Grant Agreement No.: 101095542
Call: HORIZON- HLTH-2022-IND-13
Topic: HORIZON-HLTH-2022-IND-13-01
Type of action: HORIZON-RIA

CYLCOMED

Cyber-security toolbox
for connected medical devices

D3.2 Requirements and specifications consolidation

Revision: v.1.5

Work package	WP 3
Task	3.2
Due date	31/05/2024
Submission date	31/05/2024
Deliverable lead	FHUNJ
Version	1.5
Authors	Andres Castillo PhD, Santiago Bollain (FHUNJ)
Reviewers	Juan Carlos Pérez Baun, Esteban Armas (ATOS)
Abstract	This document updates the requirements already collected in D3.1 where a study of the state of the art on the cybersecurity of connected medical devices, in accordance with current common standards, procedures and approaches, as well as directives and guides were done. It also updates the toolbox requirements
Keywords	Cybersecurity, Connected Medical Devices, Requirements, Regulations, Standards

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	01/05/23	Initial table of contents	Andrés Castillo (FHUNJ)
V0.2	09/05/23	Initial Content	Andrés Castillo (FHUNJ)
V0.3	18/02/24	Appendices rework	Santiago Bollain, Andrés Castillo (FHUNJ)
V0.4	11/04/24	Content completion	Santiago Bollain, Andrés Castillo (FHUNJ)
V0.5	15/04/24	Table of contents reorganization. Appendix B split in B and C	Santiago Bollain, Andrés Castillo (FHUNJ)
V0.6	16/04/24	Comments where links from technical partners are needed.	Santiago Bollain, Andrés Castillo (FHUNJ)
V0.7	30/04/24	Updated description for pilot 2	Simone Favrin (Mediaclinic)
V0.8	3/05/24	Created requirements for pilot 1	Ricardo Ruiz (RGB)
V0.9	3/05/24	Toolbox requirements updated	Hrvoje Ratkajec
V1.0	04/05/24	Version ready for first review	Santiago Bollain, Andrés Castillo (FHUNJ)
V1.1	10/05/24	Contribution on section 2.1.3	Juan Carlos Pérez Baún (Atos-Eviden)
V1.2	14/05/24	Suggestions from reviewer incorporated	Santiago Bollain, Andrés Castillo (FHUNJ)
V1.5	31/05/24	Final version	Santiago Bollain, Andrés Castillo (FHUNJ)

Co-funded by
the European Union

Disclaimer

The information, documentation, and figures available in this deliverable are written by the " Cyber security Toolbox for connected medical devices" (CYLCOMED) project's consortium under EC grant agreement 101095542 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

This document D3.2, serves as a continuation of deliverable D3.1, aiming to present the updates and new requirements that have emerged since the publication of D3.1.

As a reminder, there is a triple perspective in this document series: the medical needs to ensure patient safety, the legal and ethical context for cybersecurity, and the technical expertise materialized in the software assets that is brought into the project. The requirements that this document present are the basis for the development of a Toolbox to enhance the cybersecurity of connected medical devices.

Several deliverables are being used as additional input for this document, specifically D2.1 “Analysis of Ethical, Legal, Data Protection Frameworks” [1], D5.1 “CYLCOMED toolbox prototype” [2], and D6.1 “Pilots planning and evaluation strategy” [3].

The evolution of the toolbox assets requirements is being updated in Chapter 2, while Chapter 3 will focus on the evolution of the requirements for the use cases. Chapter 4 will present the map of assets and requirements while chapter 5 will present the conclusions.

There are many regulations, standards, and best practices related to cybersecurity for connected medical devices which can make it difficult for organizations planning to implement this type of solution. Appendixes are organized to help to identify what is relevant:

- Appendix A collects regulations, standards, and best practices.
- Appendix B presents general requirements for connected medical device solutions.
- Appendix C presents the requirements for the toolbox.

New requirements have been incorporated, mainly from the Cybersecurity Resilience Act and the Cyber Security Act, these new requirements are identified in yellow.

Co-funded by
the European Union

Table of contents

Co-funded by
the European Union

List of figures

List of tables

Co-funded by
the European Union

Abbreviations

ABE	Attribute-Based Encryption
AI	Artificial Intelligence
API	Application Program Interface
BF	Backend & Frontend
BLE	Bluetooth Low Energy
C-OPA	CYLCOMED Open Policy Agent
CDN	Communication Device and Network
CMD	Connected Medical Device
CPU	Central Processing Unit
CRA	Cybersecurity Resilience Act
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPD	Security & Privacy by Design (DSPD)
EC	European Commission
ENISA	European Union Agency for Cybersecurity
EU	European Union
FE4MED	Functional Encryption for Medical Data
GDPR	General Data Protection Regulation
HIS	Health Information System
HTTPs	Hypertext Transfer Protocol Secure
IaC	Infrastructure as Code
IAM	Identity and Access Management
ICU	Intensive Care Unit
IEEE	Institute of Electrical and Electronics Engineers
IMDRF	International Medical Device Regulators Forum
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
IVD	In Vitro Diagnostic Medical Device
IVDR	In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR)
JSON	JavaScript Object Notation
LAN	Local Area Network
LADS	Live Anomaly Detection System
LOMOS	Log Monitoring System
LuS4MED	Ledger uSelf for Medical Data
MDI	Medical Device Interface
MDD	Medical Device Directive 93/42/CEE
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation (EU) 2017/745 (MDR)
MHP	MediaClinics Health Platform
NIS	Network and Information Security Directive
NIST	National Institute of Standards and Technology
NMT	Neuromuscular Transmission
OPA	Open Policy Agent
SAML	Security Assertion Markup Language

Co-funded by
the European Union

SSL/TLS	Secure Socket Layer / Transport Layer Security
VC	Verifiable Credentials
VLAN	Virtual Local Area Network
WP	Work Package
YAML	Yet Another Markup Language

Co-funded by
the European Union

1. Introduction

1.1. Purpose and scope of this document

This document is part of Work Package 3 (WP3). The study of the state of the art regarding cybersecurity has been carried out in the context of Task 3.2. This is the second and final version of this document and includes all the updates and new requirements that have emerged since the publication of D3.1 [4].

Several deliverables are being used as additional input for this document, specifically D2.1 “Analysis of Ethical, Legal, Data Protection Frameworks” [1], D5.1 “CYLCOMED toolbox prototype” [2], and D6.1 “Pilots planning and evaluation strategy” [3].

1.2. Deliverable structure

Chapter 2 will address the evolution of the toolbox assets requirements, while Chapter 3 will focus on the evolution of the requirements for the use cases. Chapter 4 will present the map of assets and requirements while chapter 5 will present the conclusions.

Appendix A has been consolidated from two distinct appendices found in deliverable 3.1, namely Appendix A: Requirements (Legal and Standards) and Appendix B: Requirements from Standards and Best Practices.

Appendices B and C outline the requirements for connected medical device solutions and the toolbox, respectively. These requirements were previously contained within the same appendix in version D3.1 [4].

Co-funded by
the European Union

2. Evolution of Toolbox requirements

In this chapter a review for the toolbox assets is presented, even they were already introduced in D3.1 [4], with special focus on what has been changed since then. This is the final version for the requirements

The cybersecurity CYLCOMED Toolbox will deliver to its stakeholders (manufacturers, developers, integrators, and people/platforms using and managing CMDs), the following comprehensive set of tools, organized by function and the task involved:

1. AI-based CMD behavioural Analysis & Log Monitoring (Task 5.1)
   a. CMD Log Monitoring
   b. AI-Behavioural Analysis
2. Connected Medical Devices and Services Management Tools (Task 5.2)
   a. CMD Security Maintenance
3. Identity & Access Management & Data Protection for CMDs (Task 5.3)
   a. uSelf for Medical Data
   b. Functional Encryption for Medical Data
   c. Open Policy Agent
4. Connected Medical Devices Integrity (Task 5.4)
   a. Device Integrity check
5. Security Dashboard (Task 5.5)
   a. Cybersecurity Dashboard

The name for the tools that are being developed are shown in the following table:

Tool name	**Asset**
CMD Log Monitoring	LOMOS
AI-Behavioural Analysis	LADS
CMD Security Maintenance	MENDER
uSelf for Medical Data	Lus4MED
Functional Encryption for Medical Data	FE4MED
CYLCOMED Open Policy Agent	C-OPA
Device Integrity check	Raspberry in house development
Cybersecurity Dashboard	Dashboard

Table 1: Mapping tools name and assets

The tools will be deployed as Linux docker containers, and every tool will be provided with its own docker-compose.yml file to facilitate the deployment and the tools' consolidation in the dashboard. All the software requirements will be included in the docker containers.

2.1. AI-based CMD Behavioural Analysis & Log Monitoring

A detailed description was already included in deliverable D3.1[4] and will not be included here again. This task includes two different tools that should help to detect anomalies and nonstandard behaviour through log files and network analysis. The tools are described in deliverable D5.1 [2].

2.1.1. CMD LOG MONITORING (LOMOS)

The AI-powered log monitoring solution is responsible for the automatic detection of anomalies in system/application logs. The tool should monitor the logs generated by Connected Medical Devices (CMDs), the platform that manages CMDs, and the Identity and Access Management component of the Cybersecurity toolbox. By monitoring the logs, it should identify the anomalous events and report them (in the form of anomaly scores) to the Cybersecurity Dashboard for visual inspection by the user.

Logs suitable for LOMOS:

- Raw logs should be in TXT file (no CSV) with human-readable content.
- Each logline should have a unique timestamp (e.g. microsecond or nanosecond time resolution).

For communication with the Cybersecurity Dashboard, an API (e.g. REST API) should be developed and implemented. The anomaly score provided is in JSON format.

2.1.2. AI-BEHAVIOURAL ANALYSIS (LADS)

LADS stands for Live Anomaly Detection System. LADS is a soft real-time anomaly-based network intrusion detection system. The tool should model patterns of benign traffic and identify anomalous behaviour based on deviations. Anomaly detections should be shown in the dashboard and be kept in files to allow future analysis.

2.2. Connected Medical Devices and Services Management Tools

The primary objective of Connected Medical Devices and Services Management Tool, MENDER, is to introduce cutting-edge cloud-native and service management solutions, with the overarching goal of automating the secure delivery of services both in the cloud and within the IoT/Edge layer, specifically tailored for medical solutions. Notably, the focus lies on delivering key functionalities essential for optimizing service delivery, ensuring security, and enhancing efficiency, specifically:

- Ensure secure updates of services in the medical devices.
- Reduce attack surface in the medical devices and cloud infrastructure.
- Detection of misconfigurations.
- Ensure code integrity and configuration integrity.

2.3. Identity & Access Management and Data Protection

A detailed description was already included in deliverable 3.1 and will not be included here again. The tools are described in deliverable D5.1 [2].

Identity and Access Management (IAM) and protecting data are crucial for protecting and controlling the access to the data generated by the connected medical devices.

Co-funded by
the European Union

2.3.1. SELF-SOVEREIGN IDENTITY SOLUTION (LUS4MED)

CYLCOMED proposes a decentralized IAM based on self-sovereign identity (SSI) to protect patient privacy and the access to their sensitive data. Atos provides LuS4MED, an SSI solution, ensuring only authenticated users access CMD data, thus preventing breaches and tampering. LuS4MED gives users with full control over their identity, enhancing security and privacy. It follows W3C and Gaia-X standards, facilitating issuance, verification, and storage of verifiable credentials (VCs). LuS4MED comprises an agent for complex processes and a mobile app for user interaction, ensuring secure data management and access. The LuS4MED Agent manages SSI functionalities (issuing and verifying VCs on behalf of hospitals), connects with backend services through a ReST API and authorizing user access; and the LuS4MED Mobile app, for storing data and VCs in a wallet, easing onboarding and login processes by presenting VCs for accessing hospital services and data.

Some specific requirements for this tool are included in table 2.1.1:

Component	**Req. No.**	**Req. Type**	**Description**
LuS4MED	LuS4MED 01	Functional	An API MUST be provided for interacting with the authorisation system.
LuS4MED	LuS4MED 02	Functional	The user MUST be registered and hold a VC for accessing the patients' data

Table 2.1.1. Specific functional requirements for LuS4MED tool

2.3.2. DATA PROTECTION SOLUTION (FE4MED)

CYLCOMED provides a data protection solution (FE4MED) for securing medical data during the transmission process from the CMD to the hospital information system and when stored, avoiding unauthorized access and protecting the data in case of data leakage. It employs the Attribute-Based Encryption (ABE) cryptographic solution, to control data access based on attributes, ensuring confidentiality and integrity, as well. FE4MED uses CP-ABE, providing fine-grained access control via flexible sharing policies. It allows only users with specific attributes to decrypt certain data, enhancing privacy and security. FE4MED's modular design includes entities like the Key Issuer Authority, and the Encryptor and Decryptor entities, facilitating the key generation, encryption, and decryption processes, respectively. The system complies with GDPR and other privacy regulations, offering scalable and efficient data protection in healthcare scenarios. Some specific requirements for this tool are included in table 2.1.2:

Component	**Req. No.**	**Req. Type**	**Description**
FE4MED	FE4MED 01	Functional	Patients' data MUST be provided in JSON format for being encrypted
FE4MED	FE4MED 02	Functional	A REST API MUST be provided for communicating with the CMDs and hospital system for allowing encryption and decryption data, respectively.
FE4MED	FE4MED 03	Functional	A system administrator MUST set the attributes and policies for encrypting/decrypting patients' data
FE4MED	FE4MED 04	Functional	The FE4MED MUST generate logs file with appropriate information to be monitored

Co-funded by
the European Union

FE4MED	FE4MED 05	Functional	The allowed users MUST provide their attributes for retrieving decrypted data.

Table 2.1.2. Specific functional requirements for FE4MED tool

2.3.3. OPEN POLICY AGENT (C-OPA)

CYLCOMED Oper Policy Agent (C-OPA) leverages the open-source tool Open Policy Agent (OPA), which leverages a datalog-inspired programming language (Rego) and enables policy writers to express access control rules as high-level, declarative logic queries on data product service requests. Within the project, C-OPA is complementing LuS4MED in storing and enforcing access policies to data or services, acting as policy decision and enforcement point e.g. for requests addressed from and to the medical health platforms and the access to the encrypted data, leveraging the properties and roles issued by the SSI (LuS4MED). C-OPA also ensures that only trusted policies are enforced and can act both interactively and in server mode, leveraging state-of-the art technologies like Envoy proxy and Nginx server.

2.4. Connected Medical Device Integrity

A detailed description was already included in deliverable D3.1 [4] and will not be included here again. The tools are described in deliverable D5.1 [2], updated requirements for these tools will be presented in this chapter.

As stated in D6.1 [3], section 1.3.2, the Service Management Tools aim to provide secure management of connected medical devices.

While enabling for remote updates the tools will ensure that delivered solutions are up to date with latest security patches and in the case of faulty configurations, these are not increasing the attack surface.

While controlling the delivery of updates a security scan can be provided to inspect the software for known vulnerabilities before deployment.

The service management tools will also be used to deploy components of the CYLCOMED toolbox.

This activity corresponds to T5.4 of CYLCOMED project. Certification of medical devices is a complicated, expensive, and time-consuming process. For this purpose, the strategy is to incorporate the security features that result from CYLCOMED in a standard external Linux-based board, with enough CPU power so that the performance of essential functionalities is not compromised; for this purpose, it is connected via a serial channel to the medical monitoring device (legacy device) with monitoring functionalities preserved from cybersecurity hazards. The external module is intended to interoperate with the user interface software component of the medical monitoring device, e.g. to report about the status of the software integrity. Besides, the infusion pump controller functionality is also embedded into the external board. It has means to communicate with other medical devices such as the infusion pump tree, and the Hospital Information System (HIS) via ethernet, to report on the vital signs evolution of the patient. These gateway functionalities will be performed following the security recommendations mandated by the regulatory norms. This strategy will be followed using a legacy device (Vision Air Equipment), and the focus will be to achieve an implementation that can be used as a module for legacy devices in the Intensive Care Unit scenario.

Co-funded by the European Union

Of course, the procedure to upgrade the functionality of another device will require an integration toolkit with a protocol that includes the generation of cybersecurity alarms. The manufacturer of the legacy device will have to adapt the external board with an open protocol generated in CYLCOMED. A User´s guide for the implementation of the external board connection to the Vision Air Multiparameter monitor will be developed, including the communication protocol and the specific test actions to verify the proper integration.

The CMD will interact with CYLCOMED through a single board computer, which is the main objective of the connected medical device integrity solution that will be the core of pilot 1 around which the other tools will provide their benefits.

Table 2 shows the requirements from a functional point of view:

NMT component	**Req. No.**	**Req. Type**	**Description**
Sensing	UC1-NMT 01	Functional	Within X distance of range from the NMT target level, the sensing component shall identify overshooting or undershooting conditions.
Sensing	UC1-NMT 02	Functional	Time between NMT samples must take into consideration perturbations due to noise or patient condition or evolution.
Sensing	UC1-NMT 03	Functional	The sensing component shall perform as required in all situations. Patient behaviour has a Fuzzy nature.
Sensing	UC1-NMT 04	Functional	The sensing component shall perform as required in the face of defined component failures arising within the system.
System	UC1-NMT 05	Design Constraint	All data samples shall represent discrete NMT levels.
System	UC1-NMT 06	Design Constraint	All data samples should include common types of patients.
System	UC1-NMT 07	Design Constraint	Noise or unexpected patient´s behaviour shall be considered.
System	UC1-NMT 08	Design Constraint	The format of each data sample shall be representative of that which is captured using sensors deployed on the RGB NMT monitor.
System	UC1-NMT 09	Design Constraint	Each data sample shall assume sensor data is representative of current NMT values.
System	UC1-NMT 10	Design Constraint	The data samples shall include a sufficient range of levels belonging to the particular relaxometry category.
System	UC1-NMT 11	Design Constraint	The data samples shall include examples with acceptable levels of certitude giving a partial view of noise and patient´s behaviour.
System	UC1-NMT 12	Design Constraint	The data samples shall include a sufficient range of patient´s configurations reflecting the e.g. adaptability level of the patient to the drug.

Co-funded by
the European Union

Predict/ Control	UC1-NMT 13	Functional	Controller behaviour should be reasonably proximate to the target for more than X% of the operation time.
Predict/ Control	UC1-NMT 14	Functional	Distance to target shall not be always greater than X%.
Predict/ Control	UC1-NMT15	Functional	All sources of failure present in the data samples must be correctly identified.
Sensing	UC1-NMT16	Non-Functional	The sensing system shall use redundancy with the patient´s model to protect the patient from potential threats on sensors.
System	UC1-NMT 17	Non-Functional	Adversarial training shall be used during design to increase their robustness against adversarial conditions.
System	UC1-NMT 18	Non-Functional	Input data should be filtered during operation to remove features (such as addition of specific noise), which renders the data malicious and adversarial.

Table 2: Functional and nonfunctional requirements

2.5. Cybersecurity Dashboard

As indicated in D3.1 [4] the CYLCOMED Security Dashboard (provided by Atos) is a main component of the CYLCOMED framework, devoted to providing a centralized platform for monitoring and managing the cybersecurity of connected medical devices. “Its main objective is to collect, process and analyse security-related data from different sources, such as the AI Behavioural Analysis component, network traffic monitoring, and vulnerability assessments, to provide real-time information about the security status of the devices”.

A detailed description was already included in deliverable D3.1 [4] and will not be included here again. The tools are described in deliverable D5.1 [2].

3. Evolution of Use Cases

3.1. Generic Scenario for Connected Medical Devices

On deliverable D3.1 [4] the data journey was presented to classify the requirements by the different components and to align the use cases of the two pilots. Additionally, it also aligns with the available market solutions.

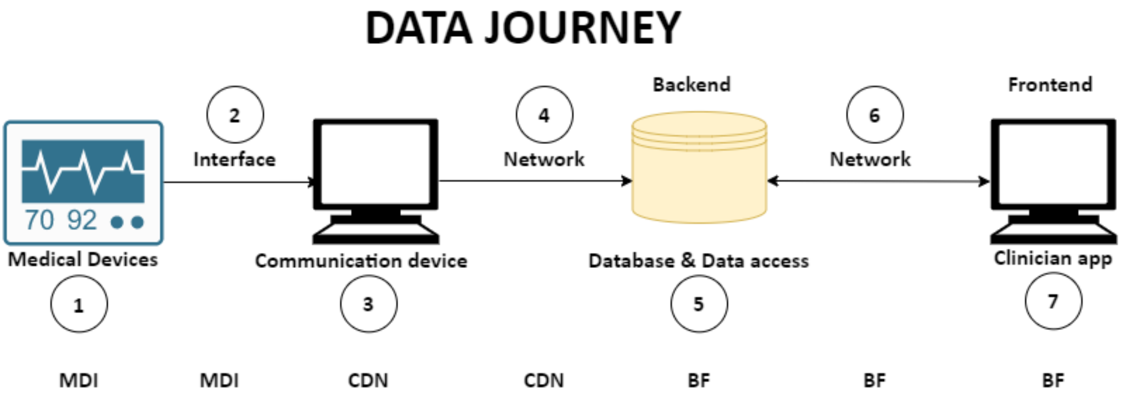

Figure 1: Data Journey

For ease of description the data flow has been separated in three areas:

- Medical Devices and their interface (1st and 2nd steps): MDI
- Communication device and network (3rd and 4th steps): CDN
- Backend & Frontend (5th, 6th and 7th steps): BF

The requirements in Appendix B use MDI, CDN, and BF as prefixes in their IDs to indicate the stage in the data journey where they are applicable.

3.2. Pilot 1: Cybersecurity in Hospital Equipment for Covid-19 ICU patients

The table below shows the tools in the CYLCOMED toolbox that will be integrated and evaluated in pilot 1 (updated from D6.1 [3]:

AI-based CMD Behavioural Analysis & Log Monitoring	
CMD Log Monitoring [LOMOS]	☑
AI-Behavioural Analysis [LADS]	☑
Connected Medical Devices and Services Management Tools	
CMD Security Maintenance [MENDER]	☑
Ansible playbook scanner	☑
Identity & Access Management and Data Protection for Connected Medical Devices	

Co-funded by the European Union

uSelf for Medical Data [Lus4MED]	☑
Functional Encryption for Medical Data [FE4MED]	☑
Connected Medical Device integrity	
Device Integrity Check	☑
CYLCOMED Security Dashboard	
Cybersecurity Dashboard	☑

Table 3: Tools for Pilot 1

The main components of the RGB use case are:

Medical device. It is used for the closed-loop control of neuromuscular transmission in the Intensive Care Unit (ICU). The data are transmitted to a backend server for its consultation by the healthcare personnel. For this operation, the medical device is connected to the Raspberry.

Raspberry PI. An external computing module for connecting and controlling the infusion pump tree. Its software OS is Linux.

Infusion pump tree. It is used to deliver to the patient the drugs according to the dose rate calculated by the medical device.

Smartphone. It is an optional device that can be used as a bridge between the Raspberry and the Backend server. Android OS is running on the smartphone.

Backend server. It receives the data from the Raspberry Linux OS running on the Raspberry. The use of Django framework is done for the client-server.

Web application. The data stored in the server can be accessed through a web application by healthcare personnel or system administrators.

The medical device is connected to the Raspberry via an RS-232 serial channel and the Raspberry is connected to the Infusion pump tree via LAN.

Two different options are being investigated for the connection between the Raspberry and the Backend server:

Option 1. Bluetooth BL (BLE) connection to a Smartphone that transmits the data to the Backend server via Wi-Fi.

Option 2. The Raspberry directly transmits the data to the Backend server via Wi-Fi.

3.3. Pilot 2: Cybersecurity for telemedicine platforms

Regarding D3.1 [4], Pilot 2 has been updated being split into different deployment to offer the possibility to exploit the most from the CYLCOMED framework.

A major deployment, (deployment A from now on), focuses on real-world hospitals needs and respect all the constraints (legal, ethical) encountered. This deployment is the one that is described in the clinical protocols[1]. and ensures the integration of the tools into a real-world telemedicine environment. The primary focus of deployment A is the exploitation of the MHP telemedicine platform to monitor health conditions of paediatric cardiac patients.

The second part of Pilot 2 is the deployment outside the hospital premises (deployment B from now on) and takes a broader approach, integrating all the possible tools to test and evaluate as much as possible the toolbox. Not involving real patients, this deployment allows for a controlled evaluation, reducing the concerns and allowing for a more "experimental" approach to the evaluation and refining of the tools.

The CYLCOMED framework is equally leveraged through the involvement of the hospital personnel in providing feedback and ideas during the whole process.

The table below shows the tools in the CYLCOMED toolbox that will be integrated and evaluated in pilot 2 (updated from D6.1 [3]:

	Pilot 2	
	Deployment A (on premises)	Deployment B (on cloud)
AI-based CMD Behavioural Analysis & Log Monitoring		
CMD Log Monitoring [LOMOS]	☑	☑
AI-Behavioural Analysis [LADS]	☑	☑
Connected Medical Devices and Services Management Tools		
CMD Security Maintenance [MENDER]	□	□
Ansible playbook scanner	□	□
Identity & Access Management and Data Protection for Connected Medical Devices		
uSelf for Medical Data [Lus4MED]	☑	☑
Functional Encryption for Medical Data [FE4MED]	☑	☑
Connected Medical Device integrity		
Device Integrity Check	□	□
CYLCOMED Security Dashboard		
Cybersecurity Dashboard	☑	☑

Table 4: Tools for pilot 2

In the telemedicine platform data are collected from a variety of CMDs provided to the patient to be used in his home environment. The CMDs employed in the platform communicates the acquired data via Bluetooth to the Hub, (a specific mobile phone, provided by Mediaclinics

[1] the clinical protocol is currently in the finalisation phase, minor adjustments can be expected to further refine and enhance efficacy.

together with the sensors) locked on MHP Mobile Application, where the patient can also visualize the latest measurements acquired.

The MHP Mobile Application receives data from the CMDs and sends them to the backend server through HTTPS (using a Wi-Fi network or mobile phone data connection), where data is stored. No storage is performed on the mobile application, that serves only as a middleware for data acquisition. Once data are stored into the backend server, Health Care professionals can visualize them through the MHP Web application, which can be accessed from any standard browser.

Co-funded by
the European Union

4. Map of Assets and Requirements

Table 5 provides updated information of the different categories of cybersecurity requirements covered by the assets brought into the CYLCOMED project.

These categories are now mapped to the toolbox requirements in Appendix C

Category	Description	CYLCOMED Tools	Security Measures
Cryptography	This includes the algorithms, protocols, key management, and procedures for encrypting data at rest and in motion.	Functional Encryption for Medical Data [FE4MED]	CP-ABE schema will be applied to health records on specific scenarios. .
Identity and Access Management	This includes the authentication mechanisms used for accessing data, for establishing secure connections, and access permissions.	uSelf for Medical Data [LuS4MED]	Decentralised user access control following SSI paradigm will be applied for accessing data, providing VC.
Configuration	General security principles applied to the configuration of devices, network systems, and services.	Functional Encryption for Medical Data [FE4MED] uSelf for Medical Data [LuS4MED] Open Policy Agent [C-OPA] AI-Behavioural Analysis [LADS] CMD Log Monitoring [LOMOS]	Makes it possible to update devices and services promptly and reliably with security patches. Also, Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working deployment state declared in the Git repository. This allows to easily recover from configuration tampering. Since the Git repository is the "single source of truth", it is also possible to automatically detect misconfigured services or devices. Moreover, besides the system administrator, no one else needs to have access to devices and services, thus dramatically reducing the attack surface.
Design	This includes design principles applied to the device/network/service.	Functional Encryption for Medical Data [FE4MED] uSelf for Medical Data [LuS4MED] Open Policy Agent [C-OPA] AI-Behavioural Analysis [LADS]	Modular design and privacy by design is applied on solution. Automation shortens deployment time and ensures reproducibility of deployment states. This makes it possible to update devices and services promptly and reliably with security patches. In turn, reproducibility dramatically reduces the time needed to recover from severe production incidents caused by faulty deployments or security breaches as Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working

Co-funded by the European Union

Category	Description	CYLCOMED Tools	Security Measures
		CMD Log Monitoring [LOMOS]	deployment state declared in the Git repository.
Secure Communication	Considerations that must be considered when establishing connection, exchanging information and allowing connection.	Functional Encryption for Medical Data [FE4MED] uSelf for Medical Data [LuS4MED] Open Policy Agent [C-OPA] AI-Behavioural Analysis [LADS] CMD Log Monitoring [LOMOS]	Components connect to devices and cloud services using mutual TLS.
Software Security	Measures were considered to make the software secure.	Security Dashboard AI-Behavioural Analysis [LADS] CMD Security Maintenance [MENDER]	By developing a correlation engine to process the events and raise security alarms when a threat is detected, the Security Dashboard contributes to software security. The LADS component uses AI and Machine Learning technologies to model normal behaviour and detect abnormalities, it indirectly contributes to making the software more secure.

Co-funded by the European Union

Category	Description	CYLCOMED Tools	Security Measures
Monitoring	Includes every monitoring system used to monitor device/service/system accesses, performances, behaviour, configuration, changes of credentials, etc.	Functional Encryption for Medical Data [FE4MED] uSelf for Medical Data [LuS4MED] Open Policy Agent [C-OPA] Security Dashboard AI-Behavioural Analysis [LADS]	FE4MED service activity audit log. Authentication activity audit log. The Git repository is the "single source of truth", so it is possible to automatically detect misconfigured services or devices because their runtime configuration would be different than that in the Git repository. Also, the Git repository stores information about who modified the platform state when, thus furnishing an audit trail. The Security Dashboard will provide an integrated view of all security events generated by the various tools within the CYLCOMED toolbox. It will consolidate monitoring system for device/service/system accesses, performances, behaviour, configuration, changes of credentials, etc. The main functionality of the LADS component, revolves around monitoring the logs generated by Connected Medical Devices (CMDs) or the platform that manages CMDs, which is a core component of security monitoring
Integrity	Measures to maintain data/device/system/service integrity.	Functional Encryption f or Medical Data [FE4MED] uSelf for Medical Data [LuS4MED] Open Policy Agent [C-OPA] AI-Behavioural Analysis [LADS]	Reproducibility allows to recover from production incidents caused by faulty deployments or security breaches as Toolbox services and devices can swiftly be reverted to a previous, known-to-be-working deployment state declared in the Git repository. Since the Git repository is the "single source of truth", it is also possible to automatically detect misconfigured services or devices. By identifying anomalies in logs due to attacks or failures, the LADS component indirectly contributes to the maintenance of data/device/system/service integrity. It facilitates the detection of events that could potentially compromise the integrity of the system
Data protection mechanisms	Mechanisms to maintain data secured.	Functional Encryption for Medical Data [FE4MED]	Data encryption by FE4MED schemes Decentralised authentication mechanisms for accessing data

Category	Description	CYLCOMED Tools	Security Measures
		uSelf for Medical Data [LuS4MED] Security Dashboard	The Security Dashboard tool will normalize, enrich, and process the security events, which are measures taken to protect the data collected and used by the tool itself
Privacy	Measures to protect data privacy.	Functional Encryption for Medical Data [FE4MED] uSelf for Medical Data [LuS4MED]	Use of Privacy Enhanced techniques (FE4MED) for protecting user data privacy Use of SSI mechanisms for user access control to data

Table 5 Requirements Mapping

5. Conclusions

This deliverable is an update and complements its first version, deliverable D3.1 [4]. It reflects the essential steps toward the successful completion of CYLCOMED project's objectives. It has collected the sources to establish the baseline analysis of regulations and standards relevant to the cybersecurity of connected medical devices. Toolbox assets and the pilots' requirements are also included and have been updated or completed from deliverable D3.1 [4].

Requirements have been updated and reorganized. Appendix A is a consolidation Appendix A: Requirements (Legal and Standards) and Appendix B: Requirements from Standards and Best Practices from D3.1 [4]. Appendix B covers the requirements for the connected medical devices solutions organized by the components introduced in the generic scenario for connected medical devices, and the requirements for the toolbox that were part of this appendix in deliverable 3.1, have now been separated in Appendix C

WP5 (Toolbox) and WP6 (Pilots) should benefit for the requirements collected in this deliverable.

Appendix A should be helpful for anyone concerned about regulations and best practices on cybersecurity when developing a solution to integrate medical devices data

Appendix B should be helpful for anyone planning to develop a solution to integrate medical devices data when planning the cybersecurity policy

Appendix C should be useful for anyone planning to develop a toolbox to manage the cybersecurity when integrating medical devices solutions

Co-funded by
the European Union

References

[1] CYLCOMED, “D2.1 Analysis of Ethical, Legal, Data Protection Frameworks,” 2023

[2] CYLCOMED, “D5.1 Toolbox prototype,” 2024

[3] CYLCOMED, “D6.1 Pilot planning and evaluation strategy incl. clinical trial submission package,” 2023

[4] CYLCOMED, “D3.1 Baseline analysis, requirements and specifications,” 2023

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0745

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0746

[7] https://health.ec.europa.eu/system/files/2022-01/md_cybersecurity_en.pdf

[8] https://www.echr.coe.int/documents/convention_eng.pdf

[9] https://www.coe.int/en/web/data-protection/convention108-and-protocol

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[13] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014L0053-20221227

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0020

[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0536

[18] https://www.wma.net/what-we-do/medical-ethics/declaration-of-helsinki/

[19] Protection of health-related data - Recommendation CM/Rec(2019)2 (coe.int)

[20] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010

[25] https://www.nist.gov/cyberframework

[26] https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/enisa_en

[27] ENISA Baseline Security Recommendations for IoT in the context of Critical Infrastructures

[28] Guidelines for Securing the Internet of Things – Secure supply chain for IoT

[29] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool

[30] https://www.enisa.europa.eu/news/enisa-news/better-security-measures-for-smartphones-enisa-has-created-a-smashing-new-tool

[31] https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/@@download/fullReport

[32] https://www.enisa.europa.eu/publications/security-aspects-of-virtualization/@@download/fullReport

[33] https://www.nist.gov/system/files/documents/pml/div683/conference/May_final.pdf

[34] https://www.nist.gov/cybersecurity

[35] NIST Special Publication 1800-1 Securing Electronic Health Records on Mobile Devices

[36] NIST Special Publication 18001-11 Data Integrity, Recovering from Ransomware and Other Destructive Events

[37] NIST Special Publication 18001-15 Securing Small-Business and Home Internet of Things (IoT)

Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)

[38] NIST Special Publication 1800-21 NIST Special Publication 1800-21 Securing Tele-Health Remote Patient Monitoring Ecosystem

[39] NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)

[40] NIS Special Publication 800-190 Application Container Security Guide

[41] https://www.iso.org/about-us.html

[42] https://www.iso.org/standard/iso-iec-27000-family

[43] https://www.iso.org/news/2015/12/Ref2032.html

[44] https://www.iso.org/iso-13485-medical-devices.html

[45] https://cloudsecurityalliance.org/

[46] https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

[47] https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/

[48] https://cloudsecurityalliance.org/artifacts/csa-iot-security-controls-framework-v2/

[49] https://www.bsa.org/about-bsa

[50] https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

[51] https://content.securecodealliance.com/SCA-BoK.pdf

[52] https://ec.europa.eu/docsroom/documents/33162

[53] https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf

[54] https://www.imdrf.org/sites/default/files/2023-04/IMDRF%20Principles%20and%20Practices%20of%20Cybersecurity%20for%20%20Legacy%20Medical%20Devices%20Final%20%28N70%29_1.pdf

[55] https://ec.europa.eu/newsroom/article29/items/612053/en?doc_id=49826

[56] https://ec.europa.eu/newsroom/article29/items/611233

[57] https://ec.europa.eu/newsroom/article29/items/622227/en

[58] https://ec.europa.eu/newsroom/article29/items/612048/en

[59] https://ec.europa.eu/newsroom/article29/items/611236/en

[60] https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

[61] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf?ref=CLIBLP

[62] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en

[63] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

[64] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

[65] file:///C:/Users/u0161701/Downloads/altai_final_14072020_cs_accessible2_jsd5pdf_correct-title_3AC24743-DE11-0B7C-7C891D1484944E0A_68342%20(3).pdf

[66] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf?trk=public_post_comment-text

[67] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

Co-funded by
the European Union

Appendix A. Requirements (Legal, Standards, and Best Practices)

This appendix covers the requirements related to cybersecurity coming from legal, standards or best practices, ordered by the source. They have been consolidated from the two different appendixes in deliverable 3.1 [4], Appendix A: Requirements (Legal and Standards) and Appendix B: Requirements from Standards and Best Practices. New requirements have been incorporated as well, mainly from the AI Act, the Cyber Security Act and the ISO 42001 standard. The code for these new requirements are in yellow.

Requirements can be duplicated as they could be part of different standards and guides.

The requirements from ENISA were compiled based on the following references:

ENISA Baseline Security Recommendations for IoT in the context of critical infrastructures [27]

ENISA smartphone guidelines tool (SMASHING tool) [29]

ENISA cloud security for healthcare services [31]

ENISA Security aspects of virtualisation [32]

ENISA procurement guides for cybersecurity in hospitals [67]

Category	Code	Name	Description	Source
Accountability	Account-1	Role Determination	It is vital to determine roles (controller and processor) and accordingly choose the governance set-up of CYLCOMED.	GDPR
Accountability	Account-2	Role Determination	In the case of joint controllership, determine respective responsibilities for compliance. The relationship between controller and processor shall be governed by a contract or other legal act.	GDPR
Accountability	Account-3	Legal Basis	Lawfully processing personal data must be ensured by defining a valid legal basis for the processing of personal data.	GDPR
Accountability	Account-4	Legal Basis	When processing special categories of personal data (e.g., health data), an additional legal basis must be established as stipulated by Article 9 (e.g., explicit consent).	GDPR
Accountability	Account-5	Legal Basis	The legal basis must be established before the processing takes place.	GDPR
Accountability	Account-6	Consent	For lawful processing of personal data in paediatric patients (less than 16 years), consent must be obtained from the holder of parental responsibility over the child.	GDPR
Accountability	Account-7	Consent	It must be ensured that data subjects can withdraw their consent at any time and	GDPR

Co-funded by the European Union

Category	Code	Name	Description	Source
			should be made aware of this right before granting consent.	
Accountability	Account-8	Transparency	The data controller should ensure that it is compliant with its transparency obligations.	GDPR
Accountability	Account-9	Purpose Limitation	The controller must collect data for specified, explicit, and legitimate purposes, and not further process the data in a manner that is incompatible with the purposes for which they were collected.	GDPR
Accountability	Account-10	Data Minimisation	The data minimisation principle requires that the data collected be relevant and limited to what is strictly necessary for the purposes for which they are processed.	GDPR
Accountability	Account-11	Data Accuracy	Personal data need to be accurate and checked regularly and kept up to date to guarantee accuracy.	GDPR
Accountability	Account-12	Data Accuracy	The platform must enable corrections in an easy and timely way to facilitate the obligation of the right to rectification.	GDPR
Accountability	Account-13	Storage Limitation	The controller must ensure that personal data is kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.	GDPR
Accountability	Account-14	Storage Limitation	Time limits should be established by the controller for erasure or for a periodic review to ensure that the data are kept for no longer than necessary.	GDPR
Accountability	Account-15	Storage Limitation	As soon as personal data are no longer needed for the purposes for which they were collected, controllers are obliged to erase or anonymise collected data.	GDPR
Accountability	Account-16	Storage Limitation	The controller shall be able to justify why the period of storage is necessary for the purpose and the personal data in question.	GDPR
Accountability	Account-17	Storage Limitation	Controllers shall determine what personal data and length of storage is necessary for back-ups and logs.	GDPR
Accountability	Account-18	Storage Limitation	Controllers should beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their “temporary” storage.	GDPR

Category	Code	Name	Description	Source
Accountability	Account-19	Integrity and Confidentiality	CYLCOMED must comply with the principle of integrity and confidentiality.	GDPR
Accountability	Account-20	Integrity and Confidentiality	Appropriate technical and organisational measures shall be implemented to protect information and personal data processed against unauthorised or unlawful access, disclosure, dissemination, alteration, destruction, or accidental loss, particularly when the processing involves transmission over a network.	GDPR
Accountability	Account-21	Integrity and Confidentiality	Regularly review and test software, hardware, systems and services, etc. to uncover vulnerabilities of the systems supporting the processing.	GDPR
Accountability	Account-22	Integrity and Confidentiality	Access control management must be in place.	GDPR
Accountability	Account-23	Integrity and Confidentiality	Access limitation (agents) – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly.	GDPR
Accountability	Account-24	Integrity and Confidentiality	Access limitation (content) – In the context of each processing operation, limit access to only those attributes per data set that are needed to perform that operation.	GDPR
Accountability	Account-25	Integrity and Confidentiality	Access segregation - shape the data processing in a way that no individual needs comprehensive access to all data collected about a data subject.	GDPR
Accountability	Account-26	Integrity and Confidentiality	Transfers shall be secured against unauthorised and accidental access and changes.	GDPR
Accountability	Account-27	Integrity and Confidentiality	Data storage shall be secure from unauthorised access and changes.	GDPR
Accountability	Account-28	Integrity and Confidentiality	Personal data and back-ups/logs should be pseudonymised as a security measure to minimise risks of potential data breaches, for example using hashing or encryption.	GDPR
Accountability	Account-29	Integrity and Confidentiality	Address information system disaster recovery and business continuity requirements to restore the availability of personal data following up major incidents.	GDPR

Co-funded by the European Union

Category	Code	Name	Description	Source
Accountability	Account-30	Integrity and Confidentiality	All categories of personal data should be protected with measures adequate with respect to the risk of a security breach.	GDPR
Accountability	Account-31	Integrity and Confidentiality	Data presenting special risks should, when possible, be kept separate from the rest of the personal data.	GDPR
Accountability	Account-32	Integrity and Confidentiality	CYLCOMED must have in place security incident response management (routines, procedures and resources to detect, contain, handle, report and learn from data breaches)	GDPR
Accountability	Account-33	Integrity and Confidentiality	CYLCOMED design must facilitate compliance with the reporting obligations in the case of a personal data breach.	GDPR
Accountability	Account-34	Right to Information	CYLCOMED design must facilitate the exercise of the data subject’s right to information.	GDPR
Accountability	Account-35	Right to Information	The information regarding processing must be provided “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”.	GDPR
Accountability	Account-36	Right to Information	The information must be given in writing, including in electronic form, as well as orally if requested.	GDPR
Accountability	Account-37	Right of Access	CYLCOMED design must facilitate the exercise of the data subject’s right to information.	GDPR
Accountability	Account-38	Right to Rectification	CYLCOMED design must enable the exercise of the right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.	GDPR
Accountability	Account-39	The Right to Erasure	CYLCOMED design must enable data subjects to have personal data erased.	GDPR
Accountability	Account-40	Right to Data Portability	CYLCOMED design should enable the data subject to have the data transferred directly from one controller to another in an interoperable format.	GDPR
Accountability	Account-41	Right to Data Portability	CYLCOMED designers are encouraged to develop interoperable formats and tools (e.g., download tools and Application Programming Interfaces), which will facilitate the exercise of a data subject right to data portability.	GDPR

Co-funded by
the European Union

Category	Code	Name	Description	Source
Accountability	Account-42	DPIA	Bearing in mind the scope and nature of processing activities that will take place, it is required to conduct the data protection impact assessment (DPIA).	GDPR
Accountability	Account-43	High-Risk Processing	It is mandatory to consult the supervisory authority prior to high-risk processing in the absence of measures taken by the controller to mitigate the risk.	GDPR
Accountability	Account-44	DPO	The processing activities performed through CYLCOMED will require the involvement and oversight of a data protection officer (DPO).	GDPR
Accountability	Account-45	Records of Processing	To demonstrate compliance the controller or processor should maintain records of processing activities under its responsibility.	GDPR
Accountability	Account-46	Data Transfer	In case of transfer of data, CYLCOMED must comply with rules on international transfers of data.	GDPR
IT Security	ITS-1	Cybersecurity Measures	Appropriate and proportionate technical, operational and organisational measures should be taken to manage the risks posed to the security of network and information systems.	NIS2
IT Security	ITS-2	Cybersecurity Measures	Cybersecurity risk-management measures should be based on an all-hazards approach.	NIS2
IT Security	ITS-3	Cybersecurity Measures	Cybersecurity risk-management measures shall include policies on risk analysis and information system security.	NIS2
IT Security	ITS-4	Cybersecurity Measures	Cybersecurity risk-management measures shall include incident handling.	NIS2
IT Security	ITS-5	Cybersecurity Measures	Cybersecurity risk-management measures shall include business continuity, such as backup management and disaster recovery, and crisis management.	NIS2
IT Security	ITS-6	Cybersecurity Measures	Cybersecurity risk-management shall include security in the network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure measures.	NIS2

Co-funded by
the European Union

Category	Code	Name	Description	Source
IT Security	ITS-7	Cybersecurity Measures	Cybersecurity risk management shall include basic cyber hygiene practices and cybersecurity training measures.	NIS2
IT Security	ITS-8	Cybersecurity Measures	Cybersecurity risk-management measures shall include policies and procedures regarding the use of cryptography and, where appropriate, encryption.	NIS2
IT Security	ITS-9	Cybersecurity Measures	Cybersecurity risk-management measures shall include human resources security, access control policies, and asset management.	NIS2
IT Security	ITS-10	Cybersecurity Measures	Measures shall include policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	NIS2
IT Security	ITS-11	Cybersecurity Measures	Measures shall include the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	NIS2
IT Security	ITS-12	Incident Notification	CYLCOMED design must facilitate compliance with the reporting obligations in the case of any incident that has a significant impact.	NIS2
IT Security	ITS-13	Information System Security Risk Analysis	The introduction of medical devices in the environment should be subject to a risk assessment.	MDCG
IT Security	ITS-14	Information System Security Policy	A set of baseline IT security policies should be defined, approved by management, and communicated to employees and relevant external parties.	MDCG
IT Security	ITS-15	Human Resource Security	Security awareness training for employees that operate critical devices and systems should be provided.	MDCG
IT Security	ITS-16	Human Resource Security	Background checks prior to authorising access to key personnel should be in place.	MDCG
IT Security	ITS-17	Systems Configuration	The operating environment must not hinder the application of security measures on the medical device or force the device to operate in lower security settings.	MDCG

Category	Code	Name	Description	Source
IT Security	ITS-18	Systems Configuration	Appropriate security measures for the use of mobile devices and teleworking should be established.	MDCG
IT Security	ITS-19	Cryptography	Encryption when storing sensitive personal data must be in place.	MDCG
IT Security	ITS-20	Cryptography	Encryption of data in transit must be in place.	MDCG
IT Security	ITS-21	Administration Information Systems	Memory protection measures to block arbitrary code execution should be implemented.	MDCG
IT Security	ITS-22	Administration Information Systems	Compatibility of medical device management software with security solutions that counter malicious code must be ensured.	MDCG
IT Security	ITS-23	Administration Information Systems	Only software programs necessary for intended uses should be installed.	MDCG
IT Security	ITS-24	Authentication and Identification	User access management should be in place (credentials for accessing software applications or devices, user access policy etc.).	MDCG
IT Security	ITS-25	Access rights	The principle of least privilege to user workstations and connected devices should be applied.	MDCG
IT Security	ITS-26	Access rights	Least privileges must consider data minimisation per role.	MDCG
IT Security	ITS-27	Procedure	The use of end-of-life third-party components and devices on the operating environment should be avoided.	MDCG
IT Security	ITS-28	Physical and Environmental Security	Roles and access rights, including those for physical access to medical devices, should be defined.	MDCG
IT Security	ITS-29	Physical and Environmental Security	Use of segregated, secure areas with appropriate access controls should be in place.	MDCG
IT Security	ITS-29	Detection	Software integrity checks and device authentication mechanisms	MDCG
IT Security	ITS-30	Detection	Data integrity should be ensured e.g. through hashing, integrity checks.	MDCG

Co-funded by
the European Union

Category	Code	Name	Description	Source
IT Security	ITS-31	Asset Management	Assets should be catalogued in an inventory of all medical devices, servers and workstations.	MDCG
IT Security	ITS-32	Logs correlation and analysis	The medical device integration solution must be able to monitor the correct operation of the equipment.	MDCG
IT Security	ITS-33	Disaster Recovery Management	Data recovery mechanisms to restore data from critical systems should be implemented.	MDCG
IT Security	ITS-34	Disaster Recovery Management	A disaster recovery plan should be developed.	MDCG
IT Security	ITS-35	Security requirements	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks	CRA / ENISA
IT Security	ITS-36	Security requirements	A cybersecurity risk analysis should be conducted and monitored during the complete lifecycle of the product	CRA / ENISA
IT Security	ITS-37	Security requirements	Cybersecurity should be taken into account in every step of the product creation (e.g. secure coding, security by design principles, etc.)	CRA / ENISA
IT Security	ITS-38	Security requirements	Products with digital elements shall be delivered without any known exploitable vulnerabilities	CRA / ENISA
IT Security	ITS-39	Security requirements	A vulnerability assessment should be performed against the digital elements of a product	CRA / ENISA
IT Security	ITS-40	Security requirements	Known exploitable vulnerabilities shall be fixed before the release of the product	CRA / ENISA
IT Security	ITS-41	Security requirements	Products with digital elements shall be delivered with a secure by default configuration, including the possibility to reset the product to its original state	CRA / ENISA
IT Security	ITS-42	Security requirements	In case default configurations foresee an initial/default credential, the same should use a complex and randomly chosen password, different for each product	CRA / ENISA
IT Security	ITS-43	Security requirements	In case default configurations cover cybersecurity items, they should adopt a reasonable level of security for each item	CRA / ENISA

Co-funded by
the European Union

Category	Code	Name	Description	Source
IT Security	ITS-44	Security requirements	The default configuration should be placed in a non-erasable memory	CRA / ENISA
IT Security	ITS-44	Security requirements	A function to reset the product configuration to the default one should be implemented	CRA / ENISA
IT Security	ITS-45	Security requirements	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems	CRA / ENISA
IT Security	ITS-46	Security requirements	In accordance with the nature of the product and to the relevant risks identified in the risk analysis, an appropriate system to provide authentication and authorisation should be implemented	CRA / ENISA
IT Security	ITS-47	Security requirements	The access to personal/protected data and to administration/configuration functions should be granted only to authenticated and authorised users	CRA / ENISA
IT Security	ITS-48	Security requirements	In accordance with the nature of the product and to the relevant risks identified in the risk analysis, physical unauthorized access should be forbidden	CRA /ENISA
IT Security	ITS-49	Security requirements	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms	CRA / ENISA
IT Security	ITS-50	Security requirements	Data stored in a product's internal memory should be encrypted at rest using current non-deprecated technology	CRA / ENISA
IT Security	ITS-51	Security requirements	Transmission protocols used to send/receive data should support encrypted communications and enable them by default	CRA / ENISA
IT Security	ITS-52	Security requirements	The product should implement symmetric or asymmetric encryption schemes (including PKIs) to ensure that confidentiality of exchanged data is protected	CRA / ENISA
IT Security	ITS-53	Security requirements	protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions	CRA / ENISA

Co-funded by
the European Union

Category	Code	Name	Description	Source
IT Security	ITS-54	Security requirements	Integrity of data, programs and configurations stored in the product's internal memory should be ensured using current non-deprecated technology, e.g. hashing	CRA / ENISA
IT Security	ITS-55	Security requirements	Transmission protocols used to send/receive data should support ways to ensure it is possible to spot data alteration during the transmission (e.g. MACs)	CRA / ENISA
IT Security	ITS-56	Security requirements	The product should implement symmetric or asymmetric encryption schemes (including PKIs) to ensure that the integrity of exchanged data is protected	CRA / ENISA
IT Security	ITS-57	Security requirements	A product should perform self-test to verify integrity of relevant code/information (e.g. firmware)	CRA / ENISA
IT Security	ITS-58	Security requirements	Process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data')	CRA / ENISA
IT Security	ITS-59	Security requirements	data no longer needed should be deleted without delay	CRA / ENISA
IT Security	ITS-60	Security requirements	protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks	CRA / ENISA
IT Security	ITS-61	Security requirements	The product should be hardened against attacks, like for instance distributed denial of service attacks, by implementing, among other things, the following measures if appropriate: • reverse proxies network segmentation • load balancing • rate limiting • redundancy and high availability solutions • backup sites • disaster recovery plans • minimize offered services	CRA / ENISA
IT Security	ITS-62	Security requirements	minimise their own negative impact on the availability of services provided by other devices or networks	CRA / ENISA
IT Security	ITS-63	Security requirements	The product should limit outgoing network connections to what is strictly needed	CRA / ENISA
IT Security	ITS-64	Security requirements	The product should implement measures such as timeouts and exception handling	CRA / ENISA

Co-funded by the European Union

Category	Code	Name	Description	Source
			to avoid generating multiple requests to a busy/not responsive service	
IT Security	ITS-65	Security requirements	be designed, developed and produced to limit attack surfaces, including external interfaces	CRA / ENISA
IT Security	ITS-66	Security requirements	The product's hardware design should limit all the connections and interfaces that are not strictly required for performing the various tasks the product is expected to do	CRA / ENISA
IT Security	ITS-67	Security requirements	If required by a risk assessment, a physical product should include tamper-resistant features	CRA / ENISA
IT Security	ITS-68	Security requirements	The product/service should have all not essential network ports closed as a default configuration	CRA / ENISA
IT Security	ITS-69	Security requirements	Software present in digital product should be designed to avoid having unnecessary entry points (e.g. API) open and available for external unauthorised callers	CRA / ENISA
IT Security	ITS-70	Security requirements	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	CRA / ENISA
IT Security	ITS-71	Security requirements	The product should be designed in a way that gaining unauthorised access to a function or data does not automatically lead to a complete access to all product's functions and data (defence in depth principles)	CRA / ENISA
IT Security	ITS-72	Security requirements	Sensitive data stored in a product's internal memory should be encrypted at rest	CRA / ENISA
IT Security	ITS-73	Security requirements	The product should not store data that is not relevant or necessary to perform its tasks (data minimisation)	CRA / ENISA
IT Security	ITS-74	Security requirements	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions	CRA / ENISA
IT Security	ITS-75	Security requirements	A product should contain a log of cybersecurity related events	CRA / ENISA
IT Security	ITS-76	Security requirements	Access or modification of data, services or functions should be logged	CRA / ENISA

Co-funded by
the European Union

Category	Code	Name	Description	Source
IT Security	ITS-77	Security requirements	Such log should be accessible to the privileged user	CRA / ENISA
IT Security	ITS-78	Security requirements	Logs should be protected from unauthorised modification or corruption	CRA / ENISA
IT Security	ITS-79	Security requirements	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users	CRA / ENISA
IT Security	ITS-80	Security requirements	The company distributing a product or service should provide timely security updates for the software components of the product/service for a reasonable amount of time.	CRA / ENISA
IT Security	ITS-81	Security requirements	A function to automatically check the presence of updates and install them, or notify the user of their presence, should be implemented, and where applicable this should be the default initial configuration	CRA / ENISA
IT Security	ITS-82	Security requirements	A product should provide a secure mechanism to install/implement updates	CRA / ENISA
IT Security	ITS-83	Security requirements	The company distributing a product should notify the user on the availability of updates	CRA / ENISA
IT Security	ITS-84	Security requirements	Manufacturers of the products with digital elements shall identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product	CRA / ENISA
IT Security	ITS-85	Security requirements	Manufacturers of the products with digital elements shall in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates	CRA / ENISA
IT Security	ITS-86	Security requirements	In case vulnerabilities are found they should be classified in accordance with standard severity metrics (e.g. CVSS)	CRA / ENISA
IT Security	ITS-87	Security requirements	vulnerabilities that can be directly fixed by the company should be fixed without delay, in accordance to their severity and the posed risks	CRA / ENISA

Co-funded by the European Union

Category	Code	Name	Description	Source
IT Security	ITS-88	Security requirements	In case a vulnerability is found in a software component of a product (including libraries and third party components), an update should be prepared and distributed as soon as possible	CRA / ENISA
IT Security	ITS-89	Security requirements	Manufacturers of the products with digital elements shall apply effective and regular tests and reviews of the security of the product with digital elements	CRA / ENISA
IT Security	ITS-90	Security requirements	Periodic vulnerability assessment should be executed, especially towards those components that present the highest risk	CRA / ENISA
IT Security	ITS-91	Security requirements	When developing or maintaining software components, automatic tests should be executed whenever a new commit/build/version is prepared, if possible using Continuous Integration/Continuous Deployment (CI/CD) techniques	CRA / ENISA
IT Security	ITS-92	Security requirements	A risk assessment should be re-evaluated whenever there is a significant change in one of the dimensions analysed (new threats, new vulnerabilities, etc.) or a new product release	CRA / ENISA
IT Security	ITS-93	Security requirements	Manufacturers of the products with digital elements shall put in place and enforce a policy on coordinated vulnerability disclosure;	CRA / ENISA
IT Security	ITS-94	Security requirements	Manufacturers of the products with digital elements shall take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements	CRA / ENISA
IT Security	ITS-95	Security requirements	Manufacturers of the products with digital elements shall provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner	CRA / ENISA
IT Security	ITS-96	Security requirements	Security updates should be digitally signed using a Code Signing Certificate to ensure the identity of the issuer	CRA / ENISA

Co-funded by
the European Union

Category	Code	Name	Description	Source
IT Security	ITS-97	Security requirements	Hashes of the updates should be made publicly available with instructions on how to verify them	CRA / ENISA
IT Security	ITS-98	Security requirements	Manufacturers of the products with digital elements shall ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	CRA / ENISA
IT Security	ITS-99	Security requirements	Users should be made aware of the existence of security updates either via automatic distribution, popup, newsletter, etc	CRA / ENISA
IT Security	ITS-100	Security requirements	This notice should contain information about the fixed issues and instructions on how to apply the update	CRA / ENISA
Healthcare providers	HCP-1	Cybersecurity Best Practices	Healthcare providers should consider adopting a risk management process to address the safety, performance, and cybersecurity aspects of medical devices that are connected to their IT infrastructure.	IMDRF
Healthcare providers	HCP-2	Cybersecurity Best Practices	Healthcare providers should implement good physical security to prevent unauthorised physical access to medical devices or network access points.	IMDRF
Healthcare providers	HCP-3	Cybersecurity Best Practices	Healthcare providers should put in place access control measures (e.g. role-based) to ensure only authorised personnel are allowed access to network elements, stored information, services and applications.	IMDRF
Healthcare providers	HCP-4	Cybersecurity Best Practices	Healthcare providers should employ configuration management to identify all current assets and track future configuration changes.	IMDRF
Healthcare providers	HCP-5	Cybersecurity Best Practices	Healthcare providers should update management practices that ensure timely security updates.	IMDRF
Healthcare providers	HCP-6	Cybersecurity Best Practices	Healthcare providers should define session timeout to prevent unauthorised access to devices left unattended for an extended period.	IMDRF

Co-funded by
the European Union

Category	Code	Name	Description	Source
Healthcare providers	HCP-7	Cybersecurity Best Practices	Healthcare providers are encouraged to provide basic cybersecurity training to create security awareness and introduce cyber hygiene practices among all users.	IMDRF
Healthcare providers	HCP-8	Cybersecurity Best Practices	Healthcare providers should establish policies for handling security incidents and mechanisms to mitigate or resolve a security incident and to disclose the related information to internal and external stakeholders.	IMDRF
AI systems	AI-1	AI Cybersecurity	High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle	AI Act
AI systems	AI-2	AI Cybersecurity	A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems	AI Act
AI systems	AI-3	AI Cybersecurity	High-risk AI systems shall technically allow for the automatic recording of events (‘logs’) over their lifetime.	AI Act
AI systems	AI-4	AI Cybersecurity	High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system’s output and use it appropriately	AI Act
AI systems	AI-5	AI Cybersecurity	High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers	AI Act
AI systems	AI-6	AI Cybersecurity	High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use	AI Act
AI systems	AI-7	AI Cybersecurity	The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans	AI Act
AI systems	AI-8	AI Cybersecurity	High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way	AI Act

Co-funded by
the European Union

Category	Code	Name	Description	Source
			as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations ('feedback loops'), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures	
AI systems	AI-9	AI Cybersecurity	High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities	AI Act
AI systems	AI-10	AI Cybersecurity	The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.	AI Act
AI systems	AI-11	AI Cybersecurity	The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set ('data poisoning'), or pre-trained components used in training ('model poisoning'), inputs designed to cause the AI model to make a mistake ('adversarial examples' or 'model evasion'), confidentiality attacks or model flaws	AI Act
AI systems	AI-12	AI Cybersecurity	Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner	AI Act
AI systems	AI-13	AI Cybersecurity	A quality management system shall be documented in a systematic and orderly manner.	AI Act
AI systems	AI-14	AI Cybersecurity	The technical solutions to address AI-specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws.	AI Act
AI systems	AI-15	AI Cybersecurity	AI-specific information security threats related to the AI systems applied and developed by the organization should be monitored. AI-specific information security threats include, but are not limited to, data and model poisoning, model stealing, membership inference and model inversion attacks	ISO 42001

Category	Code	Name	Description	Source
AI systems	AI-16	AI Impact Assessment	A process should be stablished to assess the potential consequences for individuals or groups of individuals and societies that can result from the AI system throughout its life cycle.	ISO 42001
AI systems	AI-17	AI governance	AI system should ensure a fair and responsible use from a safe and ethical point of view.	ISO 42001
AI systems	AI-18	Data quality	Requirements for data quality should be defined ensuring that data used to develop and operate the AI system meet those requirements.	ISO 42001
Cryptography	CRYPTO-1	Data at Rest	Adequate cryptographic algorithms and protocols must be used to protect confidentiality, authenticity and integrity of data and any information at rest (including control messages).	ENISA [27,29,31]
Cryptography	CRYPTO-2	Key Management	Cryptographic keys and materials must be securely managed.	ENISA [27,29,31]
Cryptography	CRYPTO-3	Data in Motion	Adequate cryptographic algorithms and protocols must be used to protect confidentiality, authenticity and integrity of data and any information in motion (including control messages).	ENISA [27,29,31]
Cryptography	CRYPTO-4	Key Recovery	Adequate key recovery processes and technologies must be in place.	ENISA [31]
Cryptography	CRYPTO-5	Risk Analysis	Cryptographic algorithms and protocols must be evaluated based on risk analysis for the data and business.	ENISA [27,29,31]
Cryptography	CRYPTO-6	Policy	Encryption policy must be defined, including controls on cryptographic authentication and integrity, and key management.	ENISA [27]
Identity and Access Management	IAM-1	Risk Analysis	Identification mechanisms, authentication mechanisms and authorisation schemes must be evaluated based on risk analysis for each device and services/communications.	ENISA [27,31,32]
Identity and Access Management	IAM-2	Authentication	Authentication mechanism must be adequate for the context they are in (based on the risk analysis).	ENISA [27,29,32]
Identity and Access Management	IAM-3	Credentials Handling	Authentication credentials, such as biometrics data, passwords, certificates, must be properly protected.	ENISA [27,29]

Category	Code	Name	Description	Source
Identity and Access Management	IAM-4	Log-in Protection	Log-in protection must be employed to protect the system/device from unauthorized access.	ENISA [29]
Identity and Access Management	IAM-5	Authentication strength	The authentication strength must reflect the risk analysis and be adequate for the context at hand.	ENISA [27,29,31]
Identity and Access Management	IAM-6	Account Recovery Mechanism	Adequate account recovery process and mechanisms must be in place.	ENISA [27,31]
Identity and Access Management	IAM-7	Permissions	Permissions must be set considering the principle of least privileges, and the implementation must enforce the defined policies.	ENISA [29,32]
Identity and Access Management	IAM-8	Biometrics	When biometrics are employed, best practices must be employed to guarantee a minimum level of security.	ENISA [29]
Identity and Access Management	IAM-9	Temporal validation	Temporal validity interval authorizations should only be used when the systems are synchronized with a trusted authoritative timeserver. In any other case, this authorization mechanism must not be used.	ENISA [29,32]
Identity and Access Management	IAM-10	Authentication information change	There must be mechanisms and/or processes in place for a user to change its authentication information, like password or any authentication tokens.	ENISA [29]
Identity and Access Management	IAM-11	Anomalous Behaviour	Monitoring systems should be in place to check for anomalous usage patterns and trigger re-authentication (e.g., abnormal change in location, user-language changes).	ENISA [29]
Identity and Access Management	IAM-12	Context data	Context data, like geo-location, IP location, should be used to add security to authentication, whenever possible and in compliance with local laws and regulatory requirements.	ENISA [29]
Identity and Access Management	IAM-13	Authentication Factors	Consider using multifactor authentication for applications/services accessing sensitive data or interfaces.	ENISA [29]
Identity and Access Management	IAM-14	Policies	The system must ensure access policies consider user access data, application interfaces, systems, and the network or network components for each service.	ENISA [29,31]

Category	Code	Name	Description	Source
Identity and Access Management	IAM-15	Privileged Accounts	The number of users and privileged accounts requiring direct access to assets should be limited to the bare minimum.	ENISA [32]
Configuration	CONF-1	Initial setup	Ensure that the initial setup enables a minimum level of security. For example, default passwords and default usernames are changed using the initial setup.	ENISA [27]
Configuration	CONF-2	Security by default	The system should provide minimum security, by deploying and configuring a minimum set of security controls.	ENISA [27,29,32]
Design	DESIGN-1	Firmware access control	The device firmware should be designed to isolate privileged code, processes and ate from portions of the firmware that do not need access to them.	ENISA [27]
Design	DESIGN-2	Hardware isolation	The device should have hardware isolation in place.	ENISA [27]
Physical Security	PHYS-1	Tamper Protection	The device must have hardware tampering solution that don´t rely on network connectivity. There should be mechanisms to control device security settings, such as remotely locking or erasing contents of a device if the device has been stolen.	ENISA [27]
Physical Security	PHYS-2	External Ports	The device should only have the essential physical external ports/interfaces (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.	ENISA [27,32]
Physical Security	PHYS-3	Secure Hardware	Secure hardware (e.g., TEE, SE) should be used whenever possible and appropriate, to store keys, credentials and other sensitive data.	ENISA [29]
Physical Security	PHYS-4	Physical Security Controls	Physical security controls are in place to protect data centres and prevent unauthorized physical access. Controls can include physical authentication mechanisms or electronic monitoring and alarm systems.	ENISA [31]
Secure Communication	SECOM-1	Certificate Handling	The application must use certificate handling: restrict an app's trusted certificates to a small set of known certificates that are used by the backend servers.	ENISA [27,29]

Co-funded by the European Union

Category	Code	Name	Description	Source
Secure Communication	SECOM-2	Data Authenticity	Data in transit must be signed.	ENISA [27]
Secure Communication	SECOM-3	Device Authenticity	Always identify and verify/authenticate the devices connected to the network before trust can be established.	ENISA [27,29]
Secure Communication	SECOM-4	Establishing connection	Connections must be intentionally established, for example, requesting user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services, helping to prevent unauthorised connections.	ENISA [27,32]
Secure Communication	SECOM-5	Rate Limiting	Traffic sent and received by a network should have rate limiting, to reduce the risk of automated attacks.	ENISA [27,32]
Secure Communication	SECOM-6	Restricted Communications	Traffic between untrusted and trusted connections of network environments and virtual instances must be restricted.	ENISA [31]
Secure Communication	SECOM-7	Document interfaces	All allowed services, protocols, ports and compensating controls are documented.	ENISA [31]
Secure Communication	SECOM-8	Network Segmentation	Separate large networks are to divide them into separate network domains, based on trust levels along organizational units or some combination. The segregation can be done using different logical networks.	ENISA [27,32]
Secure Communication	SECOM-9	Secure Session	Session communication must follow the best practices and standards.	ENISA [29]
Software Security	SOFTWARE-1	Error Messages	Do not reveal sensitive information such as usernames, personal data and others through error messages.	ENISA [29]
Software Security	SOFTWARE-2	Logout	Apps that support user authentication must have a logout function which terminates the authenticated session. Upon logout, session should also be invalidated on the server side.	ENISA [27,29,31]
Software Security	SOFTWARE-3	Session Keys	Th system must use unpredictable session identifiers with high entropy.	ENISA [27,29]
Software Security	SOFTWARE-4	Authentication and Authorisation	Both authentication and authorization controls should be implemented on the server side.	ENISA [29]
Software Security	SOFTWARE-5	Session Sensitive Data	Clear any maintained sensitive data and attempt to also terminate any server-side session after application state change (e.g., termination, backgrounding).	ENISA [29,31]

Co-funded by the European Union

Category	Code	Name	Description	Source
			Consider a user request for application termination as a request to logout. Clear any maintained sensitive data on session termination. Reset the application state and request for user re-authentication.	
Software Security	SOFTWARE-6	Session History Stack	For platforms that support application component history stack (e.g., Android), always clear the stack on session or app termination and user's request to logout.	ENISA [29]
Software Security	SOFTWARE-7	Session management	Ensure that session management is handled securely after the initial authentication, using appropriate security protocols.	ENISA [27,29,31]
Software Security	SOFTWARE-8	Input and Output Handling	The system must have data input validation (ensuring that data is safe prior to use) and output filtering.	ENISA [27]
Software Security	SOFTWARE-9	Update and security patches	The system must have a software update mechanism that enables updating the software for a newer version, and for security patches downloading and installing.	ENISA [27]
Software Security	SOFTWARE-10	Secure communication	Interoperability should be done ensuring information is transmitted in a secure way.	ENISA [67]
Monitoring	MONITOR-1	Traffic Monitoring	Traffic between untrusted and trusted connections of network environments and virtual instances must be monitored.	ENISA [27,29,31, 32]
Monitoring	MONITOR-2	Security Controls monitoring	Security controls behaviour must be logged to support auditing. Based on auditing activities, relevant sequence of actions can be identified and linked back to the relevant users.	ENISA [27,32]
Monitoring	MONITOR-3	Log data security	Log data must be protected.	ENISA [27,31,32]
Monitoring	MONITOR-4	User authentication logging	Logging system for user authentication must be in place.	ENISA [27]
Monitoring	MONITOR-5	Management of accounts and access rights logging	Logging system for account and access rights management must be in place.	ENISA [27,29,31, 32]

Co-funded by the European Union

Category	Code	Name	Description	Source
Monitoring	MONITOR-6	Security Rules Modification logging	Logging system for security rules modification must be in place.	ENISA [27,29,31, 32]
Monitoring	MONITOR-7	System functioning logging	Logging system for system functioning must be in place.	ENISA [27]
Monitoring	MONITOR-8	Audits/assessments	Conduct periodic audits and reviews.	ENISA [27,31]
Monitoring	MONITOR-9	Authentication data protection	Passwords, keys or any other credentials must not be visible in cache or logs.	ENISA [29]
Monitoring	MONITOR-10	Risk Analysis	Define or identify requirements for event logging, including logging requirements for cloud service providers.	ENISA [31]
Monitoring	MONITOR-11	Legal Requirements	Ensure data retention for log data follows legal requirements. Ensure log data is also deleted in the case of termination or change of provider.	ENISA [31]
Monitoring	MONITOR-12	User Activity	A logging system for user activities must be in place.	ENISA [27,31,32]
Monitoring	MONITOR-13	Configuration assessments	Systems configuration must be checked regularly and assessed against defined standards.	ENISA [27]
Integrity	INTEGRITY-1	Boot integrity	There must be a mechanism for boot integrity check to detect manipulation of the host OS and software, rootkits, viruses and worms.	ENISA [27]
Integrity	INTEGRITY-2	Controlled Software Installation	Software installation must be done in a controlled manner. For example, ensure that the system only uses cryptographically signed codes and that the certificates are trusted.	ENISA [27]
Integrity	INTEGRITY-3	Code monitoring and protection	The system must have runtime protection and secure execution monitoring to be sure malicious attacks do not overwrite code after it is loaded.	ENISA [29]
Integrity	INTEGRITY-4	Sandbox for unauthenticated software	In case the use of un-authenticated software being needed, it must be run with limited permissions and/or sandboxed.	ENISA [27,31,32]
Integrity	INTEGRITY-5	Secure State Restoration	The system must be able to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful.	GP-TM-06, OS-09

Category	Code	Name	Description	Source
Integrity	INTEGRITY-6	Application Integrity	Whenever possible, check the application integrity using native platform services ((e.g., Android SafetyNet attestation, iOS App Store receipt).	ENISA [27,29]
Integrity	INTEGRITY-7	Device/Platform integrity	Check the device/platform integrity to ensure that the device is not modified. Prefer using Platform services if available (e.g., Android SafetyNet attestation).	ENISA [29]
Availability	AVAILABILITY-1	Industry Standards	Data, communications, and security protocols must follow industry-standards.	ENISA [31,32]
Availability	AVAILABILITY-2	Interoperability	Service APIs must use open and published API to support interoperability between components and applications.	ENISA [31]
Availability	AVAILABILITY-3	DDoS protection	The system/service must use DDoS-resistant and Load-Balancing infrastructure to protect their services.	ENISA [27]
Availability	AVAILABILITY-4	Communication Redundancy	There must be possible to establish more than one secure communication paths between the same systems.	ENISA [32]
Availability	AVAILABILITY-5	Energy	The system must have adequate energy supply system.	ENISA [27]
Data protection mechanisms	DATA-1	Data Segmentation	The system provides segmentation for data, ensuring the data is only accessible to the right entity (device, user, application, VMs, Containers, etc.)	ENISA [32]
Data protection mechanisms	DATA-2	Data Backup	The system has a backup system that is adequate.	ENISA [27,31,32]
Data protection mechanisms	DATA-3	Data Integrity	Data integrity processes and mechanisms must be implemented.	ENISA [27,29,31, 32]
Privacy	PRIVACY-1	Consent	The system/service must have a consent mechanism that asks for permission to use the user's personal data whenever it is required, indicating exactly what personal data will be used, the purpose of the processing, who will have access to the data, where will the data be stored, how long the data will be stored. Limitations of the system/service should be stated whenever the user does not consent to the use of personal data. The user should be able to withdraw the consent at any given time. Require consent prior to providing user data to third parties. Provide clear notice of data shared cross-application with third parties. Never provide precise location	ENISA [29]

Co-funded by the European Union

Category	Code	Name	Description	Source
			data to third-party applications nor data stored in the secure containers of the application. Consent may be collected in 3 main ways: • At install time; • At run-time when data is sent; • Via "opt-in" mechanisms where a user must explicitly turn on a setting.	
Privacy	PRIVACY-2	Check data	Mechanisms and processes must be in place to check whether data collection is not excessive about the consent that has been granted by the user.	ENISA [29]
Privacy	PRIVACY-3	Sensor Data	Whenever possible and appropriate, the system/service/device should use the built-in features to require access to device sensors and data, providing a clear explanation on why the access is needed.	ENISA [29]
Privacy	PRIVACY-4	Privacy Policy	Create a privacy policy covering the usage of personal data and make it available to the user, prior to making consent choices.	ENISA [29]
Privacy	PRIVACY-5	Privacy Enhancing Technologies	Whenever possible and appropriate, deploy privacy enhancing technologies, that support data minimization, anonymization and security of personal data.	ENISA [29]
Privacy	PRIVACY-6	User Consent Record	The system/service must keep a record of user consent for the processing of different types of personal data, as well as their location.	ENISA [29]
Privacy	PRIVACY-7	Data Anonymization	Devices should reduce data granularity and anonymize data before sending it to another device or server/service (e.g., strip image metadata).	ENISA [29]
Privacy	PRIVACY-8	Retention Period	Reduce retention period on the mobile or remotely to the minimum amount of time needed to provide the service. Delete data immediately after the retention period has expired. Delete data from all locations (especially remote servers) where data might be stored.	ENISA [29,31]
Privacy	PRIVACY-9	Minimal Disclosure	Apply the principle of minimal disclosure - only collect and disclose data which is required for business use of the application. Identify in the design phase what data is needed, its sensitivity and whether it is appropriate to collect, store and use each data type.	ENISA [29,31]

Category	Code	Name	Description	Source
Third parties	TP-01	Providers commitment	Providers should commit contractually their collaboration in incident handling when their products or services are involved.	ENISA [67]
Third parties	TP-02	IT department involvement	IT department should be involved in the procurement phase to provide security requirements.	ENISA [67]

Table 6 Requirements (Legal, Standards and Best Practices)

Co-funded by the European Union

Appendix B. Requirements (CYLCOMED)

This appendix covers the requirements for the connected medical devices solutions organized by the components introduced in the generic scenario for connected medical devices, and the requirements for the toolbox. The requirements for the toolbox that were part of this appendix in deliverable 3.1 have now been separated in Appendix C.

Medical Devices and Interfaces Requirements Table

ID	Requirement
MDI01	Medical devices MUST be certified (MDR 2017/745 or IVDR 2017/746)
MDI02	Medical devices should have mechanisms for security patch updates
MDI03	Connected medical devices SHOULD only boot trusted firmware to prevent malware and other malicious software from compromising the device
MDI04	The functionality and access and permission rights of the medical devices SHOULD be limited to what is necessary for the intended purpose.
MDI05	Medical devices SHOULD have an incident response mode in the event of a security breach to inform the doctor
MDI06	Medical devices SHOULD come with an easy-to-understand cybersecurity manual
MDI07	Medical devices, if connected through ethernet, SHOULD be in a separate VLAN
MDI08	Medical devices vulnerabilities SHOULD be available in public repositories like CVE
MDI09	Medical devices SHOULD have a data backups mechanism if any information is stored only on the device
MDI10	Medical devices SHOULD only boot trusted firmware to prevent malware and other malicious software from compromising the device

Table 7 Medical devices and interfaces requirements table

Communication Device & Network Requirements Table

ID	Requirement
CDN01	The communication device MUST have an adequate authentication mechanism

Co-funded by the European Union

ID	Requirement
CDN02	The communication device software MUST protect data from unauthorised additions, deletions, and modifications
CDN03	The software MUST provide a mechanism to ensure the integrity of the code in production (web app, mobile app, backend)
CDN04	Adequate encryption schemes MUST be used to protect the confidentiality of the subject's health data
CDN05	Subject's health data MUST be protected at any time by using an encryption scheme that allows to ensure their security
CDN06	Data SHOULD be sent to the Hospital infrastructure (On premises or cloud) in order to comply with the hospital security policy
CDN07	The communication device/network MUST have a mechanism for user's credential recovery and change
CDN08	Communication devices SHOULD be properly isolated using network segmentation to prevent unauthorized access and data exfiltration
CDN09	Communication devices MUST put in place protection mechanisms to prevent configuration manipulation from affecting the proper functionality of connected medical devices
CDN10	Privacy-preserving techniques MUST be used when personal and sensitive data are shared
CDN11	Mechanisms for avoiding leaks of sensitive information MUST be provided when storing or exchanging health data between devices and hospital environment
CDN12	Mechanisms for preserving data integrity and confidentiality MUST be provided storing and exchanging health data between devices and hospital environment
CDN13	The enrolment and the access processes to the hospital IT system environment MUST provide a strong authentication mechanism to ensure only those legitimate stakeholders are allowed to perform such processes
CDN14	Communication devices SHOULD only boot trusted firmware to prevent malware and other malicious software from compromising the device
CDN15	Secure communication protocols, such as SSL/TLS, SHOULD be used to prevent eavesdropping and data tampering

ID	Requirement
CDN16	The system SHOULD monitor and log all data exchanges between devices and healthcare providers, ensuring that privacy-preserving techniques are used, and data integrity is maintained

Table 8 : Communication device & Network requirements

Backend & Frontend Requirements Table

ID	Requirement
BF01	The system MUST comply with the GDPR data protection requirements, including those on the protection of special categories of personal data (health-related data).
BF02	The system SHOULD be securely integrated with the tools developed for the secure management of devices and services.
BF03	The system MUST implement an access control mechanism to provide differentiated functionality to differentiated user profiles.
BF04	The system MUST produce audit logs allowing visualisation of access to the data (read, write, modify, delete)
BF05	The system MUST ensure the security of registered users' information
BF06	The system MUST protect data from unauthorised additions, deletions and modifications
BF07	The system MUST ensure that applications in production (web app, mobile app, backend) have not been modified by adding unauthorised code
BF08	The system MUST perform periodic backups, that are stored and protected from unauthorised access
BF09	Changes to data made by the system, including backup operations, MUST either be completely executed, or cancelled if the process fails (transactionality of operations)
BF10	The system MUST ensure the persistence of changes made to the data
BF11	The system MUST maintain data consistency when the current operation (data acquisition from the mobile app, data entry or data modification) fails
BF12	The system SHOULD restore a consistent state in the event of data corruption or application crash

Co-funded by the European Union

BF13	The implemented access control mechanism MUST ensure critical health-related operation (e.g., manual data entry) to be performed by personnel with specific role access
BF14	The system MUST maintain a viewable history of audit logs, which can be consulted at any time
BF15	The system SHOULD send medical conditions notifications on different communication channels (i.e., email, in-app, SMS)
BF16	The system MUST have a mechanism that allows adequate review of manually entered data
BF17	The system MUST be able to collect and send information about improper access attempts, possible attacks, or incorrect parameter manipulation to the CYLCOMED tools within the hospital's intranet
BF18	The administration role SHOULD be able to update user permissions and roles automatically without the intervention of technicians, nurses, or physicians.
BF19	The subject's health data MUST be protected at any time by using adequate encryption schemes that ensures their confidentiality
BF20	The subject's health data MUST be protected at any time by using adequate encryption schemes that ensures their integrity
BF21	Mechanisms for tracking data platform access MUST be provided (e.g., by using blockchain technology, or other efficient technologies)
BF22	Secure communication protocols, such as SSL/TLS, SHOULD be used to prevent eavesdropping and data tampering
BF23	The system SHOULD allow federated authentication mechanisms (e.g., OAuth, SAML) adequate token formats and encryption mechanisms.
BF24	The system SHOULD allow users access via 'two factor authentication'
BF25	The system SHOULD be able to detect anomalies in the behaviour of connected medical devices and services based on log analysis.
BF26	The system SHOULD allow setting users' permissions according to the principle of least privilege
BF27	The system SHOULD follow well-known guidelines regarding the usability of the individual UI components (buttons, text boxes etc.)
BF28	The system MUST provide fast and secure access to authorized users to manipulate its components

BF29	The system MUST be able to lock itself and prevent dangerous parameters from being entered
BF30	The system SHOULD have an external device that allows quick user authentication through biometrics or similar features
BF31	The system MUST respond to user requests under normal operating conditions
BF32	The system MUST have a robust security mechanism to prevent unauthorized access and protect against cyber attacks
BF33	The system's biometric authentication device SHOULD have a high level of accuracy and reliability, with a low false acceptance rate and false rejection rate.
BF34	The system SHOULD be capable of continuously monitoring their security status
BF35	The enrolment and the access processes MUST employ a strong authentication mechanism to ensure only those legitimate stakeholders are allowed to perform specific actions in the hospital
BF36	Container based applications SHOULD have their images scanned (e.g., using Clair, Anchore, Dagda, etc) to check that there are no existing vulnerabilities in the images
BF39	The system SHOULD allow the integration of Single Sign On system deployed at the hospital if available, to avoid a new user id and password for the clinicians
BF41	The system MUST keep track of who entered data when data is entered manually.
BF42	The system SHOULD create activity and events logs for the activity and events performed from external systems
BF43	The logs SHOULD include temporal and source information

Table 9 Backend & Frontend requirements table

Co-funded by
the European Union

Appendix C. Toolbox Requirements

The Category column has been added from D3.1[4] to map the requirements to the categories introduced in Chapter 4

ID	Requirement	Category
TB01	The system MUST comply with the GDPR data protection requirements	Privacy
TB02	The system MUST provide access to users with a proper authentication mechanism (e.g., username and password, biometrics)	Identity and Access Management
TB03	System SHOULD use secure communication protocols, such as SSL/TLS, to prevent eavesdropping and data tampering	Cryptography, Secure Communication
TB04	The system SHOULD contain an AI-based log monitoring solution.	Identity and Access Management
TB05	Log monitoring models SHOULD be trained in an unsupervised or self-supervised fashion besides supervised	Monitoring
TB06	Log monitoring solution SHOULD analyse system/application logs and assign them anomaly scores.	Monitoring
TB07	Log monitoring solution SHOULD be able to send an alert to notify the responsible administrator in case of an incident (e.g., email, Slack, MS Teams).	Monitoring
TB08	The Toolbox SHOULD match the medical devices installed at the hospital against the public known vulnerabilities.	Configuration
TB09	The cybersecurity dashboard SHOULD include advanced filtering and search features to allow users to quickly and effectively navigate the generated logs and alerts	Software Security
TB10	The cybersecurity dashboard SHOULD have an integrated alert management system that allows users to acknowledge, categorize, assign, and track alerts until they're resolved	Monitoring
TB11	The cybersecurity dashboard SHOULD incorporate an automated threat prioritization mechanism that ranks potential threats based on their severity and potential impact	Monitoring
TB12	Adequate authenticity, integrity and access control mechanisms for the training data MUST be protected	Data protection mechanisms

ID	Requirement	Category
TB13	The log monitoring models training environment MUST be properly protected against unauthorized accesses	Software Security
TB14	The system MUST provide fast and secure access to authorized users to manipulate its components	Design
TB15	The Log monitoring models SHOULD be protected with adequate integrity controls and consistency checks.	Integrity
TB16	Decentralized identity verification mechanism SHOULD be provided, to facilitate the user access to the smartphone and hospital IT system environment	Identity and Access Management

Table 10 : ToolBox Requirements

Co-funded by the European Union