HORIZON-HLTH-2022-IND-13-01

NEMECYS [101094323]: New Medical Cybersecurity assessment and design solutions

NEMECYS
New Medical Cybersecurity and design Solutions

D1.1 Initial systematic review of documentation

Project Reference No	NEMECYS – 101094323
Deliverable	D1.1 Systematic review of documentation (initial)
Work package	WP1: Systematic review and recommendations
Type	R - Document, report
Dissemination Level	PU - Public (fully open)
Date	27/06/2023
Status	Final v1.0
Editors	Salvador García (MS), Susana de Gea (MS), and Vicent Moncho (MS)
Contributors	Nektaria Kaloudi (SINTEF), Christos Androutsos (UoI), George Rigas (PDN), George Zissis (ATC), Stephan Proennecke (DB)
Reviewers	Steve Taylor (UoS) and Brian Pickering (UoS)
Document description	A comprehensive review based on desk research of current regulations, guidelines, standards, and best practices regarding cybersecurity of medical devices, identifying the relevant stakeholders for the included measures.

Disclaimer

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323, by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee grant numbers 10065802, 10050933 and 10061304, and by the Swiss State Secretariat for Education, Research, and Innovation (SERI).

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	26/05/2023	Complete draft	Salvador García, Susana de Gea, and Vicent Moncho
v0.2	31/05/2023	First review	Brian Pickering
v0.3	12/06/2023	Review	Steve Taylor
v0.4	14/06/2023	Updated after review	Salvador García, Susana de Gea, and Vicent Moncho
v1.0	27/06/2023	Final version	Karin Bernsmed

Executive Summary

The increasing use of connected medical devices within the healthcare system has enabled patient monitoring, diagnostics, and treatment. However, the adoption of new technologies conveys several challenges.

With this systematic review we aim to provide an overview of the current legislation, guidelines, best practices, and standards applied to cybersecurity of connected medical devices. The review offers a synthesis of the documentation including legislation within the European Union and the United States, together with guidelines from European agencies and international groups.

As extracted from the analysis, most of the documentation is dedicated to encouraging manufacturers to address the cybersecurity of connected medical devices. Only a few documents are focused on how healthcare providers and users need to deal with the cybersecurity of connected medical devices. Moreover, the measures to address the cybersecurity of medical devices focus on the device itself rather than the whole environment.

The gaps and challenges identified in this initial review will be further analyzed and discussed in the upcoming deliverable D1.2 "Systematic review of documentation (final)".

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Abbreviation	Definition
AAMI	Association for the Advancement of Medical Instrumentation
ANSM	Agence Nationale de Sécurité du Médicament et des Produits de Santé
BSI	Federal Office for Information Security
CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DSS	Decision Support Systems
ENISA	European Union Agency for Cybersecurity
EU	European Union
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IMDRF	International Medical Device Regulators Forum
ISAO	Information Sharing Analysis Organization
ISO	International Organization for Standardization
IT	Information Technology
IVDR	In Vitro Diagnostic Medical Devices Regulation
JSP	Joint Security Plan
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation
NEMECYS	New Medical Cybersecurity Assessment and Design Solutions
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
TGA	Therapeutic Goods Administration
TIR	Technical Information Report
TPLC	Total Product Life Cycle
TR	Technical Report
UL	Underwriters Laboratories
US	United States
WP	Work Package

1 Introduction

The New Medical Cybersecurity assessment and design solutions (NEMECYS) is a project funded by Horizon Europe EU's funding programme for research and innovation. The project aims to address the cybersecurity of connected medical devices and in vitro diagnostic devices connected to the internet.

1.1 Purpose and scope

The purpose of this document is to produce a comprehensive review by summarizing and synthesizing the existing regulations, guidelines, best practices, and standards for the cybersecurity of connected medical devices. The document focuses on legislation within the EU and US; nevertheless, regarding guidelines and best practices we have considered the main European agencies and international groups together with the United States.

This review is addressed to all the stakeholders involved in the total product life cycle of medical devices and in vitro medical devices: manufacturers, systems integrators, and operators.

1.2 Approach for WP1 and relation to other work packages and deliverables

The objective of WP1 is to identify gaps and requirements from the current standards, guidelines and best practices applied to cybersecurity of connected medical devices. In this first deliverable, an identification of the relevant stakeholders for the measures included in the documentation is provided, together with results from the initial analyses and interviews.

The upcoming deliverable from WP1: Deliverable D1.2 "Systematic review of documentation (final)" will extend these initial results with workshops and interviews with the stakeholders in the healthcare sector to offer an overview of the adherence to current guidance, and document the gaps detected.

Furthermore, a set of recommendations to cover the gaps will be provided with feedback from the experiences in WP2 and WP3, where risk benefit analysis schemes and toolboxes will be developed.

1.3 Structure of the deliverable

The deliverable is structured as follows:

- Section 2 describes the methodology followed to produce the review, including the documentation identification strategy, the inclusion and exclusion criteria together with the data extraction.
- Section 3 provides a synthesis of the documentation, including summaries of the legislation, guidelines and best practices and an overview of the standards addressing cybersecurity of medical devices together with an identification of the stakeholders affected by the included measures.
- Section 4 provides the results of the interviews with the stakeholders of the project.
- Section 5 presents the conclusions of the review.

2 Methodology

2.1 Documentation search and evaluation

To ensure the relevance and quality of the documentation included in the review, the following criteria were applied:

2.1.1 Documentation identification

We conducted a systematic review following the Guidance on Conducting a Systematic Literature Review [1]. To find documentation, we based our research on backward searching from the Guidance on Cybersecurity for Medical Devices [2] to identify applicable regulations, standards, best practices and guidelines out of the references of this document. We then continued using backward searching out of the references of these documents. We present the results of this search in Annex I.

Backward searching is a widely adopted technique in academic research to find existing literature and discover additional sources. The search strategy from this systematic review of documentation differs from the one used in Deliverable D3.1 "Requirements for Toolboxes in the Healthcare Sector" because the objective of our systematic review of documentation is to provide a comprehensive report on the existing regulations, standards, guidelines, and best practices for cybersecurity of connected medical devices. In contrast, the objective of D3.1 is to identify the challenges from the existing solutions for medical devices and connected devices from other industries and provide an aggregated list of requirements for the toolboxes.

2.1.2 Inclusion criteria

- Type of document: legislation, guideline, best practices, or standard.
- Legislation, guidelines and best practices focused on cybersecurity of medical devices.
- Standards recommended for the cybersecurity of medical devices.
- Documentation written in English.
- Documentation published between 2014 and 2023.
- Full text access.

2.1.3 Exclusion criteria

- Legislation not in force.
- Non-English documentation.
- Documents that do not directly address cybersecurity of medical devices.
- Unpublished manuscripts or grey literature.
- Full text not accessible.

2.2 Data extraction

We extracted the following information from each document:

- Title.
- Type of document.
- Publication year.
- Author, and Stakeholder.

3 Synthesis of the documentation

3.1 Legislation

Legislation provides a structured and regulatory framework for the enforcement of cybersecurity measures and the imposition of penalties or sanctions for non-compliance. It defines the authority of regulatory bodies responsible for overseeing cybersecurity practices, imposing fines or other legal actions against infringements.

3.1.1 EU

3.1.1.1 General Data Protection Regulation

At the EU level, the 2016/679 GDPR [3] sets out the rules on how personal data relating to individuals in the EU must be processed by individuals, businesses or other organizations.

This regulation focuses on the protection, privacy, and security of personal data. It emphasizes the need for organizations to implement appropriate technical and organizational measures to ensure the security of the personal data they process. These measures are expected to address the risks associated with the processing of personal data and protect against unauthorized access, accidental loss, unauthorized destruction, or alteration of personal data. The GDPR encourages organizations to consider the state of the art when implementing security measures.

3.1.1.2 Medical Device Regulation and In Vitro Device Regulation

The EU 2017/745 MDR [4] and 2017/746 IVDR [5] provide a framework to ensure the safety and effectiveness of medical devices and in vitro medical devices. Both regulations set out general requirements for manufacturers to provide their medical devices with a secure design by providing a risk management system, a quality management system, as well as an updated post-market surveillance system.

The regulations require manufacturers to create post-market surveillance systems aiming to gather and analyse relevant data about quality, performance, and safety of a device throughout its entire lifetime to take preventive and corrective actions.

The MDR and IVDR refer to devices that incorporate software or for software that are devices in themselves to be developed and manufactured in accordance with the state of the art in terms of development life cycle, risk management, including information security, verification, and validation.

It also demands manufacturers to set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized access.

3.1.1.3 Cybersecurity Act

The EU 2019/881 Cybersecurity Act [6] sets out tasks for the European Union Agency for Cybersecurity (ENISA) and a framework to establish European cybersecurity schemes to ensure an adequate level of cybersecurity for information and communications technology products, services and processes.

The European Union Agency for Cybersecurity (ENISA) is entitled by this Act to enhance cooperation and information sharing, issue technical guides and best practices together with raising public awareness of cybersecurity risks.

The objectives of the framework are to protect data; to identify and document dependencies and vulnerabilities; to make the digital products secure by default and by design; and to ensure the provision of security updates.

3.1.1.4 NIS 2 Directive

The EU 2022/2555 NIS 2 Directive [7] disposes obligations for European Union Member States to adopt national cybersecurity strategies and to designate competent authorities, cyber crisis management authorities, and single points of contact on cybersecurity and Computer Security Incident Response Teams (CSIRTs).

This piece of regulation establishes cooperation at national level as well as a European cyber crisis liaison organization network (EU-CyCLONe) to support and coordinate the management of large-scale cybersecurity incidents and to ensure the exchange of relevant information between Member States and Union Agencies.

This Directive requires ENISA to establish a European vulnerability database as well as a registry of entities.

The Directive addresses healthcare providers together with medical device and in vitro medical device manufacturers and requires their management bodies to follow training and encourages them to offer similar training to their employees on a regular basis. The Directive encourages healthcare providers and medical device manufacturers to voluntarily exchange relevant cybersecurity information as well as recommendations regarding the configuration of cybersecurity tools to detect cyber attacks.

It also requires Member States to ensure that essential and important entities take risk management measures considering the state of the art and European and international standards.

Finally, the Directive requires specific measures to protect network and information systems together with the physical environment. It also requires Member States to impose penalties and administrative fines in respect of infringements of this Directive.

3.1.2 US

At the US level, the legislation that addresses medical devices is the Medical Device Amendments Act [8] that was introduced in 1976 to provide safety and effectiveness of medical devices. Furthermore, the legislation that covers data protection is HIPAA [9] that was signed into law in 1996 and addresses various aspects of healthcare, including the privacy and security of protected health information.

However, both acts were excluded based on the inclusion criteria for the review. Accordingly, we focused on the Cybersecurity Enhancement Act of 2014 and Consolidated Appropriations Act of 2023, cited in the next two sections.

3.1.2.1 Cybersecurity Enhancement Act of 2014

The Cybersecurity Enhancement Act of 2014 [10] is a United States Public Law aimed to enhance cybersecurity. It encourages though does not mandate public-private collaboration on cybersecurity by requiring the director of the National Institute of Science and Technology (NIST) to take part in the development of standards and procedures to reduce cyber risks to critical infrastructure.

It also sets out the grounds for a cybersecurity research and development strategic plan with the aid of different agencies within the US, a national cybersecurity awareness and education program as well as the development of international technical standards related to information system security.

3.1.2.2 Consolidated Appropriations Act of 2023

The section 3305, Ensuring Cybersecurity of Medical Devices of the Consolidated Appropriations Act of 2023 [11] requires manufacturers of medical devices to submit to the Food and Drug Administration (FDA) a plan on post market cybersecurity vulnerabilities and exploits, to provide reassurance that the device is secure, supply patches and updates for cybersecurity threats, and to comply with the requirements set by the FDA through regulation.

3.2 Guidelines and best practices

Guidelines and best practices refer to a set of recommended principles, standards or instructions that serve as a reference for manufacturers, systems integrators, operators, healthcare providers, and/or users.

To provide more detailed guidance on what legislators and experts had issued about cybersecurity on medical devices we present a summary of the guidelines and best practices included in the review.

3.2.1 MDCG - Guidance on Cybersecurity for medical devices (2019)

The Medical Device Coordination Group (MDCG) issued the Guidance on Cybersecurity for medical devices [2] to help manufacturers meet the requirements of the European Union Regulations on Medical Devices (2017) [4] and In Vitro Medical Devices (2017) [5].

The document focuses on how to interpret what is stated in the MDR and IVDR regarding cybersecurity with specific examples.

The key points of this guidance are:

- Secure design: the guidance emphasizes the importance of incorporating security features and functionalities into the design of medical devices. Manufacturers should use secure coding practices and implement security controls such as encryption and access controls.
- Security risk management throughout the device's lifecycle: manufacturers should conduct a risk assessment to identify cybersecurity threats and vulnerabilities and implement appropriate security measures to mitigate the risks.

- IT requirements: such as the GDPR, physical security and patch management.
- Documentation and instructions for use: the guidance requires manufacturers to document the cybersecurity features and functionalities of their devices.
- Post-market surveillance and vigilance: including measures for investigating and reporting cybersecurity incidents and taking appropriate corrective actions.

3.2.2 IMDRF - Principles and practices for Medical Device Cybersecurity (2020)

The International Medical Device Regulators Forum (IMDRF) have produced guidance [12] for all stakeholders involved in the cybersecurity of medical devices including in vitro medical devices. This document focuses exclusively on medical device cybersecurity regarding the potential for patient harm, it does not consider other types of harm such as data privacy breaches.

The document emphasizes the importance of cybersecurity as a shared responsibility among all stakeholders: medical device manufacturers, healthcare providers, users, regulators, and vulnerability finders. It encourages all stakeholders to "*harmonize their approaches to cybersecurity across the entire life cycle of the medical device*".

On the one hand, the guideline gives pre-market considerations for manufacturers to address cybersecurity considerations during the design and development of a medical device prior to market entry. It gives examples referring to international standards bodies such as ISO, AAMI, IEC, NIST, OWASP and JSP.

On the other, the document also provides post-market considerations to all stakeholders including healthcare providers, patients, and manufacturers. The guideline offers a series of processes that should be applied by healthcare providers in terms of IT considerations as well as training among all users to prevent cybersecurity incidents.

Moreover, the guideline emphasizes the importance of information sharing between regulators, medical device manufacturers, healthcare providers and users. It especially encourages manufacturers to adopt coordinated vulnerability disclosure procedures.

3.2.3 ENISA - Procurement Guidelines for Cybersecurity in Hospitals (2020)

The Procurement Guidelines for Cybersecurity in Hospitals [13] issued by ENISA provides a set of tools and good practices to ensure that cybersecurity objectives are met in the procurement process.

The measures included in this guideline are addressed to hospital procurement officers and CIOs. This guide emphasizes the importance of risk management throughout the entire procurement lifecycle. It provides good practices by dividing the phases of the procurement and giving examples of how to address cybersecurity risks.

It also suggests that healthcare organizations should evaluate vendors' cybersecurity measures before selecting them for procurement, requesting information on their security policies, practices, and

certifications. The guideline also suggests that healthcare organizations should conduct security testing on the products and services they provide, as well as prioritize cybersecurity awareness and training for their staff.

3.2.4 ANSM - Cybersecurity of medical devices integrating software during their life cycle (2019)

The Cybersecurity of medical devices integrating software during their life cycle [14] is a guideline issued by the Agence nationale de sécurité du médicament et des produits de santé (ANSM) that gives an initial general explanation of what MDR [4] and IVDR [5] stipulate in terms of general requirements and highlights the difference between safety and security. From then on, the document provides specific guidelines on how to apply cybersecurity on medical devices by presenting standards and their application together with examples.

It gives recommendations on five key areas based on the software life cycle:

- Software design.
- Medical Device software development.
- Initialization.
- Post-market management.
  End of life for the Medical Device software.

3.2.5 eHealth Suisse - Guide for app developers, manufacturers, and distributors (2020)

The Guide for app developers, manufacturers and distributors [15] issued by eHealth Suisse focuses on software (in the form of an app) as a medical device. The guideline provides the regulatory framework in Switzerland and explains how to address cybersecurity.

The document states that security needs to be addressed from the design stage providing a list of typical points, then through a risk management process also giving examples and referring to international standards that are mandatory, and finally refers to verification and validation.

This guide also emphasizes that manufacturers have obligations after the software has been developed, such as secure updates, response to security risks and product surveillance system.

3.2.6 BSI – Cyber security Requirements for Network-Connected Medical Devices (2018)

The Bundesamt für Sicherheit in in der Informationstechnik (BSI) issued this guideline [16] to provide manufacturers of medical devices with best practices regarding cyber security requirements. This document refers to the now obsolete Council Directive 93/42/EEC concerning medical devices from 1993 [17] and presents the requirements as questions directed at manufacturers on how to address cybersecurity.

The guide is divided into two. On the one hand it sets out organizational measures regarding product life cycle and communication. The document states that "*establishing a secure development life cycle*

fundamentally improves the security of a product" and for that makes a series of specific questions about cyber security threat and risk analyses, vulnerabilities, security analyses, patches, and updates. It also focuses on the importance of communicating information regarding cybersecurity and safety-incident reporting processes.

On the other hand, the document lists product features regarding cybersecurity recommendations for all operating modes, product configuration and maintenance operations and finally the technical documentation.

3.2.7 Health Canada - Pre-market Requirements for Medical Device Cybersecurity (2019)

Health Canada issued this guidance [18] to medical device manufacturers regarding improvement of cybersecurity. However, it also acknowledges that it is a shared responsibility between all the stakeholders.

The guidance states that manufacturers are responsible for potential cybersecurity risks throughout the lifecycle of the product. It presents the NIST document "Framework for Improving Critical Infrastructure Cybersecurity" (2018) [19] as best practices to guide manufacturers in cybersecurity activities.

Health Canada identifies 5 main functions within NIST:

- Identify cybersecurity risks.
- Design controls to limit risks.
- Detect when a device has been compromised due to a cybersecurity event.
- Respond to a cybersecurity event.
- Restore the device.

This guidance presents a cybersecurity strategy by secure design, risk management, and verification and validation testing.

Moreover, it emphasizes the importance of addressing emerging risks through patching, information sharing, post-market management and vulnerability disclosure.

Health Canada requires specific elements to assess cybersecurity for Class III and Class IV medical device license and recommends conducting cybersecurity risk management processes in parallel to the safety risk management process.

3.2.8 United States Food and Drug Administration (FDA)

The FDA has issued several documents with recommendations on Cybersecurity in Medical Devices, here we focus on premarket submissions and post market management following the inclusion and exclusion criteria established for the review.

3.2.8.1 Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (2022)

This draft guidance [20] is addressed to medical device manufacturers in the framework of premarket submissions, even though the FDA recognizes that medical device security is a shared responsibility among all the stakeholders: healthcare facilities, patients, healthcare providers and manufacturers.

This guideline presents at the beginning the main principles to improve the cybersecurity of a medical device by establishing a quality system through design controls. It recommends a series of security objectives to meet during the design process and encourages manufacturers to have a secure product development framework to meet the quality system regulations requirements. It also stresses the importance of transparency via providing labelling and documentation so device users can have access to information relevant to the cybersecurity of the device.

The FDA explains in more detail why a secure product development framework is useful in terms of cybersecurity and compares it with other frameworks and international standards. This framework brings up security risk management, security architecture and cybersecurity testing to be addressed.

Finally, the document refers to cybersecurity transparency through labelling recommendations and vulnerability management plans. The FDA also gives detailed descriptions of security control categories together with recommendations on how to address them.

3.2.8.2 Postmarket Management of Cybersecurity in Medical Devices (2016)

This guidance [21] issued by the FDA on 2016 is aimed to manufacturers on how to address cybersecurity on the post market stage. The FDA acknowledges that cybersecurity risk management is a shared responsibility among stakeholders.

The document is divided into general principles that present premarket and post market considerations along with defining safety and essential performance. Moreover, it focuses on risk management as an ongoing process to identify hazards and assess the risk of patient harm. To assess the exploitability of the cybersecurity vulnerabilities the FDA suggests manufacturers consider using a cybersecurity vulnerability assessment tool and provides examples of the most common ones.

The guide presents the difference between controlled and uncontrolled risk with examples and recommendations for actions to address the vulnerabilities. It also gives recommended content to include in premarket approval periodic reports and when a manufacturer is an active participant in an Information Sharing Analysis Organisation (ISAO).

Finally, the FDA recommends the Cybersecurity Framework [19] to become a part of the cybersecurity risk management program for manufacturers and presents the elements necessary to provide an effective post market cybersecurity program:

- Identify
- Protect/Detect
- Protect/Respond/Recover

- Risk mitigation of safety and essential performance

3.2.9 Therapeutic Goods Administration (TGA), Australia

The Therapeutic Goods Administration (TGA) in Australia issued in November 2022 two guidance documents regarding medical device cybersecurity, one is addressed to manufacturers of medical devices and the other one to users including consumers, health professionals and operators.

3.2.9.1 Medical Device Cyber Security Guidance for Industry (2022)

This TGA Guidance [22] is addressed to medical device manufacturers on how the TGA interprets regulations. In the Australian market a medical device cannot be supplied unless it is included in the Australian Register of Therapeutic Goods where there is an established process of premarket considerations, market authorization, post market management and end-of-life.

In Australia manufacturers must demonstrate compliance with the Essential Principles, where the requirements are set out to demonstrate the minimization of the risks associated with the design, long-term safety and use of the device. A Total Product Lifecycle (TPLC) approach for risk management is required.

TGA requires that the Essential Principles are met by applying accepted best practice regarding quality management systems and risk management frameworks. The guidance provides considerations on how to address cybersecurity risks referring to the Essential Principles.

On the one hand, the document offers premarket guidance on the regulatory requirements addressing secure by design and quality by design approaches. Moreover, it presents potential strategies for risk management, the provision of information for users, and modularized design architecture. Additionally, it encourages manufacturers to implement cybersecurity assessment and penetration testing, as well as trusted access measures, and secure updating.

On the other hand, the guide offers post market guidance emphasizing the requirement for an ongoing cybersecurity risk management, and cybersecurity threat and risk response. Moreover, the document reminds manufacturers that they must demonstrate information gathering on cybersecurity vulnerabilities.

3.2.9.2 Medical Device Cyber Security Information for Users (2022)

The Australian guidance for users [23] makes a distinctive set of guidelines depending on to whom it is addressed. It is divided into four different users: patients and consumers, health and medical professionals, small business operators, and large-scale service providers.

The TGA presents a series of questions that patients and consumers should ask health professionals regarding potential cybersecurity risks. Moreover, the guideline refers to privacy, gives best practices for making strong passphrases, alerts on suspicious messaging, and explains the importance of updating software.

For health and medical professionals, the guidance emphasizes the need to obtain from the medical device manufacturer the information regarding cybersecurity risks, and what they need to understand from manufacturers to communicate it to patients.

For small business operators, the TGA refers to the Essential Eight, which are mitigation strategies to prevent malware delivery and execution, to limit the extent of cybersecurity incidents, and to recover data and system availability.

The guidance encourages large-scale service providers to have a risk management strategy and gives recommendations on how to apply defence-in-depth approaches. The TGA urges service providers to facilitate the environment for cross-functional collaboration between biomedical, clinical support and IT teams enabling collaborative procurement, and to raise security awareness through cybersecurity training.

3.3 Standards

Standards refers to a documented set of specifications, requirements, or practices that serve as a baseline for ensuring consistent and reliable measures. Standards provide a common framework for manufacturers, and healthcare providers to adhere to in order to establish a secure environment for connected medical devices.

The following table represents an overview of the standards used to meet requirements for cybersecurity of medical devices.

Table 1: Overview of standards.

Standard	Title
AAMI TIR 36	Validation of software for regulated processes
AAMI TIR 57	Principles for medical device security— Risk management
AAMI TIR 97	Principles for medical device security – Postmarket Risk Management for Device Manufacturers
AAMI/UL 2800	Safety and security requirements of interoperable medical systems
ANSI/IEC/ISA 62443-4-1	ANSI/ISA-62443-4-1: Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements
ANSI/CAN/UL 2900-1	Software Cybersecurity for Network-Connectable Products. Part 1: General requirements.
ANSI/CAN/UL 2900-2-1	Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems
ANSI/UL 2900	Software Cybersecurity for Network-Connectable Products
IEC 60601-1 BS EN 60601-1	Medical electrical equipment – Part 1: General requirements for basic safety and essential performance
IEC/TR 60601-4-5	Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications
IEC 62304	Medical device software — Software life cycle processes

Standard	Title
BS EN 62304	
IEC 62366-1	Medical devices — Part 1: Application of usability engineering to medical devices
IEC 62443-4-1	Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.
IEC 62443-4-2	Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.
BS EN 50159	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
BS EN IEC 80001	Application of risk management for IT-networks incorporating medical devices - Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software
IEC 80001-1	Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities
IEC TR 80001-2-2	Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls
ISO/TR 80001-2-7	Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
IEC TR 80001-2-8	Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2
ISO/IEC 80001-5-1	Application of Risk Management for IT networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.
IEC 82304-1	Health Software Part 1: General requirements for Product Safety
IEEE 802.1X	Port-Based Network Access Control
ISO 9001	Quality Management Systems
ISO/TR 11633	Health informatics - Information security management for remote maintenance of medical devices and medical information systems
ISO 13485	Medical devices – Quality management systems – Requirements for regulatory purposes
ISO 14971	Medical devices — Application of risk management to medical devices
ISO/IEC 15802	Information technology - Telecommunications and information exchange between systems. Local and metropolitan area networks. Common specifications - Part 3: Media access control (MAC) bridges
ISO/TR 24971	Medical devices – Guidance on the application of ISO 14971

Standard	Title
ISO/IEC 27000	Information Technology — Security techniques — Information security management systems (ISMS) — Overview and vocabulary
ISO/IEC 27001	Information Technology – Security techniques – Information Security management Systems – Requirements
ISO/IEC 27005	Information Technology - Security Techniques -Information security risk management
ISO 27018	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27032	Information technology — Security techniques — Guidelines for cybersecurity
ISO/IEC 27035-1	Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management
ISO/IEC 27035-2	Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
ISO 27799	Health Informatics – Information security management in health
ISO/IEC 29147	Information Technology – Security Techniques – Vulnerability Disclosure
ISO/IEC 30111	Information technology — Security techniques — Vulnerability handling processes
ISO 31000	Risk management — Guidelines
ISO/TR 11633	Health informatics - Information security management for remote maintenance of medical devices and medical information systems
ISO/TR 11633-2	Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 2: Implementation of an information security management system (ISMS)

3.4 Analysis of the documentation

The following table identifies the relevant stakeholders for the measures included in each document.

Table 2: Impacted stakeholders.

DOCUMENT	DEVICE MANUFACTURERS	HEALTHCARE PROVIDERS
General Data Protection Regulation (EU)	✓	✓
Medical Device Regulation (EU)	✓	
In Vitro Diagnostic Medical Device Regulation (EU)	✓	
Cybersecurity Act (EU)		✓
NIS 2 Directive (EU)	✓	✓
Cybersecurity Enhancement Act (US)		✓
Consolidated Appropriations Act (US)	✓	
MDCG - Guidance on Cybersecurity for medical devices	✓	✓
IMDRF - Principles and practices for Medical Device Cybersecurity	✓	✓

DOCUMENT	DEVICE MANUFACTURERS	HEALTHCARE PROVIDERS
ENISA - Procurement Guidelines for Cybersecurity in Hospitals		✓
ANSM - Cybersecurity of medical devices integrating software during their life cycle	✓	
eHealth Suisse - Guide for app developers, manufacturers and distributors	✓	
BSI - Cyber security Requirements for Network-Connected Medical Devices	✓	
Health Canada - Pre-market Requirements for Medical Device Cybersecurity	✓	
FDA - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	✓	
FDA - Postmarket Management of Cybersecurity in medical devices	✓	
TGA - Medical Device Cyber Security Guidance for Industry	✓	
TGA - Medical device cyber security information for users		✓

Of the 18 documents included in the review, 14 are addressed to device manufacturers and 8 to healthcare providers. Only 3 of the documents focus on measures for healthcare providers. This leads us to the conclusion that the main effort from the administration is yet focused on the cybersecurity of the device itself and does not take into account the whole environment where the devices are going to be deployed. It also leaves healthcare providers without the necessary tools to face cybersecurity of connected medical devices.

Even though most of the guidelines and best practices acknowledge that cybersecurity is a shared responsibility between all the stakeholders, the focus in 10 out of the 18 documents is only on the measures needed to be taken by manufacturers. Nevertheless, the Australian Government through the Therapeutic Goods Administration do present two different guidelines for industry [22] and for users [23]. With that distinct guideline, the TGA provides users, including healthcare providers, with specific measures on cybersecurity for connected medical devices. Moreover, ENISA also issued the Procurement Guidelines for Cybersecurity in Hospitals [13] focused on providing hospital procurement officers and CIOs with good practices on how to address cybersecurity during the procurement process.

The following table shows in a range of low, medium, and high at which extent each document addresses eight aspects about cybersecurity of connected medical devices.

As we can extract from Table 3, in response to the escalating cybersecurity challenges, administrations have nowadays prioritized cybersecurity awareness and education as vital components of cybersecurity strategies. The EU NIS 2 Directive [7] and the US Cybersecurity Enhancement Act of 2014 [10] exemplify the commitment to promoting a cybersecurity aware society through specific initiatives.

Table 3: Cybersecurity aspects addressed by the documentation.

Document	Critical Infrastructure Protection	Cybersecurity Awareness and Education	Data Security	Incident Response and Management	Post Market Management	Quality Management	Risk Management	Secure Software Development
General Data Protection Regulation (EU)	Low	Low	High	Medium	Low	Low	Medium	Low
Medical Device Regulation (EU)	Low	Low	Low	High	High	High	Medium	Low
In Vitro Diagnostic Medical Device Regulation (EU)	Low	Low	Low	High	High	High	Medium	Low
Cybersecurity Act (EU)	Low	High	Low	Medium	Low	Low	Low	Low
NIS 2 Directive (EU)	High	High	Low	High	Low	Low	High	Low
Cybersecurity Enhancement Act (US)	High	High	Low	Low	Low	Low	Low	Medium
Consolidated Appropriations Act (US)	Low	Low	Low	Low	Medium	Low	Low	Low
MDCG - Guidance on Cybersecurity for medical devices	Low	Medium	Low	Medium	High	Low	High	Medium

Document	Critical Infrastructure Protection	Cybersecurity Awareness and Education	Data Security	Incident Response and Management	Post Market Management	Quality Management	Risk Management	Secure Software Development
IMDRF - Principles and practices for Medical Device Cybersecurity	Low	Medium	Low	High	High	Low	High	Medium
ENISA - Procurement Guidelines for Cybersecurity in Hospitals	Low	Medium	High	Medium	High	Low	Low	Low
ANSM - Cybersecurity of medical devices integrating software during their life cycle	Medium	Low	Low	High	Medium	Medium	High	Medium
eHealth Suisse - Guide for app developers, manufacturers and distributors	Low	Low	High	Medium	High	Medium	Medium	Medium
BSI - Cyber security Requirements for Network-Connected Medical Devices	Medium	Medium	Low	Medium	High	Low	High	Medium

Document	Critical Infrastructure Protection	Cybersecurity Awareness and Education	Data Security	Incident Response and Management	Post Market Management	Quality Management	Risk Management	Secure Software Development
Health Canada - Pre-market Requirements for Medical Device Cyber-security	Medium	Low	Low	Medium	Low	Low	High	Medium
FDA – Cyber-security in Medical Devi-ces: Quality System Considerations and Content of Premarket Submissions	Medium	Medium	Low	Low	Low	Medium	High	High
FDA – Post-market Management of Cyber-security in medical devices	Medium	Medium	Low	Low	High	Low	High	Medium
TGA - Medical Device Cyber Security Guidance for Industry	Low	Medium	Medium	Low	Medium	Medium	High	Medium

Document	Critical Infrastructure Protection	Cybersecurity Awareness and Education	Data Security	Incident Response and Management	Post Market Management	Quality Management	Risk Management	Secure Software Development
TGA - Medical device cyber security information for users	Low	High	Medium	Medium	Low	Low	Medium	Low

4 Results of the interviews with the stakeholders

The literature review has been performed using backward searching and taking into account the inclusion and exclusion criteria defined in the methodology, what came out of in the legislation, guidelines, best practices and standards synthesized in the previous section.

We also conducted interviews with different representative stakeholders that are part of the project with the aim of validating the results from the work performed in the review.

The interviewed stakeholders included:

1. One medical device manufacturer working in EU and US markets. This type of stakeholder represents the most common. They have to comply with the pre and post market regulations regarding both software and hardware elements, and have also to deal with the policies in place in the deployment scenario, usually the healthcare provider's premises.
2. One software developer producing software to be incorporated as part of medical devices from different vendors. This type of stakeholder is not a device manufacturer per se and has different obligations regarding legislation, since they don't have to comply directly with regulation. It will be the device manufacturer, the stakeholder obliged by the regulators to comply with the regulations.
3. One provider of apps and cloud solutions that seek to improve the usability of the medical data acquired from medical devices. These types of solutions are becoming more common as the medical devices become more connected and different providers can foresee market opportunities derived from the utilization of such data.
4. One healthcare provider with wide experience in connected medical devices.

As such, these represent four different and important stakeholders with different relationships to distributed medical devices: (1) the manufacturer responsible for the entire development and release to the market; (2) those producing one component (in this case software) for the device(s); (3) those producing service-level applications to exploit the data available from the devices; and (4) those who actually use such devices irrespective of components or manufacturer. We maintain, therefore, that these four types provide comprehensive coverage for those working in this market. Consequently, their views can be expected to reflect a broad perspective.

The main conclusions extracted from the interviews are that the documentation obtained through the backward search correspond to what the stakeholders pointed out as regulation, guidelines and standards used in their activities.

However, it has been identified that even though there are three different types of documentation, the focus of the stakeholders is on the standards, which are the only way they can show their compliance to the regulations.

Additional insights obtained from the interviews will be part of the study that will be performed in T1.2 (Adherence to guidelines) and T1.3 (Recommendations). Specifically, #1, the device manufacturer, has remarked that one of their main challenges is the difficulty of securing the required certifications in different markets, since there is a significant lack of a unified process. This is aligned with the conclusions included in D3.1 (section 4.3.2.) and to resolve the issue, they usually search for a representative/distributor in each new target market to assign them the task of identifying which regulations are mandatory, so they can identify what extra regulatory work needs to be done.

#2, the software developer, has stated that the list of standards and regulations observed are quite similar, but their relation with it is notably different: while stakeholder #1 has a legal obligation to comply with regulations, in this case they use it as a commercial strategy since the software is not a medical device per se and will be incorporated in a device. So, from their point of view, it is the device manufacturer who evaluates the suitability of the guidelines followed.

With stakeholder #3 we have an example of a new type of use of the medical data gathered by medical devices. It is no longer the case that isolation is the main security feature of medical devices. Nowadays, the devices are connected in the sense of a physical network connection or regarding the use of the data acquired. Industry has noticed the potential of this data to build new services above it, like Decision Support Systems, mobile apps, etc. And this new type of uses of the data is being performed by stakeholders that only need to comply with GDPR since the unique risks identified are related to confidentiality. But maybe it will be needed to explore how threats to the integrity or availability may affect the individuals and, thus, if there is a need for specific regulations depending on the type of data dealt with.

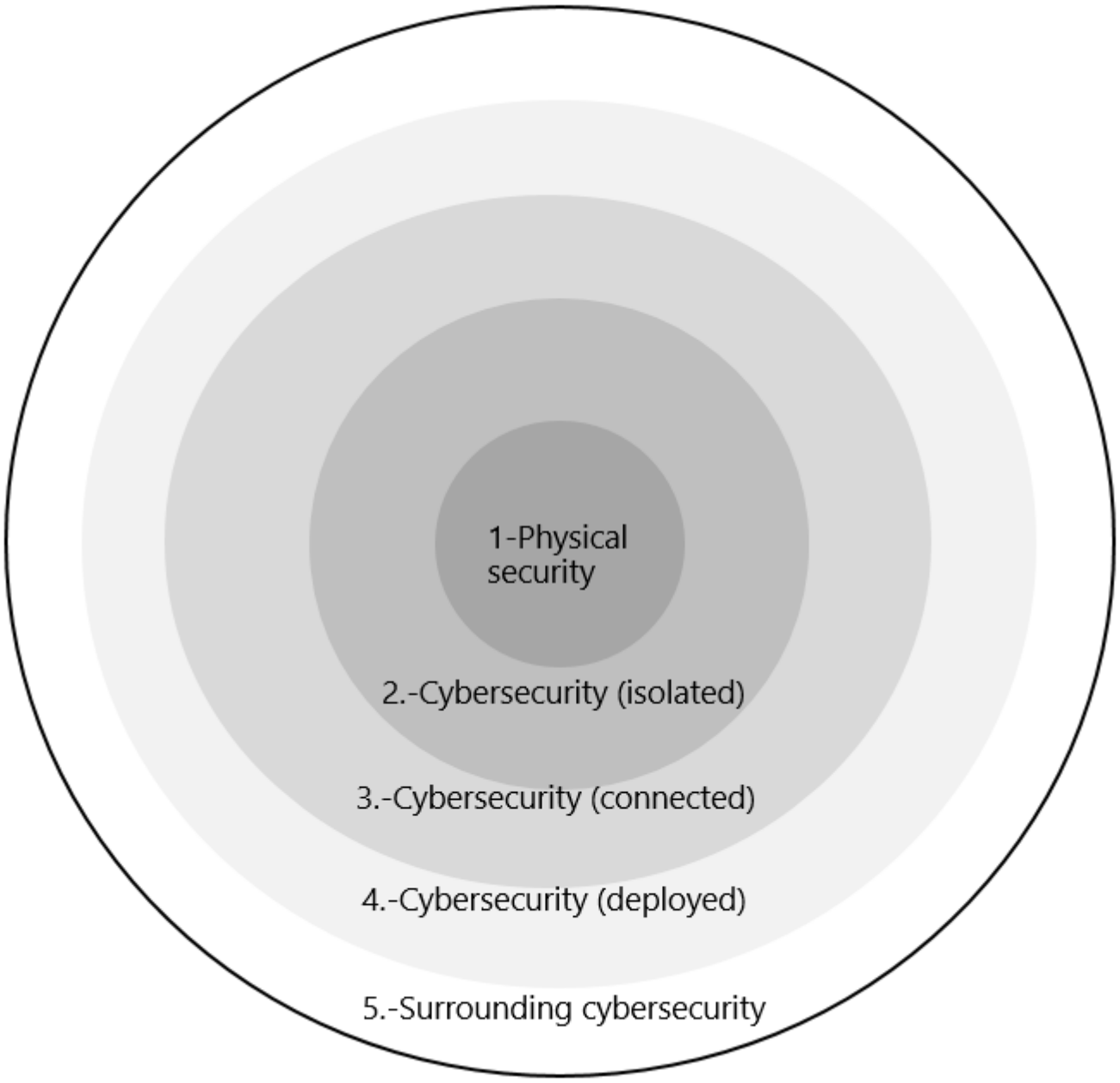
Interview #4 was performed with a healthcare provider based within the EU, specifically in Spain. It is a paperless hospital where almost all the processes and workflows are IT based and therefore there is a high dependence on IT infrastructure and digital information. Three main issues were identified:

- First of all, the lack of obligation to certify a certain level of cybersecurity considering the whole organization's IT map. There are guidelines, but while device manufacturers should demonstrate their adherence to guidelines/best practices through formal certifications, for healthcare providers it is only recommended (even if highly recommended) to be compliant with some of them, but it is not a blocking requirement in the sense that even when the hospital is not compliant, normal activities can proceed. This has also been pointed out in section 3.2.3.7 in D3.1.
- Also, the existing guidance refers to features of the device itself, while what needs to be taken into account is the overall scenario where the device will be deployed. Medical devices are to be deployed and used in organizations where there is a lack of obligation to be certified, so it leads to lack of uniformity in the deployment scenarios and, thus, it is not possible to define rules addressed to any standard scenario.
- Finally, the lack of post market assistance was highlighted, which appears typically with medical devices with outdated operating systems, that can't be patched/updated and that sometimes lead to isolation if the observed risks reach a certain level.

5 Conclusions

It has been observed that the literature has evolved aligned with the evolution of the medical devices. To better explain this idea, the following figure illustrates the different phases we observed:

Figure 1: Evolution of cybersecurity.



Starting from the inner ring, we can see five different aspects of cybersecurity that were the most relevant during different lifetimes of medical devices evolution.

#1 - First of all we have the physical security. It is not referred to cybersecurity at all and it is rather related with mechanical, chemical, or electrical issues that the medical device could experience. Nevertheless, it is worth to include it because it is not unusual that following the references across the documentation, it leads to physical security measures when what is expected is to find cybersecurity measures. That's because the different documentation evolves in a different rhythm.

#2 – Then we find the first class of cybersecurity related content. It comes from a time where the medical devices were mostly isolated and therefore there was no need to cover issues derived from the connection of medical devices with other systems. This is the largest category in the sense of quantity of currently existing content, and treats concepts as password policies, encryption of data at rest, and other measures to keep data confidentiality and incident recovery plans.

#3 – The third category corresponds to connected medical devices. There are guidelines that take into account that medical devices are connected to external systems, but without focusing much on those external systems the medical devices are connected to. It covers aspects such as trusted servers and services to connect, encrypted communications and so on.

#4 – In fourth place there is the set of content that would address the environments were the medical devices are to be deployed. This is a significant category because usually the medical devices would be required to fit the policies in place and, if not possible, could probably derive in an isolated scenario, losing part of the potential benefit of the medical device itself or the acquired data. Despite acknowledging that fact and recognizing it, the lack of clear regulations for healthcare providers' cybersecurity implies heterogeneity in those deployment scenarios, and that is the reason why there is not any regulation or guideline that covers this extensively enough. There are guidelines that clearly present cybersecurity as a shared responsibility between the device provider and the operator, but don't offer a clear guide on how to protect a device considering its final environment.

#5 – And finally we have the set of content addressed to cope with surrounding aspects of cybersecurity as, for example, the procurement process of medical devices, or the cybersecurity awareness of end users even those not linked to technical profiles. Even not being a kind of technical content, these two aspects have a great impact on cybersecurity. The procurement of medical devices focuses on explaining how to add cybersecurity criteria to clinical criteria during the procurement process, to decide what devices to acquire. By this, regulators try to force market evolution since potential customers would choose those medical devices that include a greater level of cybersecurity, provided that clinical requirements are reached.

Regarding cybersecurity awareness, this is a more general trend in cybersecurity and not only cybersecurity of medical devices because as the technical measures applied to protect the information are improved, so it becomes more expensive to break them and so social engineering arises as the best cost-benefit ratio for cybercriminals.

6 References

[1] Y. Xiao and M. Watson, 'Guidance on Conducting a Systematic Literature Review', *J. Plan. Educ. Res.*, vol. 39, no. 1, pp. 93–112, Mar. 2019, doi: 10.1177/0739456X17723971.

[2] Medical Device Coordination Group (MDCG), 'Guidance on Cybersecurity for medical devices'. Jul. 2020. Accessed: Mar. 17, 2023. [Online]. Available: https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

[3] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. Accessed: Apr. 12, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

[4] *Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC*. Accessed: Apr. 05, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R0745

[5] *Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU*. Accessed: Apr. 05, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0746

[6] *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Accessed: Apr. 06, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

[7] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Accessed: Apr. 06, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

[8] *Medical Device Amendments of 1976*. 1976. Accessed: Apr. 05, 2023. [Online]. Available: https://www.govinfo.gov/content/pkg/STATUTE-90/pdf/STATUTE-90-Pg539.pdf

[9] *Health Insurance Portability and Accountability Act of 1996*. 1996. Accessed: Apr. 18, 2023. [Online]. Available: https://www.congress.gov/bill/104th-congress/house-bill/3103

[10] *Cybersecurity Enhancement Act of 2014*. 2014. Accessed: Apr. 21, 2023. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

[11] *Consolidated Appropriations Act, 2023*. 2022. Accessed: Apr. 25, 2023. [Online]. Available: https://www.congress.gov/bill/117th-congress/house-bill/2617

[12] International Medical Device Regulators Forum (IMDRF), 'Principles and practices for Medical Device Cybersecurity'. Mar. 18, 2020. Accessed: Mar. 17, 2023. [Online]. Available: https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

[13] European Union Agency for Cybersecurity (ENISA), 'Procurement Guidelines for Cybersecurity in Hospitals'. Feb. 24, 2020. Accessed: Apr. 04, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services
[14] Agence nationale de sécurité du médicament et des produits de santé (ANSM), 'Cybersecurity of medical devices integrating software during their life cycle'. Jul. 2019. Accessed: Apr. 11, 2023. [Online]. Available: https://archiveansm.integra.fr/content/download/163697/2140145/version/1/file/pi-190719-Cybersecurite_Recommandations-Eng.pdf
[15] eHealth Suisse, 'Guide for app developers, manufacturers and distributors'. Jun. 02, 2020. Accessed: Apr. 13, 2023. [Online]. Available: https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2018/E/180731_Leitfaden_fuer_App_Entwickler_def_EN.pdf
[16] Federal Office for Information Security (BSI), 'Cyber security Requirements for Network-Connected Medical Devices'. Nov. 13, 2018. Accessed: Mar. 17, 2023. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_132E.html
[17] *Council Directive 93/42/EEC of 14 June 1993 concerning medical devices*. 1993. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31993L0042
[18] Health Canada, 'Pre-market Requirements for Medical Device Cybersecurity'. Jun. 26, 2019. Accessed: Apr. 11, 2023. [Online]. Available: https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/cybersecurity/document.html
[19] National Institute of Standards and Technology (NIST), 'Framework for Improving Critical Infrastructure Cybersecurity'. Apr. 16, 2018. Accessed: Apr. 05, 2023. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf
[20] United States Food and Drug Administration (FDA), 'Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions'. Apr. 08, 2022. Accessed: Mar. 17, 2023. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions
[21] United States Food and Drug Administration (FDA), 'Postmarket Management of Cybersecurity in Medical Devices'. Dec. 28, 2016. Accessed: Mar. 17, 2023. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices
[22] Therapeutic Goods Administration (TGA), 'Medical device cyber security guidance for industry'. Nov. 24, 2022. Accessed: Apr. 11, 2023. [Online]. Available: https://www.tga.gov.au/how-we-regulate/manufacturing/medical-devices/manufacturer-guidance-specific-types-medical-devices/regulation-software-based-medical-devices/medical-device-cyber-security-guidance-industry
[23] Therapeutic Goods Administration (TGA), 'Medical device cyber security information for users'. Nov. 24, 2022. Accessed: Apr. 11, 2023. [Online]. Available: https://www.tga.gov.au/resources/publication/publications/medical-device-cyber-security-information-users

7 Annex I: Results of the backward search

Table 4: Results of the backward search.

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
MDCG - Guidance on Cybersecurity for medical devices	Medical Device Regulation (EU) 2017/745	Legislation	✓	Meet criteria
	In Vitro Diagnostic Medical Device Regulation (EU) 2017/746	Legislation	✓	Meet criteria
	Medical Device Directive (93/42/EEC)	Legislation	X	Not in force
	Directive on active implantable medical devices (90/385/EEC)	Legislation	X	Not in force
	Directive on in vitro diagnostic medical devices (98/79/EC)	Legislation	X	Not in force
	ENISA - Definition of Cybersecurity - Gaps and overlaps in standardisation	Guideline / Best practices	X	Not focused on medical devices
	IMDRF - Principles and practices for Medical Device Cybersecurity	Guideline / Best practices	✓	Meet criteria
	Manufacturers Disclosure Statement for Medical Device Security (MDS2)	Framework	X	Type of document
	Common Vulnerability Scoring System (CVSS)	Framework	X	Type of document
	General Data Protection Regulation (EU) 2016/679	Legislation	X	Not focused on cybersecurity
	Guidelines on a Medical Devices Vigilance System MEDDEV	Guideline / Best practices	X	Not focused on cybersecurity
	NIS Directive (EU) 2016/1148	Legislation	X	Old version
	Cybersecurity Act (EU) 2019/881	Legislation	✓	Meet criteria
	ANSM - Cybersecurity of medical devices integrating software during their life cycle	Guideline / Best practices	✓	Meet criteria
	BSI - Cyber Security Requirements for Network-Connected Medical Devices	Guideline / Best practices	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	eHealth Suisse - Guideline for app developers, manufacturers and distributors	Guideline / Best practices	✓	Meet criteria
	ISO 14971: Medical devices — Application of risk management to medical devices	Standard	✓	Meet criteria
	BS EN 62304: Medical device software - Software life-cycle processes	Standard	✓	Meet criteria
	ISO 31000: Risk Management	Standard	✓	Meet criteria
	ISO/IEC 27000: Information Technology — Security techniques — Information security management systems (ISMS) — Overview and vocabulary	Standard	✓	Meet criteria
	ISO/IEC 27001: Information Technology – Security techniques – Information Security management Systems – Requirements	Standard	✓	Meet criteria
	ISO/IEC 60601-1: Medical electrical equipment – Part 1: General requirements for basic safety and essential performance	Standard	✓	Meet criteria
	IEC 82304-1 Health Software Part 1: General requirements for Product Safety	Standard	✓	Meet criteria
	ISO/IEC 80001-1 Application of Risk Management for IT networks Incorporating Medical Devices	Standard	✓	Meet criteria
	ISO/IEC 80001-5-1 Application of Risk Management for IT networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.	Standard	✓	Meet criteria
	IEC/TR 80001-2-2 Application of Risk Management for IT networks Incorporating Medical Devices Part 2-2: Guidance for the Disclosure and Communication of Medical Device Security Needs, Risks and Controls	Standard	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	IEC/TR 80001-2-8 Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2	Standard	✓	Meet criteria
	IEC 62366-1 Medical devices — Part 1: Application of usability engineering to medical devices	Standard	✓	Meet criteria
	IEC 62443-4-1 Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.	Standard	✓	Meet criteria
	IEC 62443-4-2 Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.	Standard	✓	Meet criteria
	IEC/TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.	Standard	✓	Meet criteria
ANSM - Cybersecurity of medical devices integrating software during their life cycle	Medical Device Regulation (EU) 2017/745	Legislation	✓	Meet criteria
	In Vitro Diagnostic Medical Device Regulation (EU) 2017/746	Legislation	✓	Meet criteria
	NIS Directive (EU) 2016/1148	Legislation	✗	Old version
	ISO 13485: Medical devices – Quality management systems – Requirements for regulatory purposes	Standard	✓	Meet criteria
	BSI - Cyber Security Requirements for Network-Connected Medical Devices	Guideline / Best practices	✓	Meet criteria
	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version
	FDA - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guideline / Best practices	✗	Publication year
	FDA - Postmarket Management of Cybersecurity in Medical Devices	Guideline / Best practices	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	ISO 14971: Medical devices — Application of risk management to medical devices	Standard	✓	Meet criteria
	General Data Protection Regulation (EU) 2016/679	Legislation	X	Not focused on cybersecurity
	ITU (International Telecommunication Union) Global Cybersecurity Agenda (GCA)	Other	X	Type of document
	NIST - Framework for Improving Critical Infrastructure Cybersecurity	Framework	X	Type of document
	ISO/IEC 27000: Information Technology - Security Techniques - Information security management systems - Overview and vocabulary	Standard	✓	Meet criteria
	ISO/IEC 27005: Information Technology - Security Techniques - Information security risk management	Standard	✓	Meet criteria
	ISO 27001: Information security management	Standard	✓	Meet criteria
	ISO 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.	Standard	✓	Meet criteria
	BS EN 50159 - Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems	Standard	✓	Meet criteria
	ISO/IEC 15802: Information technology - Telecommunications and information exchange between systems. Local and metropolitan area networks. Common specifications - Part 3: Media access control (MAC) bridges	Standard	✓	Meet criteria
	IEEE 802.1X: Port-Based Network Access Control	Standard	✓	Meet criteria
	ISO/TR 11633: Health informatics - Information security management for remote maintenance of medical devices and medical information systems	Standard	✓	Meet criteria
	ISO 14971: Application of risk management to medical devices	Standard	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	IEC 62366: Medical devices — Part 1: Application of usability engineering to medical devices	Standard	✓	Meet criteria
	BS EN 60601-1: Medical electrical equipment - General requirements for basic safety and essential performance	Standard	✓	Meet criteria
	IMDRF - Software as a Medical Device (SaMD): Clinical Evaluation	Guideline / Best practices	✗	Not focused on cybersecurity
	FDA - Draft Guidance - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	Guideline / Best practices	✓	Meet criteria
	IEEE Canada: Building Code for Medical Devices of the 21st Century	Other	✗	Type of document
	BS EN 62304: Medical device software - Software life-cycle processes	Standard	✓	Meet criteria
	BS EN 80001: Application of risk management for IT networks incorporating medical devices	Standard	✓	Meet criteria
	Building code for MD software security – IEEE (Institute of Electrical and Electronic Engineers)	Other	✗	Type of document
IMDRF - Principles and Practices for Medical Device Cybersecurity	NIST - Framework for Improving Critical Infrastructure Cybersecurity	Framework	✗	Type of document
	NIST - Secure Software Development Framework (SSDF)	Framework	✗	Type of document
	OWASP (e.g. Security by Design principles)	Other	✗	Type of document
	AAMI TIR57: Principles for medical device security—Risk management	Standard	✓	Meet criteria
	AAMI TIR 97: Principles for medical device security—Postmarket risk management for device manufacturers	Standard	✓	Meet criteria
	IEC 60601-1: Medical electrical equipment - Part 1: General requirements for basic safety and essential performance	Standard	✓	Meet criteria
	IEC 62304: Medical device software – Software life cycle processes	Standard	✓	Meet criteria
	IEC 62366-1: Medical devices - Part 1: Application of usability engineering to medical devices	Standard	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	IEC 80001-1: Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities	Standard	✓	Meet criteria
	IEC TR 80001-2-2: Application of risk management for IT-networks incorporating medical devices - Part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls	Standard	✓	Meet criteria
	IEC TR 80001-2-8: Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2	Standard	✓	Meet criteria
	ISO 13485: Medical devices – Quality management systems – Requirements for regulatory purposes	Standard	✓	Meet criteria
	ISO 14971: Medical devices – Application of risk management to medical devices	Standard	✓	Meet criteria
	ISO/TR 80001-2-7: Application of risk management for IT-networks incorporating medical devices – Application guidance – Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1	Standard	✓	Meet criteria
	ISO/IEC 27000 family - Information security management systems	Standard	✓	Meet criteria
	ISO/IEC 27035-1: Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management	Standard	✓	Meet criteria
	ISO/IEC 27035-2: Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response	Standard	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	ISO/IEC 29147: Information Technology – Security Techniques – Vulnerability Disclosure	Standard	✓	Meet criteria
	ISO/IEC 30111: Information Technology – Security Techniques – Vulnerability Handling Processes	Standard	✓	Meet criteria
	ISO/TR 24971: Medical devices – Guidance on the application of ISO 14971	Standard	✓	Meet criteria
	UL 2900-1: Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements	Standard	✓	Meet criteria
	UL 2900-2-1: Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems	Standard	✓	Meet criteria
	ANSM - Cybersecurity of medical devices integrating software during their life cycle	Guideline / Best practices	✓	Meet criteria
	China - Medical Device Network Security Registration on Technical Review Guidance Principle	Guideline / Best practices	✗	Not written in English
	Medical Device Regulation (EU) 2017/745	Legislation	✓	Meet criteria
	In Vitro Diagnostic Medical Device Regulation (EU) 2017/746	Legislation	✓	Meet criteria
	FDA (Draft): Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (October 2018)	Guideline / Best practices	✗	Old version
	FDA - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guideline / Best practices	✗	Publication year
	FDA - Design Considerations for Devices Intended for Home Use	Guideline / Best practices	✗	Not focused on cybersecurity
	FDA - Postmarket Management of Cybersecurity in Medical Devices	Guideline / Best practices	✓	Meet criteria
	BSI - Cyber Security Requirements for Network-Connected Medical Devices	Guideline / Best practices	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	Health Canada - Pre-market Requirements for Medical Device Cybersecurity	Guideline / Best practices	✓	Meet criteria
	Japan: Ensuring Cybersecurity of Medical Device: PFSB/ELD/OMDE Notification No. 0428-1	Other	✗	Type of document
	Japan: Guidance on Ensuring Cybersecurity of Medical Device: PSEHB/MDED-PSD Notification No. 0724-1	Other	✗	Type of document
	Singapore Standards Council Technical Reference 67: Medical device cybersecurity	Other	✗	Type of document
	TGA - Medical device cybersecurity - Consumer information	Other	✗	Type of document
	TGA - Medical device cybersecurity guidance for industry	Guideline / Best practices	✓	Meet criteria
	TGA - Medical device cybersecurity information for users	Guideline / Best practices	✓	Meet criteria
	CERT® Guide to Coordinated Vulnerability Disclosure	Framework	✗	Type of document
	NIST - Framework for Improving Critical Infrastructure Cybersecurity	Framework	✗	Type of document
	NIST - Secure Software Development Framework (SSDF)	Framework	✗	Type of document
	Medical Device and Health IT Joint Security Plan	Framework	✗	Type of document
	MITRE medical device cybersecurity playbook	Framework	✗	Type of document
	MITRE CVSS Healthcare Rubric	Framework	✗	Type of document
	Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients	Other	✗	Type of document
	Open Web Application Security Project (OWASP)	Other	✗	Type of document
	Manufacturer Disclosure Statement for Medical Device Security (MDS2)	Framework	✗	Type of document
	ECRI approach to applying the NIST framework to MD	Framework	✗	No free access
	Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group	Other	✗	Type of document

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
BSI - Cyber Security Requirements for Network-Connected Medical Devices	NIST A Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems	Other	X	Type of document
eHealth Suisse - Guideline for app developers, manufacturers and distributors	Guidelines on a Medical Devices Vigilance System MEDDEV	Guideline / Best practices	X	Not focused on cybersecurity
	Swiss Medical Devices Ordinance	Legislation	X	Not focused on cybersecurity
	Therapeutic Products Act, TPA	Legislation	X	Publication year
	Medical Device Directive (93/42/EEC)	Legislation	X	Not in force
	Directive on in vitro diagnostic medical devices (98/79/EC)	Legislation	X	Not in force
	Medical Device Regulation (EU) 2017/745	Legislation	✓	Meet criteria
	In Vitro Diagnostic Medical Device Regulation (EU) 2017/746	Legislation	✓	Meet criteria
	Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices	Other	X	Type of document
	Medical devices: conformity assessment and the UKCA mark	Guideline / Best practices	X	Not focused on cybersecurity
	ISO 13485: Medical devices – Quality management systems – Requirements for regulatory purposes	Standard	✓	Meet criteria
	ISO 9001 Quality Management Systems	Standard	✓	Meet criteria
	IEC 62304: Medical device software – Software life cycle processes	Standard	✓	Meet criteria
	IEC 62366-1: Medical devices — Application of usability engineering to medical devices	Standard	✓	Meet criteria

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	ISO 14971: Medical devices — Application of risk management to medical devices	Standard	✓	Meet criteria
	IEC 82304-1: Health software – Part 1: General requirements for product safety	Standard	✓	Meet criteria
	MDCG - Guidance on Clinical Evaluation (MDR) / Performance Evaluation (IVDR) of Medical Device Software	Guideline / Best practices	✗	Not focused on cybersecurity
	European Database on Medical Devices (Eudamed) Regulation (EU) 2021/2078	Legislation	✗	Not focused on cybersecurity
	IMDRF - Software as a Medical Device (SaMD): Clinical Evaluation	Guideline / Best practices	✗	Not focused on cybersecurity
	AAMI TIR36: Validation of software for regulated processes	Standard	✓	Meet criteria
	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version
	FDA - Postmarket Management of Cybersecurity in Medical Devices	Guideline / Best practices	✓	Meet criteria
	FDA - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guideline / Best practices	✗	Publication year
	Ireland Guide To Placing Medical Device Standalone Software on the Market	Guideline / Best practices	✗	Not focused on cybersecurity
	TGA - Medical device cybersecurity guidance for industry	Guideline / Best practices	✓	Meet criteria
	MDCG - Guidance on Cybersecurity for medical devices	Guideline / Best practices	✓	Meet criteria
	Swiss Federal Act on Data Protection	Legislation	✗	Publication year
	General Data Protection Regulation (EU) 2016/679	Legislation	✗	Not focused on cybersecurity
	FDA Recognized Consensus Standards	Other	✗	Type of document

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
FDA - Draft Guidance - Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	FDA - Appropriate Use of Voluntary Consensus Standards in Premarket Submissions for Medical Devices	Guideline / Best practices	✗	Not focused on cybersecurity
	Standards Development and the Use of Standards in Regulatory Submissions Reviewed in the Center for Biologics Evaluation and Research	Guideline / Best practices	✗	Not focused on cybersecurity
	FDA Safety Communication - Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices	Other	✗	Type of document
	FDA - Postmarket Management of Cybersecurity in Medical Devices	Guideline / Best practices	✓	Meet criteria
	FDA - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guideline / Best practices	✗	Publication year
	FDA - Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices	Guideline / Best practices	✗	Not focused on cybersecurity
	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version
	IMDRF - Principles and practices for Medical Device Cybersecurity	Guideline / Best practices	✓	Meet criteria
	FDA - The 510(k) Program: Evaluating Substantial Equivalence in Premarket Notifications [510(k)]	Guideline / Best practices	✗	Not focused on cybersecurity
	Medical Device and Health IT Joint Security Plan	Framework	✗	Type of document
	Common Vulnerability Scoring System	Framework	✗	Type of document
	AAMI TIR57: Principles for medical device security—Risk management	Standard	✓	Meet criteria
	FDA - Off-The-Shelf Software Use in Medical Devices	Guideline / Best practices	✗	Not focused on cybersecurity

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	FDA - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guideline / Best practices	✗	Publication year
	Manufacturer Disclosure Statement for Medical Device Security (MDS2)	Framework	✗	Type of document
	MITRE - Common Weakness Enumeration	Framework	✗	Type of document
	FDA - Multiple Function Device Products: Policy and Considerations	Guideline / Best practices	✗	Not focused on cybersecurity
	NIST 800-160v1, Systems Security Engineering	Framework	✗	Type of document
	FDA - Requests for Feedback and Meetings for Medical Device Submissions: The Q-Submission Program	Guideline / Best practices	✗	Not focused on cybersecurity
	FDA - Applying Human Factors and Usability Engineering to Medical Devices	Guideline / Best practices	✗	Not focused on cybersecurity
	ANSI/UL 2900 Software Cybersecurity for Network-Connectable Products	Standard	✓	Meet criteria
	ANSI/ISA-62443-4-1: Security for industrial automation and control systems Part 4-1: Product security development life-cycle requirements	Standard	✓	Meet criteria
	Health Insurance Portability and Accountability Act (HIPAA) Security Rule	Legislation	✗	Publication year
	Health Care Industry Cybersecurity Task Force - Report on improving cybersecurity in the health care industry	Other	✗	Type of document
	FDA - Factors to Consider When Making Benefit-Risk Determinations for Medical Device Investigational Device Exemptions	Guideline / Best practices	✗	Not focused on cybersecurity
FDA - Postmarket	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
Management of Cybersecurity in Medical Devices	FDA - Distinguishing Medical Device Recalls from Medical Device Enhancements	Guideline / Best practices	X	Not focused on cybersecurity
	NIST - Framework for Improving Critical Infrastructure Cybersecurity	Framework	X	Type of document
	Homeland Security Act 2002	Legislation	X	Publication year
	FDA - MOU 225-16-024	Other	X	Type of document
	IMDRF - Software as a Medical Device (SaMD): Key Definitions	Guideline / Best practices	X	Not focused on cybersecurity
	FDA - Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices	Guideline / Best practices	X	Not focused on cybersecurity
	Health Insurance Portability and Accountability Act (HIPAA)	Legislation	X	Publication year
	OWASP - Threat Modeling	Other	X	Type of document
	Common Vulnerability Scoring System (CVSS)	Framework	X	Type of document
	MITRE - Common Vulnerabilities and Exposures	Framework	X	Type of document
	MITRE - Common Weakness Enumeration	Framework	X	Type of document
	MITRE - Common Weakness Scoring System	Framework	X	Type of document
	MITRE Common Attack Pattern Enumeration and Classification	Framework	X	Type of document
	NIST - Common Configuration Enumeration	Framework	X	Type of document
	NIST - Common Platform Enumeration	Framework	X	Type of document
	ISO/IEC 29147: Information Technology – Security Techniques – Vulnerability Disclosure	Standard	✓	Meet criteria
	ISO/IEC 30111: Information Technology – Security Techniques – Vulnerability Handling Processes.	Standard	✓	Meet criteria
	FDA - PMA Supplements and Amendments	Guideline / Best practices	X	Not focused on cybersecurity
	FDA - Unique Device Identification System (UDI System)	Guideline / Best practices	X	Not focused on cybersecurity

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
Health Canada - Pre-market Requirements for Medical Device Cybersecurity	AAMI TIR57: Principles for medical device security - Risk management	Standard	✓	Meet criteria
	ANSI/CAN/UL 2900-1: Software Cybersecurity for Network-Connectable Products, Part1: General Requirements	Standard	✓	Meet criteria
	ANSI/CAN/UL 2900-2-1: Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems	Standard	✓	Meet criteria
	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version
	FDA - Postmarket Management of Cybersecurity in Medical Devices	Guideline / Best practices	✓	Meet criteria
	IEC 62304 Medical Device Software - Software life cycle processes	Standard	✓	Meet criteria
	IEC 80001-1 Application of risk management for IT-networks incorporating medical devices - Part 1: roles, responsibilities and activities	Standard	✓	Meet criteria
	IMDRF - Software as a Medical Device (SaMD): Key Definitions	Guideline / Best practices	✗	Not focused on cybersecurity
	ISO 14971 Medical devices - Application of risk management to medical devices	Standard	✓	Meet criteria
	NIST - Framework for Improving Critical Infrastructure Cybersecurity	Framework	✗	Type of document
	NIST - Guide for Conducting Risk Assessments	Guideline / Best practices	✗	Not focused on cybersecurity
	TGA - Medical device cyber security v. 1.0, December 2018, Draft guidance	Guideline / Best practices	✗	Old version
	Personal Information Protection and Electronic Documents Act (PIPEDA)	Legislation	✗	Publication year

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
TGA - Medical device cybersecurity guidance for industry	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version
	FDA - Postmarket Management of Cybersecurity in Medical Devices	Guideline / Best practices	✓	Meet criteria
	FDA - Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices	Guideline / Best practices	✗	Not focused on cybersecurity
	FDA - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software	Guideline / Best practices	✗	Publication year
	FDA - Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices	Guideline / Best practices	✗	Not focused on cybersecurity
	NIST - Securing Electronic Health Records on Mobile Devices	Framework	✗	Type of document
	NIST - Securing Wireless Infusion Pumps	Framework	✗	Type of document
	ECRI - Cybersecurity Risk Assessment for Medical Devices	Guideline / Best practices	✗	No free access
	ECRI - Cyber Threats Top ECRI Institute's 2019 Health Technology Hazards	Guideline / Best practices	✗	No free access
	ECRI - Cybersecurity: The Essentials	Guideline / Best practices	✗	No free access
	ECRI - Anti-Malware Software and Medical Devices: A Crash Course in Protecting Your Devices from Cyber Attacks	Guideline / Best practices	✗	No free access
	ECRI - Ransomware Attacks: How to Protect Your Medical Device Systems	Guideline / Best practices	✗	No free access
	IMDRF - Software as a Medical Device (SaMD): Key Definitions	Guideline / Best practices	✗	Not focused on cybersecurity
	IMDRF - Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations	Guideline / Best practices	✗	Not focused on cybersecurity

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	IMDRF- Software as a Medical Device (SaMD): Application of Quality Management System	Guideline / Best practices	✗	Not focused on cybersecurity
	IMDRF - Software as a Medical Device (SaMD): Clinical Evaluation	Guideline / Best practices	✗	Not focused on cybersecurity
	ENISA - Baseline Security Recommendations for IoT	Guideline / Best practices	✗	Not focused on medical devices
	Medical Device Regulation (EU) 2017/745	Legislation	✓	Meet criteria
	South Korea's Ministry of Science and ICT, Korea Internet and Security Agency (KISA) - Cyber Security Guide for Smart Medical Service	Guideline / Best practices	✗	No access
	Health Canada - Pre-market Requirements for Medical Device Cybersecurity	Guideline / Best practices	✓	Meet criteria
ENISA - Procurement Guidelines for Cybersecurity in Hospitals	Deloitte - Medtech and the Internet of Medical Things How connected medical devices are transforming health care	Other	✗	Type of document
	Lynne Coventry and Dawn Branley - Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward	Other	✗	Type of document
	MDCG - Guidance on Cybersecurity for medical devices	Guideline / Best practices	✓	Meet criteria
	General Data Protection Regulation (EU) 2016/679	Legislation	✗	Not focused on cybersecurity
	Health Insurance Portability and Accountability Act (HIPAA)	Legislation	✗	Publication year
	FDA - Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	Guideline / Best practices	✗	Old version
	Medical Device Regulation (EU) 2017/745	Legislation	✓	Meet criteria
	Aliya Tabasum et al. - Cybersecurity Issues in Implanted Medical Devices	Other	✗	Type of document

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	Clemens Scott Kruse et al. - Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends	Other	X	Type of document
	Ross Koppel et al. - Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?	Other	X	Type of document
	ECRI - 2019 Top 10 Health Technology Hazards Executive Brief	Guideline / Best practices	X	No free access
	NIST - Guide for Conducting Risk Assessments	Guideline / Best practices	X	Not focused on cybersecurity
	ENISA - Cyber security and resilience for Smart Hospitals	Guideline / Best practices	X	Not focused on medical devices
	ENISA - Threat Landscape Report 2018: 15 Top Cyberthreats and Trends	Other	X	Type of document
	PrivSec Report - BYOD and GDPR: Managing the compliance conundrum	Other	X	Type of document
	ENISA - Threat Landscape Report 2018	Other	X	Type of document
	ENISA - Threat Landscape Report 2018	Other	X	Type of document
	Annalena Welp et al., 'Teamwork and Clinician Burnout in Swiss Intensive Care: The Predictive Role of Workload, and Demographic and Unit Characteristics'	Other	X	Type of document
	Koppel et al., 'Workarounds to Computer Access in Healthcare Organizations'.	Other	X	Type of document
	Sean W Smith and Ross Koppel, 'Healthcare Information Technology's Relativity Problems: A Typology of How Patients' Physical Reality, Clinicians' Mental Models, and Healthcare Information Technology Differ'	Other	X	Type of document
	Hamish Porter - Overview of some major incidents in radiotherapy and their consequences	Other	X	Type of document

DOCUMENT	REFERENCE	TYPE	INCLUDED	REASON
	NIST - National Vulnerability Database	Other	X	Type of document
TGA - Medical device cyber security information for users	Therapeutic Goods Act 1989	Legislation	X	Publication year
	Privacy Act 1988	Legislation	X	Publication year
	Essential Eight Maturity Model	Other	X	Type of document
	ECRI - Anti-Malware Software And Medical Devices: A Crash Course In Protecting Your Devices From Cyber Attacks	Guideline / Best practices	X	No free access