medical device standards (e.g. IEC 60601-1 Ed 3.1) but there are no specific security standards which are directly applicable to medical devices or medical software.
- Only a few standards focus on healthcare security but mainly address the Health Delivery Organizations, e.g.:
 - ISO 80001 series – Application of risk management for IT-networks incorporating medical devices
 - ISO 27799 – Information security management in health using ISO/IEC 27002

ISO / IEC 80001 series

- 80001-1 Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities
- 80001-2-1 Step-by-Step Risk Management
- 80001-2-2 Communicating Security Needs, Risks & Controls
 - **Manufacturers Disclosure Statement for Medical Device Security (MDS2)**
- 80001-2-3 Wireless Guidance
- 80001-2-4 HDO Implementation Guidance
- 80001-2-5 Distributed Alarm Systems
- 80001-2-6 Responsibility Agreements
- 80001-2-7 Conformance Self-assessment Guidance
- 80001-2-8 Mapping Security Controls to the 19 Capabilities of 80001-2-2
- 80001-2-9 Security Assurance Case for the 19 Capabilities of 80001-2-2



“Base” security standards

There are a large number of security standards from (inter)national Standards Development Organisations and many other organisations, e.g.:

- ISO 27000 series – Generic Information security
- IEC 62443 series – Industrial control systems security
- National Institute of Standards and Technology (NIST) – Risk Management / Cybersecurity frameworks
- Open Web Application Security Project (OWASP)
- etc..

There is not a single silver bullet!

Selecting the best fit:

- Security has to be balanced against safety and performance
- Security has to fit the intended use and intended operating environment
- Security has to fit the used technologies
- Operational Security versus Information Security
 - IT → Confidentiality, Integrity, Availability
 - OT → Availability, Integrity, Confidentiality

ISO/TC215 and IEC/TC62 development activities related to MDD/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) [*Based on IEC 62443-4-1*]

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) [*Based on IEC 62443-4-2*]

Medical electrical equipment – Part 4-5 Guidance and interpretation – Safety related technical security specifications for medical devices

NWIP ISO/IEC 81001-1(:2020-Q4)

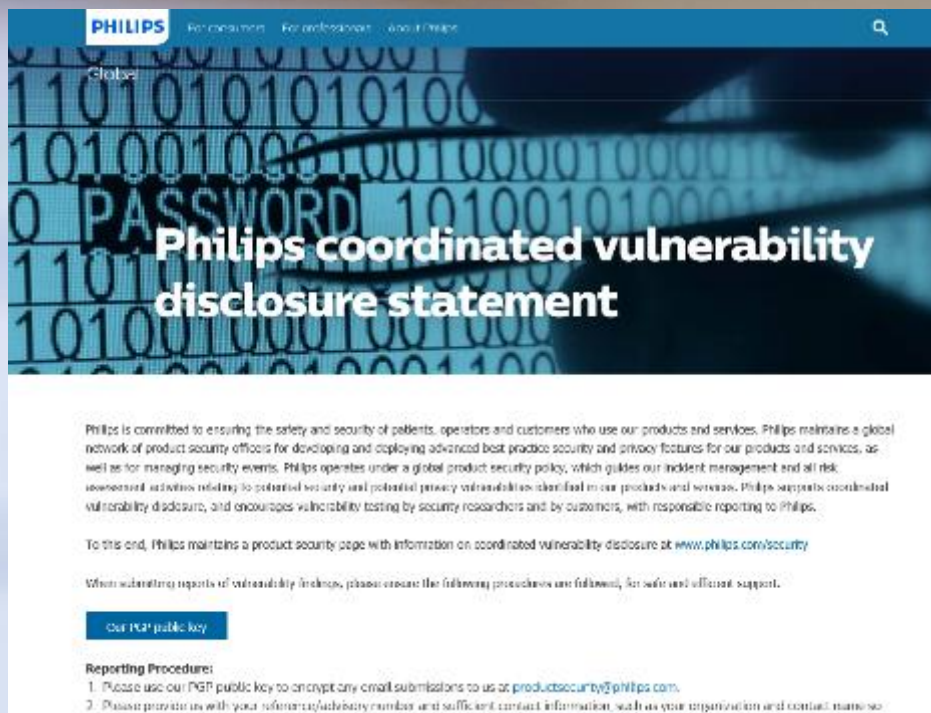
Health informatics — Health software and health IT systems safety, effectiveness and security — Part 1: Foundational principles, concepts and terms

NWIP ISO/IEC 82034-2(:2021-Q2) [*Started as a CEN/TC 251 project, based on BSI PAS 277*]

Health informatics —Quality and reliability criteria for health and wellness apps




Coordinated Vulnerability Disclosure



The screenshot shows the top portion of a webpage. At the top left is the Philips logo and navigation links for 'For consumers', 'For professionals', and 'About Philips'. Below the navigation is a search icon. The main header features a background of binary code (0s and 1s) with the word 'PASSWORD' in a stylized font. The main heading reads 'Philips coordinated vulnerability disclosure statement'. Below this, there is a paragraph of text explaining Philips's commitment to safety and security, its global network of product security officers, and its policy on vulnerability disclosure. A link is provided for more information: www.philips.com/security. A section titled 'Our PGP public key' is visible, followed by a 'Reporting Procedure' section with two numbered steps: 1. Please use our PGP public key to encrypt any email submissions to us at: productsecurity@philips.com. 2. Please provide us with your reference/advisory number and sufficient contact information, such as your organization and contact name.

ISO/IEC 29147; Vulnerability Disclosure

ISO/IEC 30111; Vulnerability Handling process

- 
- A man in a blue shirt is working inside a large, circular, metallic structure, possibly a medical scanner or industrial machine. The structure is composed of many parallel metal bars, creating a tunnel-like appearance. The man is looking towards the right, and his hands are near the inner wall of the structure. The background is slightly blurred, showing other parts of the facility.
- Determine market specific requirements for product and of the environment
 - Develop your state of the art
 - Address the total lifecycle

Questions?



Security



Fast response



In Control



Minimized risk



There are some viruses doctors can't treat.