Cyber-security toolbox
for connected medical devices

D3.1 Baseline analysis, requirements and specifications

Revision: v.2.1

Work package	WP 3
Task	3.1
Due date	31/05/2023
Submission date	13/06/2023
Deliverable lead	FHUNJ
Version	3.0
Authors	Andrés Castillo PhD (FHUNJ)
Reviewers	Juan Carlos Pérez Baún, Esteban Armas Vega (Atos)

Abstract	This document summarizes the 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. The work carried out in the first six months of the project is summarized in the collection, analysis, and synthesis of the technical, legal, clinical, and ethical requirements. This study is completed in document D2.1, more focused on legal requirements. What is exposed here is the input for the work of WP5 and WP4. The requirements collection will be followed up in Task 3.2 and D3.2.

Keywords	Cybersecurity, Connected Medical Devices, Requirements, Regulations, Standards

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	28/03/23	Initial table of contents	MARTEL
V0.2	09/05/23	Initial Content	Andrés Castillo (FHUNJ)
V0.3	11/05/23	Sections 3.2.1 until 3.2.7, Appendix B,	João Rodrigues (INOV)
V0.3	11/05/23	Section 3.1, Appendix A	Duško Milojević (KUL)
V0.3	11/05/23	Appendix C preliminary version of Requirements list description	Juan Carlos Pérez Baún, Esteban Armas Vega (Atos) Simone Favrin (Mediaclinics) Ricardo Ruiz (RGB) Giacomo Inches (MARTEL) Nejc (XLAB) João Rodrigues (INOV) Duško Milojević (KUL) Alberto Tozzi (OPBG) Andrés Castillo (FHUNJ)
V0.3	11/05/23	Section 4	Juan Carlos Pérez Baún, Esteban Armas Vega (Atos) Simone Favrin (Mediaclinics) Ricardo Ruiz (RGB) Giacomo Inches (MARTEL) Nejc (XLAB) Andrés Castillo, Santiago Bollaín (FHUNJ)
V0.3	11/05/23	Appendix D	Alberto Crespo (Atos)
V0.3	15/05/23	Section 3.1, Introduction, Conclusion	Andrés Castillo (FHUNJ)
V0.4	22/05/23	Content completion	Andrés Castillo (FHUNJ)
V1.0	26/05/23	First review	Juan Carlos Pérez Baún, Esteban Armas Vega (Atos)
V1.5	04/06/23	Corrections and Formatting	Andrés Castillo (FHUNJ)
V2.0	06/06/23	Final Internal review	Juan Carlos Pérez Baún, Esteban Armas Vega (Atos)
V2.1	06/06/23	Quality Review	João Rodrigues (INOV)
V3.0			

Disclaimer

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, e.g., web*	**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

The security of medical devices is a concern for healthcare globally. Cyber-attacks can disrupt business in any sector. However, in the healthcare sector, which already lags behind other sectors when it comes to cyber security, a business disruption can be a matter of life and death. Equipment malfunctions can put patients at risk, and the repercussions of the theft of patient and hospital personal data can last for years. Cyber threats are not going to go away. This means that hospitals need to take appropriate measures to protect their IT systems, their data, their medical devices and, above all, their patients.

Fortunately, there already exist many regulations, standards, and good practices regarding cybersecurity specifically for connected medical devices. Nevertheless, it is a growing domain that need constant vigilance. CYLCOMED project has been designed to identify the existing gaps and propose new guidelines for all the stakeholders. This document gives an account of the first steps in that direction.

CYLCOMED addresses the overall ambitious goal of strengthening the cybersecurity of connected, in vitro diagnostic and software as medical devices, by:

- maintaining their performance and safety for patients and preserving or enhancing the confidentiality, integrity and availability of private data they exchange;
- allowing private data to be remotely and securely accessed;
- Tailoring training and awareness measures to healthcare staff needs, focussed on humans operating the technology, as they are usually considered the weakest link in the chain for security and privacy.

This deliverable is the report of the analysis of different applicable legal instruments (including those specific to domains of novel technologies where medical devices will be used), and their interrelations and intersections. A thorough review of the state of the art regarding the cybersecurity standards and legal regulations is also added. This document provides the conclusions of the study of the state of the art on the cybersecurity baselines, in accordance with the common cybersecurity procedures and approaches, and the current directive and guidance. Appendix C entails a first collection of the technical, legal, clinical and ethical requirements for designing a pathway for a comprehensive guidance document.

All over this document there is a triple perspective: 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 begin to present are the basis for the development of a Toolbox to enhance the cybersecurity of connected medical devices in hospital and closest-to-patients telemedicine settings.

This public deliverable will serve as input primarily for D3.2 as he next iteration. At the same time that this document was drafted a re-evaluation of the state of the art has been carried out in WP5 (for D5.1 “CYLCOMED Toolbox prototype”) as it is reflected in the initial specifications of Toolbox elements found in Appendix C. It is also the first step for WP4 (D4.1 “CMD Risk Management Methodologies”).

The legal framework section in this document is being complemented in the Task T2.1” Identification of Ethical and Legal Frameworks”, which is the first task of Work Package 2 “Legal, Ethical and Regulatory Issues”. Together D3.1 and D2.1 will provide a preliminary ethical and legal analysis and guidance from the onset of the CYLCOMED.

Targeting researchers, clinicians, policymakers, technical people, and the IT departments involved in the integration of CMDs in the hospital environment and medical device manufacturers, this report addresses the crucial issue of medical device security, a global healthcare concern. The security of medical devices is a concern for healthcare globally.

Table of Contents

List of figures

List of tables

Abbreviations

Abbreviation	Definition
ABE	Attribute-Based Encryption
AI	Artificial Intelligence
AIRMF	AI Risk Management Framework
ALTAI	The Assessment List for Trustworthy Artificial Intelligence
API	Application Program Interface

BLE	Bluetooth Low Energy
BSA	Business Software Alliance
CCM	Cloud Controls Matrix
CIS	Clinical Information System
CMD	Connected Medical Device
COPE	Corporate-Owned Personally-Enabled
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CVE	Common Vulnerabilities and Exposures
D	Deliverable
DDoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSPD	Security & Privacy by Design (DSPD)
EC	European Commission
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EHDS	The European Health Data Space
EHR	Electronic Health Record
eIDAS	electronic Identification, Authentication and Trust Services
EMS	Emergency Medical Services
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union

FE4MED	Functional Encryption for Medical Data
GCP	Good Clinical Practice
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HE	Horizon Europe
HE	Hospital Equipment (CYLCOMED Pilot)
HIS	Health Information System
HLEG AI	High-Level Expert Group on Artificial Intelligence
HTA	Health Technology Assessments
HTTPs	Hypertext Transfer Protocol Secure
IaC	Infrastructure As Code
IAM	Identity and Access Management
ICT	Information and Communication Technologies
ICU	Intensive Care Unit
ID	Identification Data
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMDRF	International Medical Device Regulators Forum
IoMT	Internet of Medical Things
IoT	Internet of Things
IPR	Intellectual Property Rights
ISMS	Information Security Management System
ISO	International Organization for Standardization

IT	Information Technology
ITU	International Telecommunication Union
IVD	In Vitro Diagnostic Medical Device
IVDR	In Vitro Diagnostic Medical Devices Regulation (EU) 2017/746 (IVDR)
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LAN	Local Area Network
MDD	Medical Device Directive 93/42/CEE
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation (EU) 2017/745 (MDR)
MHP	MediaClinics Health Platform
MUD	Manufacturer Usage Description
NIS	Network and Information Security Directive
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NMT	Neuromuscular Transmission
OS	Operating System
PACS	Picture Archiving and Communication System
PICU	Paediatric Intensive Care Unit
RED	Radio Equipment Directive
SaMD	Software as Medical Device
SAML	Security Assertion Markup Language
SCA	Secure Code Alliance
SPD	Secure Software Development Practices (SDP)
SSL/TLS	Secure Socket Layer / Transport Layer Security

SW	Software
TFEU	Treaty on the Functioning of the European Union
TMP	Telemedicine Platform
TRL	Technology Readiness Level
UI	User Interface
US	United States (of America)
VC	Verifiable Credentials
VLAN	Virtual Local Area Network
WiFi	Wireless Fidelity: Trademarked Phrase (IEEE 802.11x Standards)
WMA	World Medical Association
WP	Work Package
YAML	Yet Another Markup Language

....

2 Introduction

CYLCOMED aim is to provide a methodological and technical cybersecurity framework designed for healthcare services that use Connected Medical Devices (CMDs). Such a framework must be aligned with the Medical Device Regulation (MDR (EU) 2017/745)[1] and In Vitro Device Regulation (IVDR (EU) 2017/746)[7], but strengthens the adherence to requirements concerning safety, performance and IT security. CYLCOMED strives to:

- identify gaps and introduce new safety and security requirements based on evidence, adapting such requirements to novel technologies (e.g., cloud computing, artificial intelligence);
- identify security-related hazard categories and risk acceptance criteria according to the classification of medical devices;
- promote a risk assessment framework built on risk-benefit analyses that responds to the identified requirements and gaps and considers the impacts of novel scenarios on risks (e.g., safety, performance and environmental differences of in-hospital versus remote monitoring of patients);
- provide tools that help mitigate risks and the increase of safety, security and performance of healthcare services relying on CMD, In Vitro Diagnostic Medical Device (IVD), and Software as Medical Device (SaMD) with consideration to challenges involving legacy devices.;
- demonstrate the performance and applicability of the implemented tools in two dedicated pilots, with a real-world validation performed by relevant stakeholders.

The first objective of CYLCOMED is the Identification of ethical, legal, and regulatory frameworks and challenges and providing recommendations to extend cybersecurity guidelines for CMDs from the legal and ethical perspective.

With the rise of cyber threats addressed at CMD, the need to develop new security solutions is more obvious than ever. However, it is crucial to increase compliance between security solutions and domain-specific requirements in terms of ethics and privacy, in a highly regulated environment. The Medical Device Coordination Group (MDCG 2019-16) Guidance on Cybersecurity for Medical Devices[7] as the utmost importance to increase compliance with 2017 regulations on medical devices (MDR, IVDR). However, with the increasing number of applicable legal instruments, the application of the guidance may not be straightforward in all cases. Thus, CYLCOMED will demonstrate which ethical, legal, and regulatory challenges are faced in the context of cybersecurity of CMD and how these ethical, legal and regulatory landscapes can be advanced, by paying special attention to MDCG 2019-16 Guidance on Cybersecurity for Medical Devices.

In order to achieve that objective, this deliverable reports the analysis of different applicable legal instruments (including those specific to domains of novel technologies where medical devices will be used), and their interrelations and intersections. A thorough review of the state of the art regarding the cybersecurity standards and guidelines is also added.

Purpose and scope of this document

This document is part of the Work Package 3 (WP3). The study of the state of the art regarding the cybersecurity has been carried out in the context of Task 3.1. The requirements regarding cybersecurity have been collected analysed, and synthesized from a technical, legal, clinical, and ethical perspective. A preliminary set of technical, functional and non-functional, requirements have been compiled as a first step contributing to the overall objective of developing the cybersecurity Toolbox (also in connection with legal and ethical requirements traced in WP2), so that it is user-friendly, trustworthy, reliable, and scalable.

.

Deliverable structure

This deliverable contains the following sections. First, section 3 takes an exhaustive look at the regulations and standards, after introducing the broad subject of cybersecurity for connected medical devices. Section 4 presents the first attempt to collect the technical requirements of the assets the partners' organizations are bringing into the project. It takes specifically into consideration the pilot scenarios and the clinical trials to be conducted in the hospitals as part of CYLCOMED project. It is preceded by a general description of the assets brought into the project and the architecture of the security Toolbox to be developed during the life of the project.

The appendixes contain both the complete revision of the requirements derived from regulations and standards relevant to the domain of connected medical devices, and the first collection of technical requirements. A comprehensive Glossary is available as a last Appendix.

3 Baseline Analysis

This section provides an in-depth exploration of the regulatory frameworks and standards pertinent to the cybersecurity of medical devices. It specifically focuses on devices that interact with external systems, not only within hospital networks but also in broader contexts, such as patients' homes, ambulances, and other emergency medical service vehicles. The analysis presented in this section offers a robust understanding of the interconnected and multifaceted aspects of cybersecurity in medical devices, guiding manufacturers, operators, and medical professionals in comprehending and applying the necessary safety and security measures.

Introduction

In general[1], cybersecurity can be defined as a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, insurance, and technologies that can be used to protect the environment, cyber and user organizations and assets. Assets can be understood as all kinds of resources, such as devices, software, staff members, various services, telecommunications systems, infrastructure, and all information transmitted and/or stored.

In summary, cybersecurity is a set of measures, tools and practices that aim to protect technology, data or information and people. Technology in the healthcare sector is used to receive, send, store and process data. The data, or information, is used to treat people, in medical research, to process payments, to order medical supplies, to process personal information, and many more purposes. And healthcare professionals use technology and data to do their jobs in the best way possible.

Cybersecurity is closely related to information security. This focuses on three central aspects of information, the preservation of confidentiality, integrity, and availability. In other words, their goal is to ensure that information is not leaked to unauthorized sources, cannot be compromised in any way, and is not impossible to access when needed.

Cybersecurity issues focus on technologies and how they can be used to breach security or how they could be breached to obtain data. Cybersecurity is also more concerned with the potential harm it can cause to people. Due to this, it can be said that technology, data, and people are three central components of cybersecurity. An incident where these three components come together is very likely to be a cybersecurity incident.

CYLCOMED focuses on developing mechanisms that guarantee the cybersecurity of medical devices that are in contact with patients and therefore more directly affect their security. More and more medical devices are connected to hospital information systems through software and hardware systems that thus become other types of medical devices as reflected in CYLCOMED pilots and real-world clinical trials. All systems qualified as medical devices must be previously certified. The certification process includes demonstrating that the necessary cybersecurity mechanisms have been established, as they are summarized next.

General safety considerations

---

[1] This introductory subsection is inspired in the Cybersecurity in Healthcare MOOC developed as part the SecureHospitals.eu project (Horizon 2020 Coordination Research and Innovation Action under Grant Agreement No. 826497).

It is recognised in Medical Device Regulations[2] that all medical devices carry inherent risks. Striking an appropriate balance between these risks and the highest level of health and safety achievable through correct device use is vital, as with any type of device.

Manufacturers bear the responsibility of defining security best practices to minimize or eradicate potential risks and threats. In doing this, they should contemplate the device type, usage environment, and utilization method to establish pertinent security controls and usage rules.

Medical facilities should tailor their risk management processes to align with these best practices, which include[3]:

- Robust physical security to prevent unauthorized access to medical devices or access points;
- Role-based access control measures to access network elements, stored information and/or services;
- Security patch management;
- Malware protection;
- Security awareness training;
- Methods to verify who has made changes to the system.

In addition to manufacturers and medical facilities, it is necessary to consider the other main actors in medical devices, such as:

- **Integrators**: They ensure the correct installation and configuration of the device, following manufacturers' instructions, and providing support to operators when required.
- **Operators**: They are responsible for ensuring that the devices are used and maintained safely according to the manufacturer's instructions.
- **Medical Professionals**: They are responsible for using the medical device itself to deliver the required monitoring of and treatment to the patient. Therefore, they should be instructed to make proper use of the device from a cybersecurity point of view.
- **Patients**: As the ultimate recipients of treatment via the medical device and, like medical professionals, must be instructed to make proper use of the device from a cybersecurity point of view in case they can consult their medical data or have any kind of interaction with the device.

Insurance design and manufacturing

As with any IT device, security, safety, and efficiency must be considered throughout the entire lifecycle of the medical device, from the design and manufacturing processes to the decommissioning process.

In order to achieve an adequate level of security, it is necessary that security is taken into account from the design stage, otherwise it may be necessary to go back at later stages of the project to redefine manufacturing requirements to meet the necessary security requirements.

---

[2] *https://www.jtsec.es/blog-entry/41/ce-marking-medical-devices-and-cybersecurity*

[3] *https://www.tuvsud.com/en/industries/healthcare-and-medical-devices/medical-devices-and-ivd/medical-device-market-approval-and-certification/medical-device-regulation*

This should be done throughout the product life cycle by carrying out the following list of good practices:

- **Safety management**: This involves planning and documenting safety activities required to meet the safety requirements documents requested by current regulations. After analysing these safety requirements, a security management plan should be established to ensure that the requirements are met throughout the device's lifecycle.
- **Determine the necessary security requirements**: This consists of identifying the necessary security functions to be fulfilled by the device inherent in the requirements mentioned in the previous step to ensure the confidentiality, integrity, and availability of the data for its intended purpose**.**
  These measures could involve physical security implementations or protections for external interfaces. It also involves deciding whether to implement mechanisms such as authentication, authorisation, encryption, or auditing. Commonly used measures which are in certifications such as FIPS 140-2 and Common Criteria.
- **Security verification and validation testing:** This stage involves defining tests needed to verify that the product meets all security requirements during its lifecycle. Commonly used measures which are in certifications such as FIPS 140-2 and Common Criteria.
- **Security incident management**: This process outline how potential security incidents should be handled. One approach could be to follow the ALC_FLR family of Common Criteria certification, which mandates the manufacturer to keep track of the vulnerabilities discovered and how to remediate them during the entire lifecycle of the device. Another example could be to lock down the device requiring technical assistance in case a security issue is detected to prevent patients from being harmed due to improper device behaviour.
- **Security update management**: This process is responsible for determining how security updates will be tested so that the team can verify that it is legitimate by verifying its hash, and for defining the time period and the way in which they will be made available.
- **Security rules**: This process determines the user documentation that describes how to carry out the integration, configuration, and maintenance of the product in order to operate securely. Again, this section is reminiscent of the Common Criteria and FIPS 140-2 installation (AGD_PRE) and usage (AGD_OPE) guides.

The following are the steps necessary to implement the list of best practices detailed above, in order to consider cybersecurity from the outset and avoid having to go backwards at later stages of development:

Security risk management[4]

Security Risk Management is the overall process to guarantee acceptable levels of risk, and to mitigate and/or eliminate the risks, and restore the correct functioning of the systems. This process consists of carrying out a risk analysis and risk control specifying the measures to be taken to mitigate risks should they occur to an acceptable level.

- **Security risk acceptance analysis.** It is based on establishing security risk acceptance criteria based on the purpose of the device and its operating environment.

---

[4] https://www.jtsec.es/blog-entry/41/ce-marking-medical-devices-and-cybersecurity

- **Minimum IT requirements.** The manufacturer must provide documentation on the use, security configuration and security controls related to the operating environment and have it electronically available and up to date for user. This documentation is similar to that required by certifications such as Common Criteria, FIPS 140-2 and LINCE which require specifying the conditions of the environment and how to proceed to perform the secure configuration of the device.
- **Verification/validation.** The main security measure to use is testing, based on performing fuzz testing, vulnerability scanning, penetration testing and code analysis. These validation measures are similar to those required by the PCI-PTS standard, which performs penetration testing on the device itself and requires evidence of having performed fuzz testing and code analysis from the manufacturer.

Lifecycle aspects

Although addressing security risks by design helps to mitigate potential risks and threats, it is necessary to carry out security-related maintenance tasks, because at the time of certification a medical device may be considered secure according to the vulnerabilities known at that time, however, new attack vectors may emerge that make it no longer secure, therefore, it is necessary that throughout the lifecycle, manufacturers keep a record of the information detailed below[5]:

- **Incidents related to the device software**. Security vulnerabilities related to the device hardware and third-party hardware embedded in the device.
- **Existence of new attack vectors**. The manufacturer shall assess the identified risks and carry out the necessary software update or hardware modification at the operator's premises.
- **Documentation and instructions for use.** The documentation to be provided by the manufacturer must contain information demonstrating compliance with the general safety and performance requirements specified in regulations that are listed and described in next subsection. In case of not doing so or not complying with what is required, the manufacturer will not be able to obtain the certificate that enables him to sell his device within the European Union. In addition, this documentation must be kept up to date with information regarding vulnerabilities discovered after the sale of the device and how to remediate them.

Legal Framework

The development and use of CYLCOMED technology fall under the scope of several legal regimes, such as data protection, cybersecurity of connected medical devices and artificial intelligence frameworks. These legal frameworks give rise to numerous legal requirements and obligations which have to be taken into account in the development and design of CYLCOMED technology. However, it is also crucial to increase compliance between security solutions and domain-specific requirements in terms of ethics and privacy. It is noteworthy to mention that task 2.1 (T2.1)," Identification of Ethical and Legal Frameworks", which is the first task of Work Package 2 (WP2) "Legal, Ethical and Regulatory Issues", will provide a preliminary ethical and legal analysis. Therefore, in order to avoid duplication, under this deliverable legal framework

[5] https://www.jtsec.es/blog-entry/41/ce-marking-medical-devices-and-cybersecurity

will be only briefly introduced, while task 2.1 (T2.1)," Identification of Ethical and Legal Frameworks", will further elaborate on relevance of the legal and ethical frameworks.

3.1.1 International Treaties

European Convention on Human Rights

The European Convention on Human Rights (ECHR)[7] is the first Council of Europe's convention and the cornerstone of all its activities. It was adopted in 1950 and entered into force in 1953. The ECHR is an international instrument, ratified by the 47 member states of the Council of Europe, which protects human rights and political freedoms in Europe. The right to personal data protection forms part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect private and family life, home and correspondence. It lays down the conditions under which restrictions of this right are permitted. Taking into account the scope of the project and data processing, CYLCOMED shall fully comply with the ECHR.

Council of Europe Convention 108

The Council of Europe Convention for the protection of individuals concerning the automatic processing of personal data (Convention 108)[7] entered into force in 1985. It was the first and the only legally binding international instrument in the data protection domain. The purpose of the Convention is to secure the rights and fundamental freedoms of individuals, in particular, the right to privacy, with regard to the automatic processing of personal data. Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities. As under this Convention, the Contracting States are required to take the necessary steps in their domestic legislation to apply the principles it lays down. The Convention provides a benchmark for CYLCOMED to understand the fundamental rights that all individuals from the Contracting States enjoy regarding the processing of personal data.

3.1.2 Primary EU Legislation

Charter of Fundamental Rights

The Charter of Fundamental Rights[7] is the European Union's bill of human rights which entered into force with the Treaty of Lisbon on 1 December 2009. These rights enforce important principles like dignity, fairness, respect, and equality. The charter applies to EU institutions, bodies, offices, and agencies in all their actions, and Member States have a duty to respect the rights guaranteed by the Charter when they are implementing EU law. Taking into account the fact that the Charter explicitly raises the level of personal data protection to that of a fundamental right in EU law, the design and deployment of the CYLCOMED project shall take into consideration the rights and freedoms guaranteed by the Charter, specifically the protection of personal data.

The Treaty on the European Union and the Treaty on the Functioning of the European Union

The two Treaties[7] lay the foundation of EU primary law together with the Charter. In their consolidated version of 2009, they are also known as Lisbon Treaties. They establish the governance structure of the EU, its agencies, fundamental principles, the legal basis for all EU legislation and underlying policy objectives. In the context of CYLCOMED several provisions

are relevant. Starting from the Treaty on the Functioning of the European Union (TFEU), Article 16 restates data protection as a fundamental right of the EU and lays the legal basis for legislation in the sphere of data protection.

3.1.3 Secondary EU Legislation

General Data Protection Regulation (GDPR)

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. The General Data Protection Regulation (GDPR)[8] is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR is a vital component of EU privacy law and human rights law, particularly Article 8 (1) of the Charter of Fundamental Rights of the European Union. It imposes obligations onto organisations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.

The most relevant GDPR obligations that are imposed on controllers and processors are summarised in the Appendix A.

Directive on Privacy and Electronic Communications (E-Privacy Directive)

The Directive on Privacy and Electronic Communications concerning the processing of personal data and the protection of privacy in the electronic communications sector[9], or better known as the e-Privacy Directive, is an EU directive that deals with the regulation of several important aspects of privacy in the digital age, such as confidentiality of information, treatment of internet traffic data, use of cookies, spam etc. The e-Privacy Directive was adopted to supplement the then Data Protection Directive (later replaced by the GDPR) addressing in detail the confidentiality of electronic communications, and the tracking of internet users more broadly. The broad subject matter of the e-Privacy Directive is the right to privacy in the electronic communication sector and free movement of data, communication equipment and services. The Directive harmonises the rules of the EU Member States required to ensure equivalent protection of the right to privacy within the European Union.

Medical Device Regulation (MDR)

The Medical device regulation (MDR) aims to ensure the smooth functioning of the internal market as regards to medical devices, taking as a base a high level of protection of health for patients and users, and considering the small- and medium-sized enterprises that are active in this sector. At the same time, this Regulation sets high standards of quality and safety for medical devices to meet common safety concerns as regards to such products. Both objectives are being pursued simultaneously and are inseparably linked whilst one not being secondary to the other. The MDR scope is briefly explained in previous section, whereas it will be subject of the legal analysis under the WP2.

In vitro diagnostic medical devices (IVDR)

Regulation (EU) 2017/746 on in vitro diagnostic medical devices (IVDR) aims to ensure the smooth functioning of the internal market with regards to in vitro diagnostic medical devices, taking as a base a high level of protection of health for patients and users, and taking into account the small and medium-sized enterprises that are active in this sector. At the same time, this Regulation sets high standards of quality and safety for in vitro diagnostic medical

devices in order to meet common safety concerns regarding such products. Broadly speaking, IVDR follows the same logic as the MDR. For instance, manufacturers that are seeking market access throughout the EU must comply with Annex I - General Safety and Performance Requirements in terms of meeting these requirements. IVDR Annex I follows the same structure as the MDR.

Guidance on Cybersecurity for medical devices - MDCG 2019-16

This document's main purpose is to give manufacturers guidance on how to fulfil all the relevant essential requirements of Annex I to the MDR and IVDR regarding cybersecurity. The Guidance lays down certain new essential safety requirements for all medical devices that incorporate electronic programmable systems and software that are medical devices in themselves. They require manufacturers to develop and manufacture their products in accordance with the state of the art taking into account the principles of risk management, including information security, as well as to set out minimum requirements concerning IT security measures, including protection against unauthorised access. However, in light of the complexity of medical device supply chains and the role played by different operators in ensuring that devices are protected against unauthorised access and possible cyber threats, additional considerations concerning expectations from actors other than manufacturers are provided.

Cybersecurity Act

Cybersecurity Act[10] lays down objectives, tasks and organisational matters relating to the European Union Agency for Cybersecurity (ENISA) and a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union. In other words, the Cybersecurity Act strengthens the ENISA and establishes a cybersecurity certification framework for products and services.

NIS 2 Directive

The Directive (EU) 2022/2555 on measures for a high common level of network and information security across the Union (NIS 2 Directive)[11] sets out the baseline for cybersecurity risk-management measures and reporting obligations across the sectors that fall within its scope. The Directive sets common security requirements to ensure network and information security across the EU. The Directive is relevant to the healthcare sector. The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

The actors identified as essential and important entities are subject to obligations regarding cybersecurity risk-management measures. In particular, Member States have to ensure that such entities take appropriate and proportionate technical, operational, and organisational measures in order to manage the risks for network and information systems used in their operations and provision of their services. Furthermore, the impact of incidents should be prevented or minimised. The measures should be based on an all-hazards approach.

The Critical Entities Resilience Directive

The Directive on the resilience of critical entities[12] aims to reduce vulnerabilities and strengthen the physical resilience of critical entities in the European Union (EU) in order to ensure the uninterrupted provision of services that are essential for the economy and society as a whole, increasing the resilience of the critical entities that provide these services. Critical entities are entities providing essential services that are crucial for the maintenance of vital societal functions, economic activities, public health and safety, and the environment. They need to be able to prevent, protect against, respond to, cope with and recover from hybrid attacks, natural disasters, terrorist threats and public health emergencies. This directive is part of a package of legislative measures to improve the resilience and incident-response capacities of public and private entities in the EU in the field of cybersecurity and critical infrastructure protection.

Radio Equipment Directive (RED)

The Radio Equipment Directive (RED)[13] establishes a regulatory framework for making available on the market and putting into service in the Union of radio equipment. ”Radio equipment” means an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as an antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination. Hence, all internet-connected radio equipment, including Internet of Things (IoT) with a radio (wireless) function and wearables (i.e., smart watches) fall under the Directive’s scope. A wide range of electronic products that are Wi-Fi, Bluetooth, LTE, 5G, or GPS enabled are under the RED scope. Additionally, medical devices such as pacemakers or implantable cardioverter defibrillators are likely to fall under the scope of the Directive and thus be subject to its security requirements.

Directive on the application of patients’ rights in cross-border healthcare

The general objective of the Directive on patients' rights in cross-border healthcare[14] is to facilitate access to safe and high-quality healthcare in another Member State. To this end, patients are reimbursed for healthcare in accordance with the principles established by the European Court of Justice of the European Union and codified by the Directive. At the same time, Member States remain responsible for providing adequate healthcare in their territory. Moreover, the Directive promotes cross-border cooperation in healthcare between Member States for the benefit of EU citizens, regarding prescriptions, digital health (eHealth), rare diseases and health technology assessments (HTAs). It sets out the conditions under which a patient may travel to another EU country to receive safe and high-quality medical care and have the cost reimbursed by their own health insurance scheme.

3.1.4 Clinical Trials and Ethics

The advancement of medical science largely depends on investigations in humans intended to discover or verify the effects of one or more investigational medicinal products. Clinical trials aim to attain generalised knowledge that can be used to advance healthcare. However, involving human subjects in clinical research, although critical for the welfare of future patients, may not directly benefit the patient involved. In situations where patients may not directly benefit from the research, they are faced with the risk of being exploited or harmed. Therefore, every clinical study must be conducted with the utmost respect for ethical standards.

The Clinical Trials Directive

The Clinical Trials Directive[15] aims to standardise the conduction of interventional clinical trials in the EU and ensure equality in safeguarding public health. Additionally, it defines the overall responsibility of the sponsor for the clinical trial, the requirement of clinical trial authorisation within given time frames by all involved national competent authorities and of one favourable opinion from a responsible ethics committee per Member State as a pre-condition for allowing the sponsor to start the trial in this country. It applies to all academic and commercial interventional clinical trials with an investigational medicinal product in the European Union.

Clinical Trials Regulation

Clinical Trails Regulation[16] aims at achieving an internal market as regards clinical trials and medicinal products for human use, taking as a base a high level of protection of health. At the same time, this Regulation sets high standards of quality and safety for medicinal products in order to meet common safety concerns as regards these products.

Declaration of Helsinki

The World Medical Association (WMA) has developed the Declaration of Helsinki[17] as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data. The World Medical Association's (WMA) Declaration of Helsinki provides guidelines for medical research on human beings. It aims to promote the ethical conduct of research and to protect human subjects from associated risks. The Declaration of Helsinki was the first set of international research guidelines that required research participants to provide informed consent.

Declaration of Taipei

Declaration of Taipei[18] provides guidance for the protection of research subjects who allow their health data and/or body tissues to be used for future research or other uses. This policy aims to address any use of health databases and biobanks excluding individual treatment and is not restricted to research.

Council of Europe Recommendation on the protection of health-related data

This Recommendation[19] provides a set of principles applicable to the processing of personal data relating to health in the public and private sectors. It therefore also applies to the exchange and sharing of health-related data through digital tools.

Ethics guidelines for trustworthy AI

The High-Level Expert Group on Artificial Intelligence (HLEG AI) presented the "Ethics Guidelines for Trustworthy AI" in April 2019, as practical guidance on how developers, deployers and end-users of AI systems can comply with ethical principles.The aim of the Guidelines[20] is to promote Trustworthy AI. Trustworthy AI has three components, which should be met throughout the system's entire life cycle: (1) it should be lawful, complying with all applicable laws and regulations (2) it should be ethical, ensuring adherence to ethical principles and values and (3) it should be robust, both from a technical and social perspective since, even with good intentions, AI systems can cause unintentional harm. These Guidelines seek to go beyond a list of ethical principles, by providing guidance on how such principles can be operationalised in socio-technical systems. Moreover, it sets out a concrete and non-exhaustive Trustworthy AI assessment list.

Taking into account the scope of the CYLCOMED project, the proposals of the following legislative acts will be closely followed due to their possible influence and interplay with CYLCOMED solutions.

Proposal for an Artificial Intelligence Act (AI Act)

The AI Act Proposal[21] is the first-ever attempt to enact a horizontal regulation of AI. The proposed legal framework focuses on the specific utilisation of AI systems and associated risks. More specifically, Artificial Intelligence Act proposal aims to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values and ensure legal certainty to facilitate investment and innovation in AI. Additionally, one of the goals of the AI Act is to enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems and to facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation. The proposal sets harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach.

Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements

The objective of the Proposal[22] is to improve the functioning of the internal market by laying down a uniform legal framework for essential cybersecurity requirements for placing products with digital elements on the Union market. In particular, the Proposal aims to set the boundary conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout a product's life cycle. The Proposal mandates that products with digital elements will only be made available on the market if they meet specific essential cybersecurity requirements for the design, development and production of these products. Besides, Proposal aims to improve the internal market's functioning.

Proposal for a Regulation for the European Health Data Space

The European Health Data Space (EHDS)[23] is the first proposal of such domain-specific common European data spaces. It will address health-specific challenges to electronic health data access and sharing, is one of the priorities of the European Commission in the area of health and will be an integral part of building a European Health Union. EHDS will, inter alia, create a common space where natural persons can easily control their electronic health data. It will also make it possible for researchers, innovators and policymakers to use this electronic health data in a trusted and secure way that preserves privacy and clarify the safety and liability of artificial intelligence in health.

Proposal for Regulation on Privacy and Electronic Communications (E-privacy regulation)

The draft ePrivacy Regulation[24] , if adopted, will repeal the existing ePrivacy directive. As lex specialist to the general data protection regulation (GDPR), it will particularise and complement the GDPR. This Regulation will lay down rules regarding the protection of fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services, and in particular, the rights to respect for private life and communications and the protection of natural persons with regard to the processing of personal data. The proposal also includes rules on Internet of Things to cover machine-to-machine data transmitted via a public network. The Regulation also contains rules on cookies. The text also includes rules online identification, public directories, and unsolicited and direct marketing.

Standards

3.2.1 Cybersecurity Risk Management Framework

The field of cybersecurity includes not only technical tools to protect the digital assets, but also includes processes, procedures, and also managerial and governance aspects in order to manage the cybersecurity risks. Many cybersecurity risk management frameworks and standards exist nowadays. To illustrate a cybersecurity framework, we will analyse the NIST Framework for Improving Critical Infrastructure Cybersecurity[25], an example that organises activities for ongoing cyber risk management. They are organized in 5 categories: Identify; Protect; Detect; Respond and Recover.

The Identify category encompasses activities for understanding the organizational context; for inventorying the assets supporting the organizations' business activities; activities for planning the cybersecurity protection; activities for identifying roles and responsibilities; activities for understanding and documenting the interdependencies with other organizations (e.g., analysing the supply chain); activities for identifying cybersecurity risk levels and risk management strategies.

The Protect category comprises technical and non-technical security controls to guarantee a minimum level of protection required for guaranteeing the risk management strategies.

Technical security controls include:

- Audit log systems;
- Protection against media removal;
- Security controls for networks and all type of communications
- Resilience mechanisms (load balancing mechanisms, failsafe mechanisms, redundant energy supply);
- Data protection mechanisms (encryption, data leak protections, data integrity controls);
- Identity and access management controls;
- Systems supporting backup;
- Systems supporting baseline configurations (that incorporating security principles).

Non-technical activities include:

- Definition and enforcement of the security policies (detailing the purposes, scope, roles, responsibilities, management commitment, and coordination among organizational entities);
- Backup processes;
- Baseline configuration procedure and processes;
- Data elimination processes, including safe disposal of both paper-based and digital information;
- Awareness and training activities, which can include training classes, e-learning and certifications according to roles and responsibilities, phishing campaigns, awareness posters and screensavers;
- Maintenance procedures and processes for the industrial controls and information system components.

Other activities include:

- Vulnerability management;
- Incident response;
- Disaster recovery;
- Business continuity planning;

- Testing activities for the above-mentioned plans.

Even with the protective controls, cybersecurity incidents can occur. For that reason, the **Detect category** includes monitoring activities, such as periodic audit log analysis, internal and external auditing, or any technology, process or procedure that enables the detection of any event that can potentially lead to a cybersecurity incident.

The Respond category encompasses activities related to all the activities for responding to an incident, when it is detected. It includes activities such as incident data analysis, coordination and relevant data sharing among the appropriate personnel within the organization, and with external stakeholders (including law enforcement agencies, technology suppliers) take place to synchronize an appropriate and timely response to the incident. Once the incident is contained, and its effects mitigated, the incident must be documented.

After a cybersecurity event is contained and its effects mitigated/eliminated, activities for restoring the normal functioning of systems and processes takes place. Activities related to recovery are captured in the **Recover category**. It includes the execution of the recovery plan, continuous improvements activities of the organization's cybersecurity risk management like incorporating lessons learned from incidents into the recovery planning and training updates.

Like the NIST Framework briefly described here, other standards and frameworks covers, in different ways, the various aspects for managing cyber risks.

Cybersecurity risk management frameworks must be carefully adopted into the context the organization is in, for better use the resources to control the risks they face, and for better plan the activities for guaranteeing cybersecurity.

3.2.2 Requirements categorisation methodology

Best practices and standards analysis, with respect to cybersecurity, was carried out considering:

- Renowned cybersecurity entities (e.g., ENISA, ENISA, ISO) that develop tools, standards and recommendations for cybersecurity in various settings.
- The description of the tools that are going to be used within this project.

Based on the aforementioned tools, an extensive search through the specific cybersecurity standards and best practices documents were made. More specifically, cybersecurity documents published by internationally recognized organizations were collected. Preference was given to documents detailing cybersecurity best practices on healthcare and inventoried assets (e.g., IoT devices, cloud services, Virtual Machines/Containers, Artificial Intelligence).

Then, a first set of controls were defined. We performed an analysis of the ENISA documents, as they contain the best practices and experts' opinions on to the most relevant problems facing the components/systems. An initial analysis and classification of security controls was made taking into account the following guidelines:

- The controls must be easy understanding of the cybersecurity control domains and description.
- The controls most reflect the most pressing technical requirements for the development of the technical components.
- These controls should be used as guidelines for the development, deployment and usage of the component/set of components, and not be technology specific.

The analysis of the best practices, standards and the definition of requirements is an on-going work, and this deliverable is a snapshot onto the state the analysis in month 6 of the project.

Due to the large number of documents that could potentially contain useful information, we started to analyse first the best practices studies from the European Union Agency for Cybersecurity, which contains recommendations for specific technologies and settings that are aligned with our settings. Most of these analysed documents contain mapping between the controls/best practices and other standards and cybersecurity guides from other entities, like NIST Cybersecurity Framework[1] and ISO27001 cybersecurity controls, which are general in nature and tries to cover all the cybersecurity domains that must be taken into account in order to make an organization cyber secure.

The result of the performed analysis can be found on 0

For the next phases of the project, we will move on to the analysis of the National Institute of Standards and Technology documents, moving from the ones focused on specific technologies in the context of this project to the more general Cybersecurity Framework. Also, documents from the ISO organization (e.g., ISO 27001, ISO 27002), the Cloud Security Alliance Organization, and the BSA Software Alliance.

More entities and documents were and will be compiled during the activities of Work Package 3, as we progress with the refinement of the cybersecurity requirements of CYLCOMED project.

3.2.3 European Union Agency for Cybersecurity

The European Union Agency for Cybersecurity[6] (ENISA) was established in 2004 to support the European Union Member states in achieving a high and common level of cybersecurity within the European Union.[26] The agency plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It works with groups of EU experts, the private sector, and European citizens to develop advice and recommendations on good practices in information security.

Some of the analysed documents from ENISA are the following:

- The ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures[27];
- Guidelines for securing the Internet of Things – Secure Supply Chain for IoT[28];
- Smartphone Secure Development Guidelines Tool[29][30];
- Cloud Security for Healthcare Services[31];
- ENISA's Security aspects of virtualization report[32].

The ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, published in November 2017. In this document, ENISA reported security requirements for the use of IoT technologies, the assets and their relevant threats, and also good practices for guaranteeing cybersecurity [27].

With the input of IoT experts, ENISA has produced the Guidelines for securing the Internet of Things – Secure Supply Chain for IoT, where security guidelines for the entire supply chain was reported, from the requirements and design to the final phases of the IoT lifespan. It covers aspects of security about the end product and the processes to develop the product[28].

ENISA has released SMAShiNG (Smartphone Secure Development Guidelines Tool), an online tool with security guidelines for the smartphone. It supports developers on building secure mobile applications [29],[30].

---

[6] *https://www.enisa.europa.eu/*

The ENISA's Cloud Security for Healthcare Services delivers a set of general practices for delivering a secure cloud service for the healthcare sector. The document is structured around three use cases: Electronic Health Record, Remote Care and Medical devices. 17 security and data protection measures were documented as relevant for ensuring cloud security [31].

The ENISA's Security aspects of virtualization report, published in 2017, provides an overview of the status of security of virtualized environments. It gives the basis to understand issues and challenges related to virtualization security, as well as a discussion on common best practices for security protection in virtualized environments and gaps that need to be filled in to implement secure virtualized and containerized environments. A set of recommendations for next-generation countermeasures is also present in the report [32].

3.2.4 National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is part of the United States Department of Commerce. Its mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology" [33].

In the context of cybersecurity, NIST develops cybersecurity standards, best practices, and other resources, driven by the needs of the U.S. industry. They engage with stakeholders to prioritize their activities towards addressing the U.S. industry needs and issues. [34]

Some of the compiled documents from NIST are the following:

- Framework for Improving Critical Infrastructure Cybersecurity;
- Mitigating Cybersecurity Risk in Tele-Heath Smart Home Integration;
- Securing Electronic Health Records on Mobile Devices;
- Data Integrity – Recovering from Ransomware and Other Destructive Events;
- Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD);
- Mobile Device Security: Corporate-Owned Personally-Enabled (COPE);
- Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector;
- Securing Tele-Health Remote Patient Monitoring Ecosystem;
- Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management – Enhancing Internet Protocol-Based IoT Device and Network Security;
- Artificial Intelligence Risk Management Framework (AI RMF 1.0);
- Application Container Security Guide.

The NIST Framework for Improving Critical Infrastructure Cybersecurity is a framework designed for guiding cybersecurity activities and to function as part of an organization's risk management processes. It organized cybersecurity activities into the Identify, Protect, Detect, Respond and recover functions. Within these functions, there are categories and subcategories of activities that are mapped to cybersecurity controls contained in other standards, like the ones in ISO 27001.

The document entitled as "Mitigating Cybersecurity Risk in Tele-Health Smart Home Integration" describes how domestic IoT users can use these devices as part of a remote healthcare solution. The document details the challenges and approaches to limit the cybersecurity risks of tele-health following the NIST Cybersecurity Framework.

The document "Securing Electronic Health Records on Mobile Devices" is a guideline to implement an example solution, using commercially available products, to protect electronic health records [35].

“Data Integrity – Recovering from Ransomware and Other Destructive Events” details how an organization, using commercially available products, can respond to a detected cybersecurity event pertaining to compromise integrity [36].

“Securing Small-Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)”, details how MUD can be deployed to protect IoT devices from being compromised and from participate in a large scale network-based attacks, such as DDoS[37].

“Securing Tele-Health Remote Patient Monitoring Ecosystem” is a guide for Healthcare Delivery Organizations to implement cybersecurity and privacy controls to increase the resilience of telehealth remote patient monitoring [38] .

The Artificial Intelligence Risk Management Framework presents a framework that helps organizations to increase the trustworthiness of AI systems, fostering a responsible design, development, deployment and use of AI systems [39].

This document describes the security concerns and requirements that should be kept in mind when using container technologies. It analyses all the components of the container, describing the risk they face, and presenting the countermeasures [40].

3.2.5 International Organization for Standardization

ISO (International Organization for Standardization) is an independent, non-governmental international organization with a membership of 168 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges[41].

IT security, cybersecurity and privacy protection are vital for companies and organizations today. The ISO/IEC 27000 family of standards keeps them safe. ISO/IEC 27001 is the world’s best-known standard for information security management systems (ISMS) and their requirements. Additional best practice in data protection and cyber resilience are covered by more than a dozen standards in the ISO/IEC 27000 family. Together, they enable organizations of all sectors and sizes to manage the security of assets such as financial information, intellectual property, employee data and information entrusted by third parties. ISO/IEC 27000 and the other standards in the family have been developed by the ISO/IEC joint technical committee JTC 1, or more precisely its subcommittee 27 on Information security, cybersecurity and privacy protection [42].

ISO 13485 Medical Devices – regulatory requirements are increasingly stringent throughout every step of a product’s life cycle, including service and delivery. Increasingly, organizations in the industry are expected to demonstrate their quality management processes and ensure best practice in everything they do. This internationally agreed standard sets out the requirements for a quality management system specific to the medical devices industry [44].

3.2.6 Cloud Security Alliance organization

The Cloud Security Alliance (CSA) is the world’s leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment [45].

In 2017, the Alliance published the Security Guidance for Critical Areas of Focus in Cloud Computing 4.0, which incorporates advances in cloud, security, and supporting technologies.

It reflects on real-world cloud security practices; In integrates the latest Cloud Security Alliance research projects; an offers guidance for related technologies [46].

The Cloud Controls Matrix (CCM), the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices, and regulations. CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing. CCM is currently considered a de-facto standard for cloud security assurance and compliance[47].

The “CSA IoT Security Controls Framework” provides security controls for organizations to incorporate multiple types of connected devices, cloud services, and networking technologies. It covers many IoT domains from systems processing only “low-value” data with limited impact potential, to highly sensitive systems that support critical services [48].

3.2.7 BSA – The Software Alliance

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy [49][49].

The document "The BSA Framework for Secure Software - a new approach to securing the software lifecycle" is intended to establish an approach to software security that is flexible, adaptable, outcome-focused, risk-based, cost-effective, and repeatable. It considers the different ways software is used in several emerging technologies: Internet of Things Software-as-a-Service, and Artificial Intelligence. The framework is structured to be applicable to the entire spectrum of (1) software development organizations and vendors, (2) software development methods and (3) software products, from simple IoT sensors to complex AI algorithms. Software security encompasses what a software development organization does to protect a software product and the associated critical data from vulnerabilities, internal and external threats, critical errors, or misconfigurations that can affect performance or expose data[50].

The Secure Code Alliance (SCA) is focused on technical competence. The Developing Security & Privacy by Design (DSPD) initiative is a conformity assessment methodology designed to issue individual-level certifications, specific to Secure Software Development Practices (SDP). Application developers are vital to the success of any organization, regardless of the industry. Developers create the tools that we all use, from operating systems (OS) to mobile apps, backend programming, firmware, front-end interface design and other forms of applications. Based on the new realities of an interconnected world that we live in, developers need to implement SSDP in order to protect their code from malicious attacks. By following SSDP, developers serve a crucial role in helping ensure security and safety, not just within an organization, but across the supply chain and society, as a whole [51].

3.2.8 Procedural (Training, Guidelines, Best Practices, Management)

Guide to the Radio Equipment Directive

The Guide to the Radio Equipment Directive[52] is intended to serve as a manual for all parties directly or indirectly affected by the Radio Equipment Directive (RED). It should assist in the interpretation of the RED but cannot take its place; it explains and clarifies some of the most important issues related to the Directive’s application. The Guide also aims to

disseminate widely the explanations and clarifications reached by consensus among Member States and other stakeholders.

Principles and Practices for Medical Device Cybersecurity **IMDRF/CYBER WG/N60**

The purpose of this International Medical Device Regulators Forum (IMDRF) guidance document[53] is to provide general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity. This document is designed to provide concrete recommendations to all responsible stakeholders on the general principles and best practices for medical device cybersecurity (including in vitro diagnostic (IVD) medical devices). This is the first IMDRF guidance document to focus exclusively on medical device cybersecurity. It outlines recommendations for medical device manufacturers, healthcare providers, regulators, and users to: minimise cybersecurity risks that could arise from the use of the device for its intended purposes; and to ensure maintenance and continuity of device safety and performance.

Principles and Practices for the Cybersecurity of Legacy Medical Devices **IMDRF/CYBER WG/N70**

This International Medical Device Regulators Forum (IMDRF) guidance document[54] is intended to provide stakeholders with clear ways of identifying potential legacy devices and practical, feasible approaches to maintain the cybersecurity of legacy medical devices. It considers cybersecurity in the context of legacy medical devices that either contain software, including firmware and programmable logic controllers (e.g., pacemakers, infusion pumps) or exist as software only (e.g., SaMD).

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

The GDPR specifically addresses profiling and automated individual decision-making, including profiling. Guidelines on Automated individual decision-making and Profiling[55] provide further explanation regarding this matter as well as best practice recommendations, building on the experience gained in EU Member States.

Guidelines on the Right to data portability

Guidelines on the Right to data portability[56] provide guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing (either the data subject's consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject.

Guidelines on transparency under Regulation 2016/679

Transparency is an overarching obligation under the GDPR applying to three central areas, namely: the provision of information to data subjects related to fair processing, how data controllers communicate with data subjects in relation to their rights under the GDPR, and how data controllers facilitate the exercise by data subjects of their rights. These guidelines[57] provide practical guidance and interpretative assistance on the obligation of transparency concerning the processing of personal data under the GDPR.

Guidelines on Data Protection Officer under Regulation 2016/679

Data Protection Officer (DPO) is at the heart of the GDPR. Under the GDPR, it is mandatory for certain controllers and processors to designate a DPO. The GDPR recognizes the DPO as a key player in the new data governance system and lays down conditions for his or her appointment, position and tasks. The aim of Guidelines on Data Protection Officer[58] is to clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law, but also to assist DPOs in their role. The guidelines also provide best practice recommendations, building on the experience gained in some EU Member States.

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data4 by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help controllers not only to comply with the requirements of the GDPR but also to demonstrate that appropriate measures have been taken to ensure compliance with GDPR. In other words, a DPIA is a process for building and demonstrating compliance. Hence, the Guidelines on Data Protection Impact Assessment[59] clarify the relevant provisions in the GDPR in order to help controllers and processors to comply with the law.

Guidelines 9/2022 on personal data breach notification under GDPR

The GDPR introduced the requirement for a personal data breach to be notified to the competent national supervisory authority (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach. Guidelines on personal data breach notification[60] explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these obligations. Additionally, also give examples of various types of breaches and who would need to be notified in different scenarios.

EDPB Guidelines 05/2020 on consent under Regulation 2016/679

The Guidelines on consent[61] provide a thorough analysis of the notion of consent in GDPR. The concept of consent as used in the Data Protection Directive and in the e-Privacy Directive to date, has evolved. The GDPR provides further clarification and specification of the requirements for obtaining and demonstrating valid consent. These Guidelines focus on these changes, providing practical guidance to ensure compliance with the GDPR and building upon Article 29 Working Party Opinion on consent.

EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Adherence to Data Protection by Design and by Default requirements plays a crucial part in promoting privacy and data protection in society. It is therefore essential that controllers take this responsibility seriously and implement the GDPR obligations when designing processing operations. Data Protection by Design and by Default Guidelines[62] give general guidance on the obligation of Data Protection by Design and by Default stipulated by GDPR Article 25. Data Protection by Design and by Default is an obligation for all controllers, irrespective of size and varying complexity of processing.

EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR

The concepts of controller, joint controller and processor play a crucial role in the application of the GDPR since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. Guidelines on the concepts of controller and processor[63] seek to provide guidance on the concepts of controller and processor based on the GDPR's rules on definitions in Article 4 and the provisions on imposed obligations. The main aim is to clarify the meaning of the concepts and to clarify the different roles and the distribution of responsibilities between these actors.

Guidelines 01/2022 on data subject rights - Right of access

The overall aim of the right of access is to provide individuals with sufficient, transparent and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. The right of access of data subjects is enshrined in Arti. 8 of the EU Charter of Fundamental Rights. It has been a part of the European data protection legal framework since its beginning and is now further developed by more specified and precise rules in Art. 15 GDPR. Guidelines on data subject rights – the right of access[64] aim at analysing the various aspects of the right of access. More particularly, the section hereafter is meant to give a general overview and explanation of the content of the Art. itself whereas the subsequent sections provide a deeper analysis of the most frequent practical questions and issues concerning the implementation of the right of access.

Assessment List for Trustworthy Artificial Intelligence (ALTAI)

The Assessment List for Trustworthy Artificial Intelligence (ALTAI)[65], is a practical tool that helps business and organisations to self-assess the trustworthiness of their AI systems under development. ALTAI is intended for self-evaluation purposes and it provides an initial approach for the evaluation of Trustworthy AI. It builds on the outlined in the Ethics Guidelines for Trustworthy AI. Besides, ALTAI is firmly grounded in the protection of people's fundamental rights, which is the term used in the European Union to refer to human rights enshrined in the EU Treaties, the Charter of Fundamental Rights, and international human rights Law.

Guidance note on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence

Guidance note on Ethics By Design and Ethics of Use Approaches for Artificial Intelligence[66] concerns all research activities involving the development or/and use of artificial intelligence (AI)-based systems or techniques, including robotics. This document offers guidance for adopting an ethically-focused approach while designing, developing, and deploying and/or using AI based solutions. It explains the ethical principles which AI systems must support and discusses the key characteristics that an AI-based system/ applications must have.

4 CYLCOMED Requirements and Specifications

This section describes briefly the tools to be developed together with the design of the CYLCOMED Toolbox, with the aim to understand the requirements that are being collected and listed thoroughly the Appendix C. On top of that, a high-level view of the technical architecture that will be implemented in the pilots is also considered, because some requirements are deeply related to them.

Assets from Toolbox

This section provides a description of the current status of the technologies and scenarios to be developed during the CYLCOMED project. Also, a description of the assets building the CYLCOMED Toolbox (Figure 1) including a high-level architecture and the interactions with the rest of the elements of CYLCOMED. This information will contribute to derive some functional requirements listed in the Requirements (CYLCOMED)Appendix C.

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

1. AI-based CMD behavioural Analysis;
2. AI-powered log monitoring;
3. Multi-tenancy cloud-native device and platform management;
4. Decentralised Identity Management & Data Protection;
5. Device integrity check tools;
6. Security Dashboard.

Figure 1 : CYLCOMED Cybersecurity Toolbox set

4.1.1 AI-based CMD Behavioural Analysis

During the development of the CYLCOMED project, new AI models will be trained and tunned taking into account the specificities of CMD.

The AI Behavioural Analysis component of CYLCOMED is an integral part of the project's cybersecurity measures, aimed at identifying potential security threats in the use of CMDs. This component (provided by Atos) utilizes machine learning algorithms to analyse patterns in data transmissions from the devices, including the frequency and types of data, to detect any abnormal behaviour that may indicate a security breach.

The main objectives of this component are to improve the security of CMDs and ensure their safe use in personalized healthcare services. To achieve these objectives, the AI Behavioural Analysis component is designed to:

- Identify potential security threats early;
- Alert healthcare providers and device manufacturers;
- Continuously learn and adapt.

To this end, the AI Behavioural Analysis component will need to include the development of machine learning algorithms for analysing patterns in data transmissions, as well as the integration of these algorithms into the overall cybersecurity framework of CYLCOMED project. Regular updates and improvements to the algorithms will also be required to ensure their effectiveness in identifying potential security threats.

Finally, effective communication channels will need to be established to ensure that healthcare providers and device manufacturers are promptly alerted to any potential security threats detected by the AI Behavioural Analysis component.

4.1.2 AI-Powered Log Monitoring Solution

The AI-powered log monitoring solution (brought by XLAB) is responsible for the automatic detection of anomalies in system/application logs. Log messages are generated by software systems to capture and report events that occur during system operation. They are critical for diagnosing and troubleshooting issues, detecting system failures, improving performance, and ensuring security. However, the sheer volume and complexity of logs make it difficult for system administrators to manually monitor them for anomalies, requiring automated tools to assist with log analysis and anomaly detection.

The solution will follow a typical log-based anomaly detection workflow known in the literature. First, the initial number of logs has to be collected. The required amount depends on the complexity of patterns present in log sequences. As a rule of thumb, several hundred thousand logs are enough for most use cases. Sometimes even less is sufficient. The important thing is, that the data contains the events and patterns which are expected during the normal operation of the monitored system. The logs are stored in a database (e.g., Elasticsearch[7]).

After the initial amount of data is collected, the training phase has to be initiated. The first step in the training phase is the automatic log template extraction. Unsupervised methods are used for log template extraction from historical log data. A log template represents a static part of a log message with placeholders for parameters which are variable parts of a log message. Extensive hyperparameter tuning is usually not needed for such methods. However, manually adding regular expressions for masking general variables can significantly improve the quality of extracted log templates. Regular expressions are usually used to mask IP addresses, timestamps, identification strings, etc. The trained log template extractor is saved in the model registry (e.g., MLflow[8]).

Next, the anomaly detection model is trained. The log monitoring solution will utilize natural language processing (NLP) techniques to automatically detect anomalies in log messages. The models will be trained in a self-supervised or unsupervised fashion, where they will learn to identify regular patterns and relationships between log templates. The solution will analyse sequences of logs and detect anomalies based on the context in which a log message

---

[7] *https://www.elastic.co/es/what-is/elasticsearch*

[8] *https://mlflow.org/*

appeared. The models are trained on historical data with the assumption that there are no, or a low number of anomalies. The model then learns patterns in the sequences of log messages. There are two main approaches for aggregating log messages into sequences: sliding window and session window sequences. The sliding window can be time-based or can aggregate based on the number of consecutive log messages. Session window sequences are generated based on the session id present in logs. Training the model is compute intensive task and requires Graphics Processing Units (GPUs). A trained model is saved in the model registry.

After the model is trained, inference mode can be initiated. Central Processing Unit (CPU) is usually sufficient for inference. Both, the trained template extractor, and trained model are pulled from the model registry at the inference initialization phase. Next, logs are pulled from the log database. Logs are processed in the same way as in the training phase. First log templates are extracted and aggregated into the sequences. Next, the model is used to compute anomaly scores for logs. An anomaly score is a number between 0 and 1. The higher the number, the more anomalous are the logs. Anomaly detection can also be executed as a periodical job. In this case, the log monitoring tool has to periodically pull the new data since the last execution from the database and run the inference. Alerts can be triggered in case of a high anomaly score in order to notify the system administrator.

4.1.3 Multi-tenancy cloud-native device and platform management

The envisaged cloud-native device and service management solution (provided by Martel) centres around an automated workflow to manage service delivery. CYLCOMED Toolbox services and device software are described by a set of files versioned in an online Git repository. Each file declares a desired instantiation and runtime configuration for some of the components in the Toolbox or connected medical devices. Collectively, the files at a given Git revision describe the deployment state of the Toolbox and connected devices at a point in time. An Infrastructure-as-Code (IaC) operator monitors the Git repository in order to automatically reconcile the desired deployment state with the actual live state of the Toolbox and connected devices. For example, if some connected devices require a security patch, a new Git revision would be created with configuration files that specify which device should get updated. The IaC operator would detect the new Git revision and update the specified devices accordingly.

Automated, version-controlled service delivery has several benefits. 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 as required by the following two requirements MDI02 and TB08 from Appendix C. 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 deployment state declared in the Git repository. This allows to easily recover from tampering and to maintain configuration and software integrity as required by CDN02, CDN03, CDN09, CDN14, BF07, BF12 requirements. Since the Git repository is the "single source of truth", it is also possible to automatically detect misconfigured services or devices, as required by MDI04 requirement, because their runtime configuration would be different than that in the Git repository. Yet another benefit of automation is that, besides the system administrator, no one else need to have access to devices and services, thus dramatically reducing attack surface as required by MDI04 requirement. Finally, the Git repository stores information about who modified the platform state and when, thus furnishing an audit trail that may help to detect security breaches and failure to comply with regulations such as GDPR as required by BF25, TB01 requirements.

We now delve into the mechanics of the deployment process. The visual below (Figure 2) illustrates the context in which the envisaged solution operates and exemplifies the GitOps[9] workflow resulting in the update of a Toolbox service from version-controlled deployment declarations.

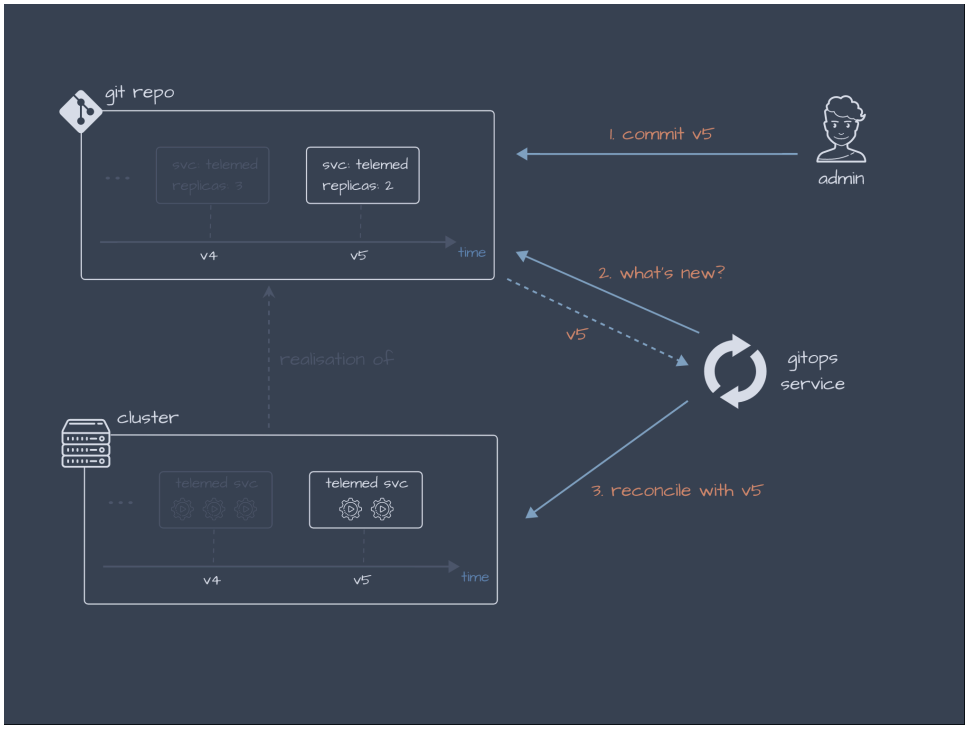

Figure 2 : The GitOps workflow

In this example scenario, the Git repository contains the configuration of Toolbox services. The administrator would like to modify a certain operational parameter (the number of service replicas) of a service (telemed) currently deployed in the CYLCOMED cluster. As hinted by the diagram, the last time this service was modified (Git revision v4), the number of replicas was set to a 3 in the YAML file containing the deployment instructions. Accordingly, the last time the reconciliation process ran, it realised the deployment configuration declared in revision v4 which demanded a telemed service with three replicas.

To enact the desired change, the administrator edits the YAML file to set number of replicas to 2 and subsequently commits the edited file to the Git repository. On receiving a fresh version of this file, Git assigns it a new revision of v5. An IaC operator (GitOps service) periodically polls the Git repository to detect any updates so that the current state of the live CYLCOMED deployment can be reconciled with the latest instructions present in the Git repository. Thus, shortly after revision v5 is committed, the IaC operator recognises that the live system reflects the deployment instructions at revision v4 which has now been superseded by v5, hence it is necessary to bring the live deployment up to date. Therefore, the IaC operator proceeds to issue commands to scale down the number of telemed service instances from three to two which reconciles the cluster state with the current Git revision, v5.

---

[9] *https://www.redhat.com/en/topics/devops/what-is-gitops*

Device updates work similarly with an update service installed on the device and polling the Git repository for changes. Upon detecting a new repository version, the update service reconciles the device software stack with the desired one declared in the repository, e.g., by applying a security patch declared in a YAML file in the Git repository.

To implement the cloud-native device and service management solution outlined so far, we plan to use and build on the following software:

- Argo CD[10] is a comprehensive cloud solution for IaC/DevOps/GitOps. Its main tenet is that the system runtime should be defined declaratively, and version controlled which then makes it possible to automate service deployment and lifecycle management. In this regard it is a good fit for our automated, version-controlled delivery of Toolbox services.
- Mender[11] is a distributed system that provides secure and reliable updates for IoT devices. For our purposes, it complements Argo CD by providing the infrastructure to deliver software updates to connected medical devices.

4.1.4 Decentralized identity management and Data Protection using novel encryption schemes

In the context of CYLCOMED project centralised and decentralised Identity and Access Management (IAM) solutions will be used. Also, advanced cryptography for data protection, combined with decentralised data access control will be implemented.

Figure 3 shows the connections between the IAM & data protection assets and the CYLCOMED pilot environment and other Toolbox components.

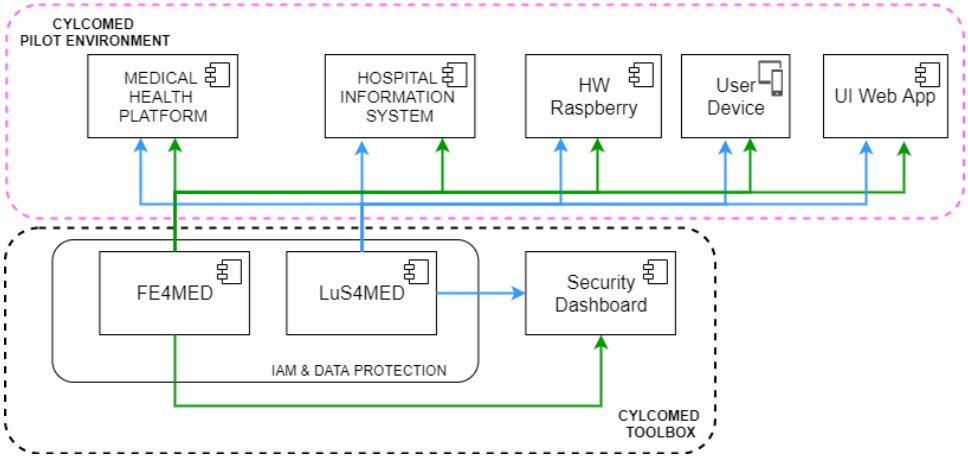

Figure 3 : Connections between the IAM & Data Protection assets and the CYLCOMED environment components and the Security Dashboard asset

Identity and Access Management asset

For the decentralised access control to data, CYLCOMED will provide a self-sovereign data access control solution developed by Atos named LuS4MED. The improvements envisaged

[10] *https://github.com/argoproj/argo-cd*

[11] *https://mender.io/*

during CYLCOMED project to decentralised identity management (alignment with specifications of GAIA-X applicable to EU Health Data Spaces and EU Digital Identity Wallets in the revised eIDAS regulation) will allow to mature identity and data protection assets to TRL 6.

Blue arrows in Figure 3 depicts the connections between the LuS4MED asset and the different components of the CYLCOMED pilot environment, and also with the Security Dashboard asset.

The LuS4MED asset is built by two components (Figure 4):

- The LuS4MED mobile application for storing the verifiable credentials (VC) created by the issuer, i.e., the hospital information system (HIS) or the medical health platform (MHP).
- The LuS4MED broker for integrating the service provider (e.g., HIS or MHP) with the Self-Sovereign Identity (SSI) solution, easing the complexity of this decentralised protocol.

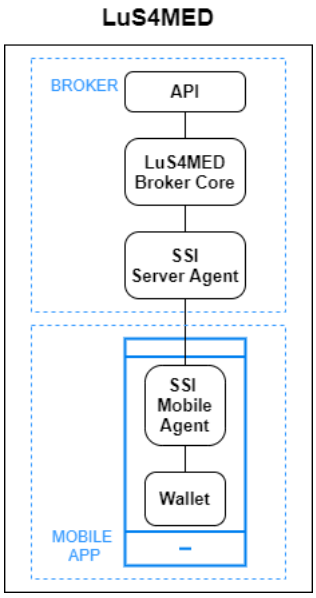

Figure 4 : LuS4MED high-level architecture

The LuS4MED broker will be deployed on the service provider side. In the case of CYLCOMED project on the Raspberry hardware board or the HIS for the hospital equipment (HE) pilot, and on the hospital premises (MHP) for telemedicine platform (TMP) pilot.

The LuS4MED asset provides a simple API for a fast authentication process. The content of the VC must be defined by the HIS and the MHP of each pilot.

Data Protection asset

Regarding data protection, Atos will use novel encryption schemes, namely an attribute-based encryption (ABE) solution, named Functional Encryption for Medical Data (FE4MED) for encrypting data. These data will be decrypted by the final consumer based on the role they play. In this way the final consumer only will see those attributes they are allowed to.

Green arrows in Figure 3 depicts the connections between the FE4MED asset and the different components of the CYLCOMED pilot environment, and also with the Security Dashboard asset.

The FE4MED asset (provided by Atos) comprises two components ():Figure 5):

- A backend service in charge of encrypting/decrypting the data and generating the decryption keys based on ABE scheme. These services are accessible through an API.
- A frontend providing a graphical user interface (GUI) for supporting the user during the encryption process and supporting the asset's configuration and the roles' creation for accessing data.

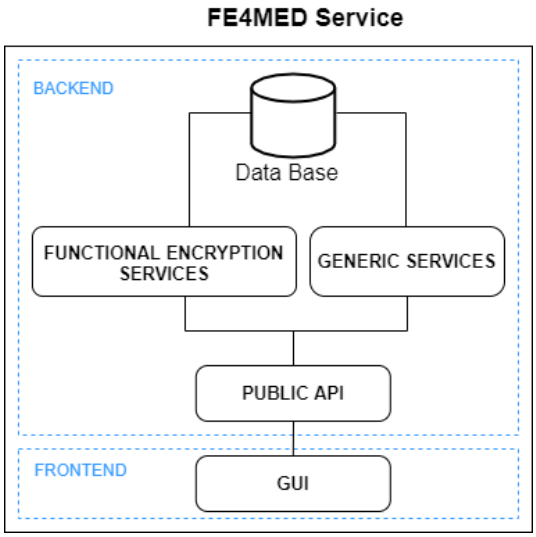

Figure 5 : FE4MED high-level architecture

FE4MED asset will be deployed on the data provider side as trusted entity managing the encryption/decryption process. For the HE pilot on the Raspberry hardware board or the HIS, and on the MHP for TMP pilot. In both cases the encryption process can be triggered automatically based on the frequency set by the hospital system administrator, or manually by the data provider.

FE4MED asset offers an API to users for accessing the functionalities this component provides:

- To the data provider (e.g., devices):
  - Request the data encryption.
  - Request generation of decryption keys for doctors, nurses and hospital staff based on ABE scheme.
- To the data consumer (e.g., doctors, nurses):
  - Request decrypted data based on ABE scheme.
- To administrator staff:
  - Set FE4MED configuration such as the role's creation.

Additionally, relevant information is provided to the Security Dashboard asset for generating security alarms.

Based on the data journey described in section "Generic Scenario for Connected Medical Devices" the functionalities provided by these two assets developed in the IAM & Data Protection set, are related with the requirements of the data protection category included from the step 3 to step 7 of the data journey, i.e., communication device, the transport used to send the data, the data access and the clinician application.

4.1.5 Device integrity checks tools

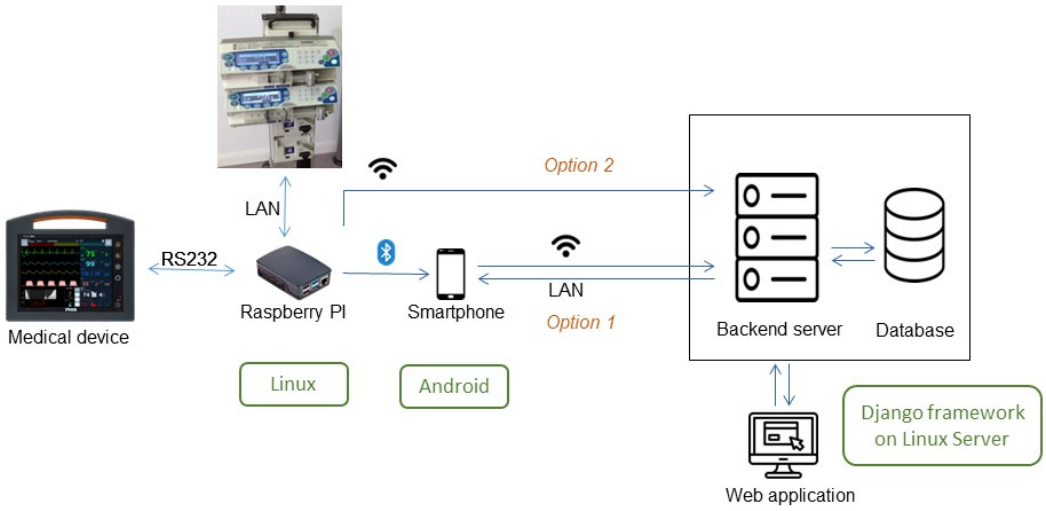

Figure 6 : Hospital Equipment Pilot Architecture

Figure 6 shows current understanding of how the Pilot 1 (Hospital Equipment) should be implemented.

On the one side, the medical device is a multiparameter monitor, which interoperates with an intermediate module, a Raspberry running under Linux OS. It contains the CYLCOMED cybersecurity features as well as performing the interoperability with the infusion pump tree. All three components together represent the medical controller of NMT (muscle relaxation). The operation is carried out to maintain the relaxation values within predefined targets by means of Rocuronium drug infusion.

The medical Data generated during the test will be transmitted to a repository, which is a database with access through a web application. The data to be sent is the patient's relaxation control data (neuromuscular transmission and drug dose). Data is sent in a specific and grouped way (the complete control session or every certain period, if the control is very long). The data delivery format will be JSON.

Regarding the communication between the Raspberry and the server, option 2 depicted in figure 6 is for the moment the preferred one, that is, not to use the mobile as communication means and making instead the communication links directly from the Raspberry to the backend server infrastructure. In principle, this communication is the same as WiFi or Ethernet, although the use of Ethernet may be more secure.

It must be precisely defined the type of data that is going to be exchanged, because the cybersecurity tool operates differently depending on the data type (anonymous, sensitive, non-sensitive) and, in addition, it must be defined the access rights of the roles or user profiles regarding data (system administrators, doctors, nurses, etc).

7Figure 7 depicts the envisaged scenario for integrating the tools related to the IAM & Data Protection Toolbox (the FE4MED for data encryption and Lus4MED for authentication) with the Backend server.

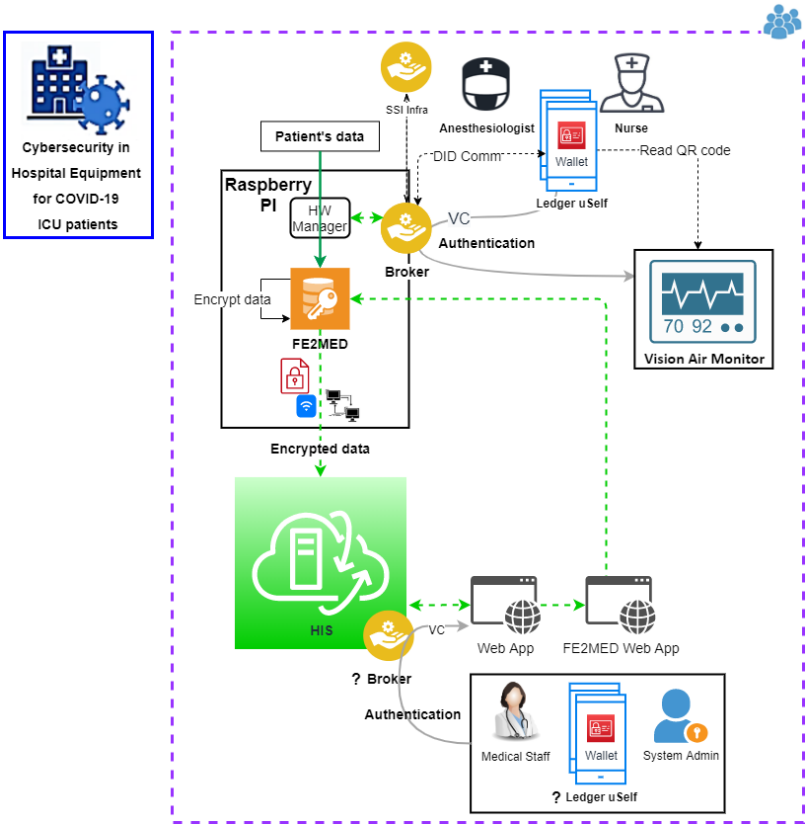

Figure 7 : Envisaged integration of IAM & Data Protection assets in Pilot 1

Regarding authentication, there are concerns about authentication on the monitor side. The proposed solution makes use of the QR code, and it seems that it could solve the access in a very short period of 1 second. In any case, this authentication can be critical on the monitor side; authentication also applies to the users of the web application, so that the authentication part could be covered in the project even if it is ruled out using authentication on the monitor side.

Regarding the "Device Integrity Checker" component, this component must collect information from various CYLCOMED cybersecurity components about security aspects of our devices (monitor, pump tree, Raspberry, server) to the "Security Dashboard". This information is specific to security aspects (e.g., pump tree disconnection, consecutive authentication failures, unauthorized access attempt detection, etc.) and the component is RGB's responsibility.

The objective is to integrate the security related SW components that results from CYLCOMED´s project in a way such that the currently certified legacy devices can avoid going through complete safety or performance verification/validation procedures for re-certification.

4.1.6 Security Dashboard

The CYLCOMED Security Dashboard (provided by Atos) is an integral part of the CYLCOMED framework, designed to provide a centralized platform for monitoring and managing the cybersecurity of connected medical devices. Its main task 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.

The Security Dashboard will have several key responsibilities within the CYLCOMED project, including:

- Real-time monitoring of connected medical devices;
- Alert generation and notification;
- Vulnerability assessment and management;
- Reporting and analysis.

Overall, the CYLCOMED Security Dashboard will play a critical role in ensuring the cybersecurity of connected medical devices, providing needed information to take proactive steps to prevent security breaches and protect patient safety.

4.1.7 Telemedicine platform

MediaClinics Health Platform (MHP) is a telemedicine platform, developed during different EU projects, with the main focus on remote monitoring and it has been tested in different scenarios, ranging from diabetic patients to cardiac patients. Furthermore, MHP covers the whole data cycle, from the acquisition from CMD (that can also be legacy devices) through a mobile application hub to a web application.

Therefore, this makes MHP a suitable example of SaMD because it can be representative of a wide range of telemonitoring scenarios, that can benefit from CYLCOMED Toolbox application and offers the possibility to integrate different tools in different parts.

Particularly, MHP will be the central point of pilot 2, where it will be used to monitor paediatric cardiac patients.

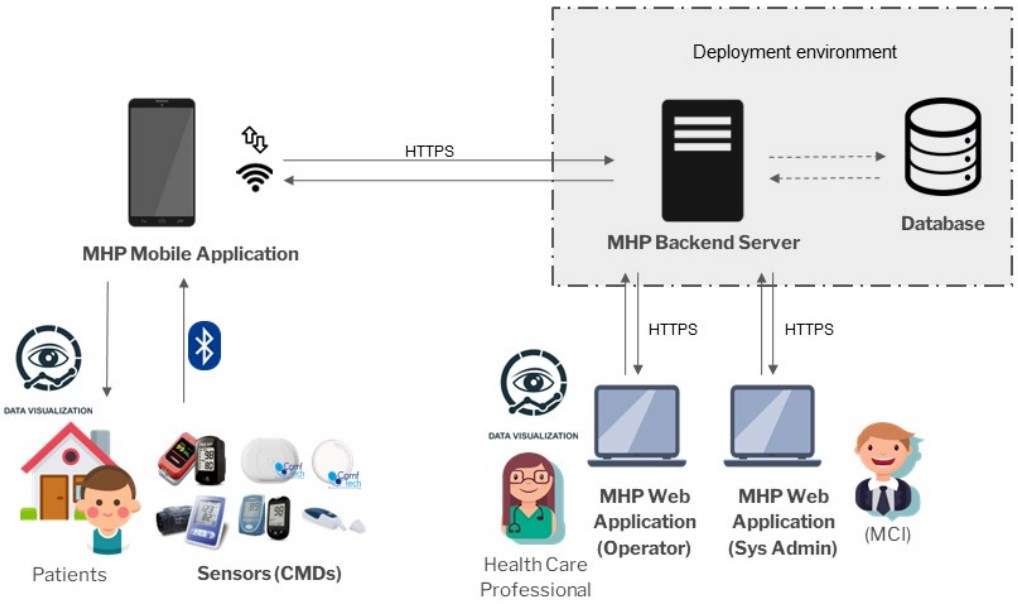

Figure 8 : Baseline data flow of the MHP platform

Figure 8Figure 8 shows the baseline data flow of the MHP platform, from the acquisition at patient's home to the visualization by health care professionals.

As a SaMD, MHP already presents security features, that will be improved during the CYLCOMED project:

- Access to the platform is protected using OAuth authentication, requiring all users to perform login (using credentials) to access the systems;
- The platform enforces access control policies to limit the permissions of each user, following the principle of least privilege;
- All the internet communications occurring in MHP use the HTTPS protocol, ensuring that data are encrypted in transit.

TOOLBOX ARCHITECTURE

CYLCOMED will deliver to its stakeholders (manufacturers, integrators and users of CMDs), as well as to platforms managing CMDs, a comprehensive set of tools.

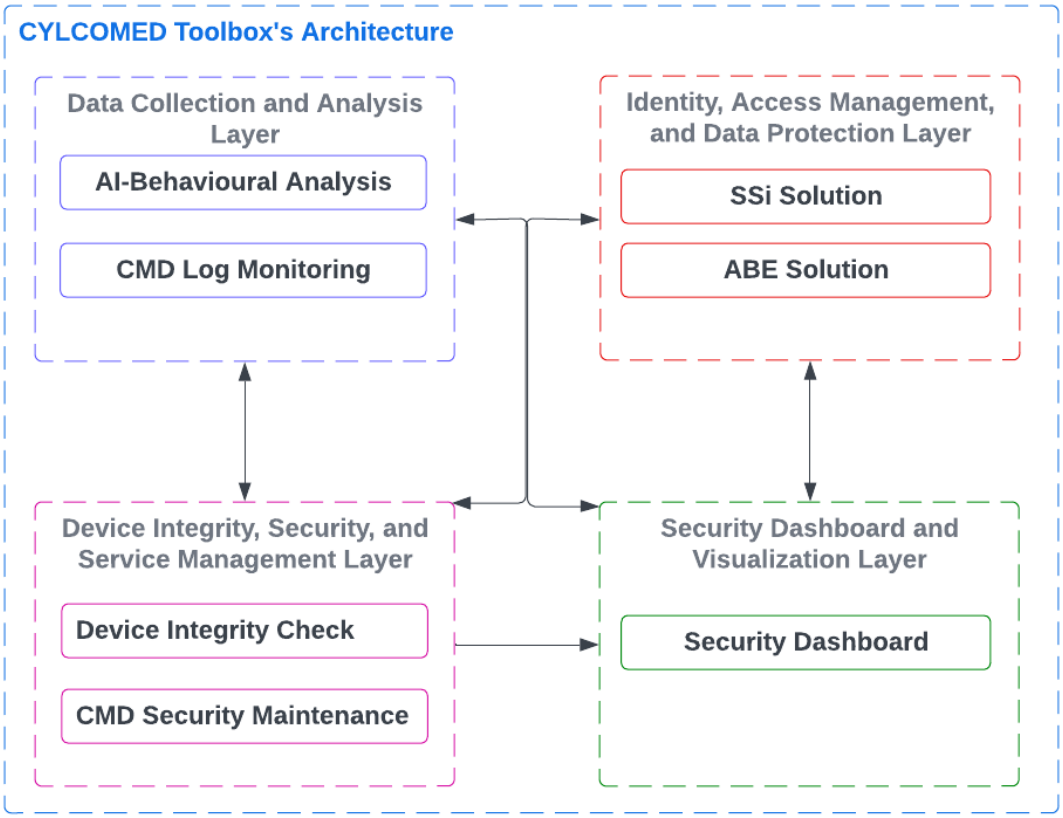

Figure 9 : Current CYLCOMED's Toolbox Architecture

The present CYLCOMED Toolbox architecture proposal effectively addresses the requirements identified during the initial stage of the project, as well as those outlined in the original project proposal. This thorough analysis has led to the development of an architecture comprising four distinct layers, each containing various components that will be developed throughout the project's duration. A detailed description of each layer within this architecture is provided below:

- **Data Collection and Analysis Layer**: This layer is responsible for collecting, analyzing, and detecting anomalies in logs generated by CMDs and the platform that manages CMDs. It includes AI-based CMD Behavioral Analysis & Log Monitoring,

which leverages state-of-the-art AI techniques to monitor logs and detect potential attacks or malfunctions. The Anomaly Detection capability of this layer identifies unusual behavior within the logs, while the CMD Log Monitoring component processes logs in real-time to identify threats.
    - **Interaction**: The Data Collection and Analysis Layer provides input to the Device Integrity, Security, and Service Management Layer, helping to identify threats and potential security issues that need to be addressed.
- **Device Integrity, Security, and Service Management Layer**: This layer is responsible for managing the security of devices and services while maintaining their integrity.
  The layer ensures that connected medical devices are up to date with the latest security patches and can securely update their configurations as needed. It also checks for potential security risks in configuration settings to minimize vulnerabilities.
  In addition, this layer provides support for secure management of devices and services, allowing different providers to manage their devices and services without conflicts while ensuring accountability in the management process. This layer also aims to protect CMDs from cybersecurity hazards and streamline communication with other medical devices and the hospital information system.
  Lastly, the Device Integrity Check and CMD Security Maintenance components play a critical role in ensuring the proper functioning and security of connected medical devices.
    - **Interaction**: This layer leverages the data and analysis provided by the Data Collection and Analysis Layer to address security concerns and maintain device integrity. Furthermore, it offers input to the Identity, Access Management, and Data Protection Layer, which is responsible for managing access control and secure data exchange.
- **Identity, Access Management, and Data Protection Layer**: This layer contributes to handling authentication, authorization, and accountability in the CYLCOMED Toolbox. It implements decentralized and user-centric identity management (SSI), ensuring secure access control and protection against unauthorized access. This layer facilitates privacy-friendly data sharing among devices and healthcare providers, while providing novel encryption schemes (ABE) to protect sensitive data.
    - **Interaction**: This layer relies on the Device Integrity, Security, and Service Management Layer to manage access control and data protection, while also providing input to the Security Dashboard and Visualization Layer for visualizing security events and alerts. Furthermore, this layer provides information regarding unusual behaviour, if any, to the data collection analysis and log analysis.
- **Security Dashboard and Visualization Layer**: This layer focuses on collecting, correlating, and visually representing security events and alerts from the other layers in real-time. It normalizes and enriches security events, processes them using a correlation engine, and generates a 360-degree situational picture for detecting threats and calculating risk exposure.
    - **Interaction**: The Security Dashboard and Visualization Layer receives input from the Identity, Access Management, and Data Protection Layer, the Device Integrity, Security, and Service Management Layer and, the Data Collection and Analysis Layer to create a comprehensive visualization of the security landscape and potential threats.

4.2.1 Generic Scenario for Connected Medical Devices

With the aim of making the requirements that are to be elicited, applicable not only for the specifically determiner pilots for testing the CYLCOMED tools and dashboard, but a broad analysis has also been carried out that tries to capture the minimal elements for the immense variety of different medical devices that can be connected for medical purposes both in the clinical environment and in the diverse settings of telemonitoring care.

Ensuring cybersecurity for data collected from medical devices is a challenging task due to the complex journey that data undergoes from the device to the clinician using it. The purpose of this section is to analyse the data journey and identify its steps. In the following section, we will outline the generic data journey as the first step towards organizing these requirements.

Data journey

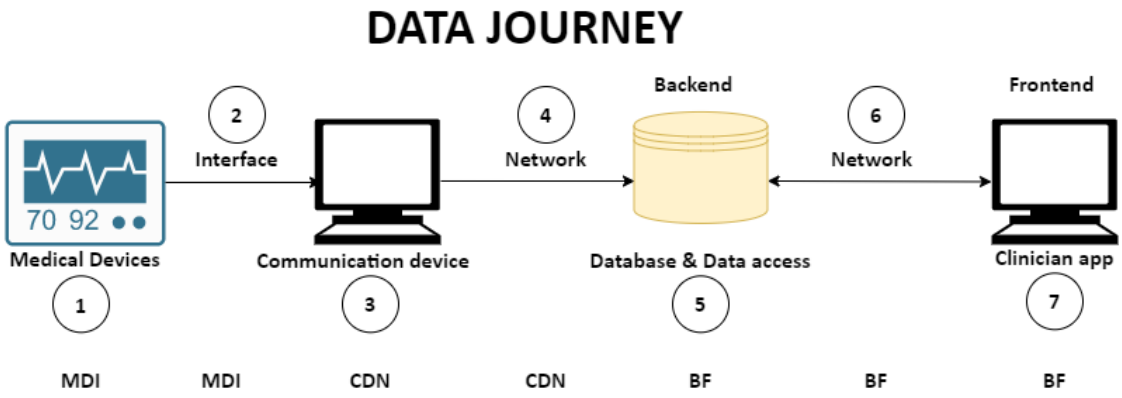

Figure 10 : Data Journey

Figure 10 shows the journey for data from the medical device to the clinician application. Each step has its own cybersecurity requirements. 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

This general model was created for aligning the different use cases of the two pilots. Additionally, it also aligns with the available market solutions.

Medical devices and their interfaces

Data is collected using a sensor (1) that could be either a medical device by itself or that can be part of a machine which the patient is connected to. The sensor produces typically a flow of numeric values that are sent (2) to another device capable of transmitting them to a remote server. There are thousands of different medical devices from many different manufacturers, using many different protocols (mainly proprietary) and different interfaces. In general, data is sent without any encryption technology.

The most common connection interfaces used by medical devices available in the market are:

- Ethernet;
- Bluetooth;
- Wi-Fi;

- Serial RS232;
- USB to Serial RS232.

Medical devices have one or two different interfaces to provide a connectivity channel that will allow the communication device to transmit medical data.

From a cybersecurity perspective, each technology has a different set of requirements that must be considered.

Communication device

The communication device (step 3) receives the data coming from the medical device, and optionally does some processing to the data and sends them through a network to a database (backend). An application is usually deployed in this communication device to monitor the data being captured, to configure the medical devices that are being connected and to perform some additional tasks.

Network to database

When data is produced at a patient's home, 4G or Wi-Fi + home internet connectivity are typically used as the transport layer (step 4). Data destination can be a cloud environment outside the hospital network or can be in the hospital intranet infrastructure.

When medical data is produced inside the hospital, ethernet network or Wi-Fi connection are used.

Database & Data Access (backend)

Medical data will be stored in a database (step 5). Data governance and compliance must be guaranteed, and GDPR must be considered at this stage. Usually, a backend application will manage the data and its access.

Network to clinician application

Requirements for the communication channel (step 6) between the frontend application and the backend can be different depending on where the database is installed (external cloud or hospital network).

When backend is in the hospital network, private ethernet network or Wi-Fi connection are typically used.

When backend is located in an external cloud, additional considerations should be taken, as data will be transmitted from an external site to the hospital network.

Clinicians' application (frontend)

The clinical application (step 7) is the interface for clinicians to use, explore and analyse all the data coming from medical devices.

4.2.2 Use Case 1: MediaClinics Health Platform

In the telemedicine platform (Figure 8) 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 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 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 backend server, Health Care professional and system administrator can visualize them through the MHP Web application, that can be accessed from any standard browser.

4.2.3 Use Case 2: Hospital Equipment

Figure 6 of section 4.1.5 shows the main components of the RGB use case. These components 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 is running on the Raspberry. 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 WiFi.
- Option 2. The Raspberry directly transmits the data to the Backend server via WiFi.

REQUIREMENTS LIST DESCRIPTION

An initial version of the list of technical requirements for the development of the CYLCOMED Toolbox has been elicited. After several iterations it has been determined that it is most productive to organize the requirements around the generic data flow scenario for connected medical devices. The so-called patient's data journey has been worked out with the joint effort of technical and clinical partners of the consortium and it has been described in the previous section. For ease of reading, they have been separated into four different tables which can be found in the Appendix C.

The first table, **Medical Devices and Interface Table** (1st and 2nd steps of the patient's data journey) lists requirements to be taken into account in order to increase the security of the raw data from the time it is collected from the sensor attached to the patient until it is sent to the communications device that will transmit the clinical parameters to the next element of the

information architecture. In this case it is necessary to note that we are working with the assumption that the medical devices have already been certified and comply with the security measures already foreseen in the legislation. The project is concerned with cybersecurity issues from the time the data leaves the sensor until it reaches the communication device that acts as hub to relay data.

The second table, **Communication Device and Network Table** (3rd and 4th steps of the patient's data journey), enumerates a first compilation of the requirements the CYLCOMED Toolbox must contemplate to ensure the integrity, confidentiality and traceability of the clinical data that are sent from the CMDs in the patient's environment to the backend where they will be stored.

The raw clinical data stored in the backend is useless without the processing and visualization software that help doctors and nurses assess the health status of the patient. Usually, a graphical interface as desktop or web application is implemented for that purpose. The third **Backend & Frontend Table** (5th, 6th and 7th steps of the patient's data journey) corresponds to the functional and non-functional requirements for the CYLCOMED Toolbox to be able to protect the telemonitoring application in the hospital IT environment.

A more focused approach has indicated that a fourth table should be added to the other three in order to concentrate on the technical requirements for the CYLCOMED security Toolbox: The **Toolbox Requirements Table**.

There has been a trade-off between general requirements that should apply to comply with current regulations and standards, and the actual scenarios for the pilots that will be carried out during the project. In deliverable 3.2 relevant requirements that fit more closely the pilots and the Toolbox will be elicited. Additionally, the current set of requirements will be updated according to the work effort of WP3 aligned to WP4 and WP5 efforts.

4.3.1 Map of Assets and Requirements

Table 1 provides information of the different categories of cybersecurity requirements covered by the assets brought into the CYLCOMED project.

Category	Description	CYLCOMED Tools	Security Measures
Cryptography	This includes the algorithms, protocols, key management and procedures for encrypting data at rest and in motion.	ABE solution	KP/CP-ABE schemas will be applied on health records on specific scenarios. .
Identity and Access Management	This includes the authentication mechanisms used for accessing devices, data, for establishing secure connections, access permissions.	SSI solution	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.	IaC solution	IaC 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 attack surface.
Design	This includes design principles applied to the device/network/service.	ABE solution IaC solution	Modular design and privacy by design is applied on ABE solution. IaC 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 deployment state declared in the Git repository.
Secure Communication	Considerations that must be taken into account when establishing connection, exchanging information and allowing connection.	IaC solution	IaC components connect to devices and cloud services using mutual TLS.
Software Security	Measures taken into account to make the software secure.	Security Dashboard AI-based Behavioural Analysis	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 AI-based Behavioural Analysis component uses AI and Machine Learning technologies to model normal behaviour and detect abnormalities, it indirectly contributes to making the software more secure.

Monitoring	Includes every monitoring system used to monitor device/service/system accesses, performances, behaviour, configuration, changes of credentials, etc.	ABE solution SSI solution IaC solution Security Dashboard AI-based Behavioural Analysis	ABE 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 AI-based Behavioural Analysis 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.	IaC solution AI-based Behavioural Analysis	IaC 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 AI-based Behavioural Analysis 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
Availability	Measures to maintain data/device/service/system available for authorized use.	IaC solution Security Dashboard	Automated, version-controlled service delivery dramatically reduces the time needed to recover from severe production incidents caused by faulty deployments or security breaches. Thus, IaC plays a role in increasing overall system availability. By providing a real-time graphical representation of detected threats, the Security Dashboard tool ensures that important security information is always available for authorized use

Data protection mechanisms	Mechanisms to maintain data secured.	ABE solution SSI solution Security Dashboard	Data encryption by ABE schemes Decentralised authentication mechanisms for accessing data 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.	ABE solution	Use of Privacy Enhanced techniques (ABE) for protecting user data privacy

Table 1 : Requirements Mapping

Conclusions

This deliverable reflects the essential first steps towards the successful completion of CYLCOMED project's objectives. It has collected the sources to establish the baseline analysis of regulations and standards relevant to cybersecurity of connected medical devices, for both in hospitals' premises and in telemedicine settings.

An initial description of each asset brought into the project has been provided, as well as a first draft of the architecture of the security Toolbox, as a main outcome of the project. At the same time the planned architecture for the test pilots have been exposed. That way the context for the technical requirements has been set. A short summary of the requirements finishes off the document.

For ease of reference, the bulk of the output of this task 3.1 has been placed in the Appendixes, namely, the catalogue of legal sources, the listing of standards and guides, and the enumeration of the technical, functional, and non-functional, requirements.

In particular, this is the initial process for identifying requirements for the project technologies and in defining recommendations for an appropriate management of cybersecurity aspects. This thorough review of the state of the art for CMD cybersecurity includes the identification of requirements based on evidence and assessment of the applicability (and revision) of current cybersecurity guidance (MDCG 2019-16, IMDRF/CYBER WG/N60, IMDRF/GRRP WG/N47, Cybersecurity Act among others), to CMDs, including software.

The work implemented for this report has run in parallel with two other Work Packages that are strongly related to this one, namely, WP2 and WP5.

WP2 aims to provide an ethical and legal framework paying special attention to MDCG 2019-16 Guidance on Cybersecurity for Medical Devices, the Medical Device Regulations as well as the EU data protection, privacy, and cybersecurity legislation. The outcome of this Work Package will be a comprehensive overview of legal frameworks, including guidelines for compliance on relevant ethical and legal principles regarding the CYLCOMED technologies. The output of WP2 aligned to the results of WP3 will serve to define further actions that should be taken by regulators, lawmakers, and policymakers to advance the right ethically and legally compliant use of innovative solutions to protect CMD.

On top of that, Work Package 5 is already working on both the detailed technical design and implementation (including suitable packaging and easy to integrate APIs) in two major iterations for CYLCOMED Cybersecurity Toolbox, because WP5 relies on the cybersecurity baseline studies, functional (also legal and ethical) requirements and high-level specifications from WP2 and WP3. Outcomes of WP5 will then be integrated and demonstrated in WP6. The interactions among the two work packages will allow the continuous improvement of the algorithms, as well as obtaining feedback about the usability of the developed solutions in both iterations for improvement of the final Toolbox.

This work will be continued into the identification of legal and regulatory challenges, in the context of potential needs for revision of the cybersecurity MDCG 2019-16. The ultimate goal is to provide recommendations to regulators, policymakers, and lawmakers with the objective of advancing the right ethically and legally compliant use of innovative solutions to enhance cybersecurity of CMDs, with a special focus on how the MDCG 2019-16 Guidance should be revised. Based on the consortium's experience gained in CYLCOMED, the project will make recommendations to better address specificities of CMDs/IVDs/SaMD, of different risk classes.

The following report in this Work Package will collect the next phase in the development started off here. Risk and gap analysis will be conducted when the patient safety concerns, regulations, performance of devices, and a most fitted solution are considered. So, it will be done within WP3 (for D3.2 "Requirements and specifications consolidation") when a more fine-

grained list of requirements is elicited. Finally, WP4 “Risk Management for Connected Medical Devices” has also contributed to this deliverable, as it can be seen in the requirements collection.

References

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

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

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

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

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

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

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

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

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

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1685784856203

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1685569446136

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1685569634127

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

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

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

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

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

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

[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

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

Appendix A. Requirements (Legal and Standards)

Funded by Horizon Europe Framework Programme of the European Union

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 should be made aware of this right before granting consent.	GDPR
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

Funded by Horizon Europe Framework Programme of the European Union

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
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

Funded by Horizon Europe Framework Programme of the European Union

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
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

Funded by Horizon Europe Framework Programme of the European Union

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
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

Funded by Horizon Europe Framework Programme of the European Union

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
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 programmes 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

Funded by Horizon Europe Framework Programme of the European Union

IT Security	ITS-26	Access rights	Least privileges must take into account 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
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 Health Information System (HIS) 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
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

Funded by Horizon Europe Framework Programme of the European Union

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 should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity in accordance with the generally acknowledged state of the art.	AI Act Proposal
AI systems	AI-2	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 Proposal
AI systems	AI-3	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 Proposal
AI systems	AI-4	AI Cybersecurity	A quality management system shall be documented in a systematic and orderly manner.	AI Act Proposal
AI systems	AI-5	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 Proposal

Table 2 : Requirements (Legal and Standards)

Funded by Horizon Europe Framework Programme of the European Union

Appendix B. Requirements from Standards and Best Practices

The requirements from standards and best practices table were compiled based on the following references:

- ENISA Baseline Security Recommendations for IoT in the context of Critical Infrastructures [27] – IoT-BASELINE
- ENISA smartphone guidelines tool (SMASHING tool) [29] - SMASHING
- ENISA cloud security for healthcare services [31] – CLOUD-HEALTH
- ENISA security aspects of virtualization [32] - VIRTUAL

Category	Code	Control name	Description	Source
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).	IOT-BASELINE SMASHING CLOUD-HEALTH
Cryptography	CRYPTO-2	Key Management	Cryptographic keys and materials must be securely managed.	IOT-BASELINE SMASHING CLOUD-HEALTH
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).	IOT-BASELINE SMASHING CLOUD-HEALTH
Cryptography	CRYPTO-4	Key Recovery	Adequate key recovery processes and technologies must be in place.	CLOUD-HEALTH
Cryptography	CRYPTO-5	Risk Analysis	Cryptographic algorithms and protocols must be evaluated based on risk analysis for the data and business.	IOT-BASELINE SMASHING CLOUD-HEALTH
Cryptography	CRYPTO-6	Policy	Encryption policy must be defined, including controls on cryptographic authentication and integrity, and key management.	IOT-BASELINE
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.	IOT-BASELINE CLOUD-HEALTH VIRTUAL

Funded by Horizon Europe Framework Programme of the European Union

Identity and Access Management	IAM-2	Authentication	Authentication mechanism must be adequate for the context they are in (based on the risk analysis).	IOT-BASELINE SMASHING VIRTUAL
Identity and Access Management	IAM-3	Credentials Handling	Authentication credentials, such as biometrics data, passwords, certificates, must be properly protected.	IOT-BASELINE SMASHING
Identity and Access Management	IAM-4	Log-in Protection	Log-in protection must be employed in order to protect the system/device from unauthorized access.	SMASHING
Identity and Access Management	IAM-5	Authentication strength	The authentication strength must reflect the risk analysis and be adequate for the context at hand.	IOT-BASELINE SMASHING CLOUD-HEALTH
Identity and Access Management	IAM-6	Account Recovery Mechanism	Adequate account recovery process and mechanisms must be in place.	IOT-BASELINE CLOUD-HEALTH
Identity and Access Management	IAM-7	Permissions	Permissions must be set taking into account the principle of least privileges, and the implementation must enforce the defined policies.	SMASHING VIRTUAL
Identity and Access Management	IAM-8	Biometrics	When biometrics are employed, best practices must be employed in order to guarantee a minimum level of security.	SMASHING
Identity and Access Management	IAM-9	Temporal validation	Temporal validity interval authorizations should only be used when the systems should be synchronized with a trusted authoritative timeserver. In any other case, this authorization mechanism must not be used.	SMASHING VIRTUAL
Identity and Access Management	IAM-10	Authentication information change	There must be mechanisms and/or processes in place in order for a user to change its authentication information, like password or any authentication tokens.	SMASHING
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).	SMASHING
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.	SMASHING
Identity and Access Management	IAM-13	Authentication Factors	Consider using multifactor authentication for applications/services accessing sensitive data or interfaces.	SMASHING
Identity and Access Management	IAM-14	Policies	The system must ensure access policies take into account user access data, application interfaces, systems, and the network or network components for each service.	SMASHING CLOUD-HEALTH

Funded by Horizon Europe Framework Programme of the European Union

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.	VIRTUAL
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.	IOT-BASELINE
Configuration	CONF-2	Security by default	The system should provide minimum security, by deploying and configuring a minimum set of security controls.	VIRTUAL IOT-BASELINE SMASHING
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.	IOT-BASELINE
Design	DESIGN-2	Hardware isolation	The device should have hardware isolation in place.	IOT-BASELINE
Design	DESIGN-3	Hard disassemble	The device should be hardly disassembled.	ITO-BASELINE
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.	IOT-BASELINE
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.	VIRTUAL ITO-BASELINE
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.	SMASHING
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.	CLOUD-HEALTH
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.	SMASHING IOT-BASELINE
Secure Communication	SECOM-2	Data Authenticity	Data in transit must be signed.	IOT-BASELINE
Secure Communication	SECOM-3	Device Authenticity	Always identify and verify/authenticate the devices connected to the network before trust can be established.	IOT-BASELINE SMASHING
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.	VIRTUAL IOT-BASELINE

Funded by Horizon Europe Framework Programme of the European Union

Secure Communication	SECOM-5	Rate Limiting	Traffic sent and received by a network should have rate limiting, to reduce the risk of automated attacks.	IOT-BASELINE VIRTUAL
Secure Communication	SECOM-6	Restricted Communications	Traffic between untrusted and trusted connections of network environments and virtual instances must be restricted.	CLOUD-HEALTH
Secure Communication	SECOM-7	Document interfaces	All allowed services, protocols, ports and compensating controls are documented.	CLOUD-HEALTH
Secure Communication	SECOM-8	Network Segmentation	Separate large networks is 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.	IOT-BASELINE CLOUD-HEALTH
Secure Communication	SECOM-9	Secure Session	Session communication must follow the best practices and standards.	SMASHING
Software Security	SOFTWARE-1	Error Messages	Do not reveal sensitive information such as usernames, personal data and others through error messages.	SMASHING
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.	IOT-BASELINE SMASHING CLOUD-HEALTH
Software Security	SOFTWARE-3	Session Keys	Th system must use unpredictable session identifiers with high entropy.	IOT-BASELINE SMASHING
Software Security	SOFTWARE-4	Authentication and Authorisation	Both authentication and authorization controls should be implemented on the server side.	SMASHING
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). 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.	SMASHING CLOUD-HEALTH
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.	SMASHING
Software Security	SOFTWARE-7	Session management	Ensure that session management is handled securely after the initial authentication, using appropriate security protocols.	SMASHING IOT-BASELINE CLOUD-HEALTH
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.	IOT-BASELINE
Software Security	SOFTWARE-9	Update and security patches	The system must have a software update mechanism that enables updating the software for	ITO-BASELINE

Funded by Horizon Europe Framework Programme of the European Union

			a newer version, and for security patches downloading and installing.	
Monitoring	MONITOR-1	Traffic Monitoring	Traffic between untrusted and trusted connections of network environments and virtual instances must be monitored.	IOT-BASELINE SMASHING CLOUD-HEALTH VIRTUAL
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.	VIRTUAL IOT-BASELINE
Monitoring	MONITOR-3	Log data security	Log data must be protected.	IOT-BASELINE CLOUD-HEALTH VIRTUAL
Monitoring	MONITOR-4	User authentication logging	Logging system for user authentication must be in place.	ITO-BASELINE
Monitoring	MONITOR-5	Management of accounts and access rights logging	Logging system for account and access rights management must be in place.	IOT-BASELINE SMASHING CLOUD-HEALTH VIRTUAL
Monitoring	MONITOR-6	Security Rules Modification logging	Logging system for security rules modification must be in place.	IOT-BASELINE SMASHING CLOUD-HEALTH VIRTUAL
Monitoring	MONITOR-7	System functioning logging	Logging system for system functioning must be in place.	IOT-BASELINE
Monitoring	MONITOR-8	Audits/assessments	Conduct periodic audits and reviews.	IOT-BASELINE CLOUD-HEALTH
Monitoring	MONITOR-9	Authentication data protection	Passwords, keys or any other credentials must not be visible in cache or logs.	SMASHING
Monitoring	MONITOR-10	Risk Analysis	Define or identify requirements for event logging, including logging requirements for cloud service providers.	CLOUD-HEALTH
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.	CLOUD-HEALTH
Monitoring	MONITOR-12	User Activity	Logging system for users activities must be in place.	IOT-BASELINE CLOUD-HEALTH VIRTUAL
Monitoring	MONITOR-13	Configuration assessments	Systems configuration must be checked regularly and assessed against defined standards.	IOT-BASELINE

Funded by Horizon Europe Framework Programme of the European Union

Integrity	INTEGRITY-1	Boot integrity	There must be a mechanism for boot integrity check in order to detect manipulation of the host OS and software, rootkits, viruses and worms.	IOT-BASELINE
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.	ITO-BASELINE
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.	SMASHING
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.	IOT-BASELINE CLOUD-HEALTH VIRTUAL
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
Integrity	INTEGRITY-6	Application Integrity	Whenever possible, check the application integrity using native platform services ((e.g., Android SafetyNet attestation, iOS App Store receipt).	SMASHING IOT-BASELINE
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).	SMASHING
Availability	AVAILABILITY-1	Industry Standards	Data, communications, and security protocols must follow industry-standards.	VIRTUAL CLOUD-HEALTH
Availability	AVAILABILITY-2	Interoperability	Service APIs must use open and published API to support interoperability between components and applications.	CLOUD-HEALTH
Availability	AVAILABILITY-3	DDoS protection	The system/service must use DDoS-resistant an Load-Balancing infrastructure to protect their services.	IOT-BASELINE
Availability	AVAILABILITY-4	Communication Redundancy	There must be possible to establish more than one secure communication paths between the same systems.	VIRTUAL
Availability	AVAILABILITY-5	Energy	The system must have adequate energy supply system.	IOT-BASELINE
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.)	VIRTUAL
Data protection mechanisms	DATA-2	Data Backup	The system has a backup system that is adequate.	IOT-BASELINE CLOUD-HEALTH VIRTUAL
Data protection mechanisms	DATA-3	Data Integrity	Data integrity processes and mechanisms must be implemented.	IOT-BASELINE SMASHING

Funded by Horizon Europe Framework Programme of the European Union

				CLOUD-HEALTH VIRTUAL
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 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 has to explicitly turn on a setting.	SMASHING
Privacy	PRIVACY-2	Check data	Mechanisms and processes must be in place to check whether data collection is not excessive with regard to the consent that has been granted by the user.	SMASHING
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.	SMASHING
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.	SMASHING
Privacy	PRIVACY-5	Privacy Enhancing Technologies	Whenever possible and appropriate, deploy privacy enhancing technologies, that support data minimization, anonymization and security of personal data.	SMASHING
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.	SMASHING
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).	SMASHING
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.	CLOUD-HEALTH SMASHING
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.	SHASHING COULD-HEALTH

Funded by Horizon Europe Framework Programme of the European Union

Table 3 : Requirements from Standards and Best Practices

Funded by Horizon Europe Framework Programme of the European Union

Appendix C. Requirements (CYLCOMED)

Medical Devices and Interfaces Requirements Table

ID	Requirement
MDI01	Medical devices MUST be certified (MDR 2017/745 and 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 4 : Medical devices and interfaces requirements table

Communication Device & Network Requirements Table

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

Funded by Horizon Europe Framework Programme of the European Union

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
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 5 : Communication device & Network requirements

Funded by Horizon Europe Framework Programme of the European Union

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
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)

Funded by Horizon Europe Framework Programme of the European Union

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

Funded by Horizon Europe Framework Programme of the European Union

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 6 : Backend & Frontend requirements table

Toolbox Requirements Table

ID	Requirement
TB01	The system MUST comply with the GDPR data protection requirements
TB02	The system MUST provide access to users through the use of a proper authentication mechanisms (e.g., username and password, biometrics)
TB03	System SHOULD use secure communication protocols, such as SSL/TLS, to prevent eavesdropping and data tampering
TB04	The system SHOULD contain an AI-based log monitoring solution.
TB05	Log monitoring models SHOULD be trained in an unsupervised or self-supervised fashion besides supervised
TB06	Log monitoring solution SHOULD analyse system/application logs and assign them anomaly scores.
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).
TB08	The Toolbox SHOULD match the medical devices installed at the hospital against the public known vulnerabilities.

Funded by Horizon Europe Framework Programme of the European Union

TB09	The cybersecurity dashboard SHOULD include advanced filtering and search features to allow users to quickly and effectively navigate the generated logs and alerts
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
TB11	The cybersecurity dashboard SHOULD incorporate an automated threat prioritization mechanism that ranks potential threats based on their severity and potential impact
TB12	Adequate authenticity, integrity and access control mechanisms for the training data MUST be protected
TB13	The log monitoring models training environment MUST be properly protected against unauthorized accesses
TB14	The system MUST provide fast and secure access to authorized users to manipulate its components
TB15	The Log monitoring models SHOULD be protected with adequate integrity controls and consistency checks.
TB16	Decentralized identity verification mechanism SHOULD be provided, in order to facilitate the user access to the smartphone and hospital IT system environment

Table 7 : ToolBox Requirements table

Funded by Horizon Europe Framework Programme of the European Union

Appendix D. Glossary

This table compiles a glossary of the most important terms appearing in current regulation concerning cybersecurity of connected devices.

Term	Definition/Meaning
Communication Security Domain	Protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users
Documentation	MDR explicitly requests from manufacturers to establish, implement, document and maintain a risk management system. Manufacturers of devices other than custom-made devices shall draw up and keep up to date technical documentation for those devices that shall include the elements set in Annexes II (technical documentation) and III (technical documentation on post-market surveillance). Documentation shall contain information for the demonstration of conformity with the general safety and performance requirements set out in Medical Devices Regulations Annex I. These include security requirements to ensure safety and effectiveness of products against security risks and threats and shall comprise a justification, validation and verification of the solutions adopted to meet those requirements (e.g., methods and results of security testing).
Expectations on the Operating Environment	Expectations on the operating environment might include protection and performance characteristics. Often the expectations are common best practice, often called “good security hygiene”. Expectations on the intended operating environment should be clearly documented and communicated to the operator.
Exploitable Cybersecurity Vulnerabilities and Reasonably Foreseeable Misuse	Due to the complexity of software development, software configuration and interdependencies between software components, cybersecurity vulnerabilities exist in most products. Whether or not a vulnerability will be discovered and if it will be exploited is unknown until it occurs. The general assumption is that any vulnerability which is deemed to be exploitable for a given implementation of software, might be discovered, and exploited over time and as such should be regarded as an enabler for reasonably foreseeable misuse. During the risk management process, the manufacturer should foresee or evaluate the potential exploitation of those vulnerabilities that may be a result of reasonably foreseeable misuse. This, however, may depend on the specific situation.

Funded by Horizon Europe Framework Programme of the European Union

Healthcare and medical professionals	Healthcare and medical professionals (including medical doctors, nurses, radiologists and radiographers, pathologists, etc.) are responsible for the use of medical devices for their purposes, e.g., to diagnose, prevent, monitor, treat or alleviate disease or injury patients. These users may access, review and exchange data with the devices, and may be responsible for the patient's education and establishing software and devices parameters of usage.
Information Security	Protection against the threat of theft, deletion, or alteration of stored or transmitted data within a cyber system
Information to be provided to healthcare providers	See non-exhaustive list in pp.27-28 of MDCG 2019-16 Clinicians/physicians should be provided with the information they need to have meaningful discussion with their patients about the risks and benefits of the device they use, including cybersecurity risks. Provision of information for Medical Device Software (MDSW) users should be tailored to where the device is used (e.g. home environment with limited cyber protection, public environment).
Instructions for Use	See details in pp.24-27 of MDCG 2019-16. Main aspects to include: - High level summary of risk profile of the medical device and the corresponding IT security objectives (e.g., processing/protection of sensitive information, requirement for uninterrupted operation etc.) - Medical device IT characteristics - Installation, configuration and operation of the medical device - User requirements in terms of training / required skills, including IT skills required for the installation, configuration and operation of the medical device - Secure configuration and application of security updates for the medical device - Minimum requirements for the workstations intended for user operations: hardware features, operating system versions, peripheral devices, etc. - Requirements regarding the operating environment (hardware, network characteristics, security controls etc.). - Instructions for administrators or security operation manuals
Integrator	The main responsibility of the integrator is the installation and configuration of the system and the integration into the operator's environment. The integrator should ensure that the system is configured in such a way that it can operate securely in the health and medical service target environment. Integration per se does not alter or extend the intended use of the essential medical functions of the individual medical devices.

Funded by Horizon Europe Framework Programme of the European Union

	• Assess reasonable level of security for the operating environment; • Integrate the system into the environment at the operator site, including secure configuration of the system; • Provide required documentation and training to operator and operator personnel; • Provide support for patching and security incident handling. Integrating a medical device may often enable practical features of other network components towards a more efficient use of the existing functions of a connectable medical device. Integration has the potential to improve information security because it will allow the implementation of additional technical protection measures that have to be based on the specific integration environment. The integrator is contracted either by the manufacturer or the operator.
IT Security	The protection of computer systems from adverse effects on assets including hardware, software, or electronic data, as well as from disruption or misdirection of the services they provide. Key concepts involved in IT security specifically for medical devices are the following: - Confidentiality of information at rest and in transit (must be ensured dependent on the risk management) - Integrity, which is necessary to ensure information authenticity and accuracy (i.e., non-repudiation) - Availability of the processes, devices, data, and connected systems
Joint Responsibility	For the provision of secured healthcare services, it is important to recognise the roles and expectations of all stakeholders, such as manufacturers, suppliers, healthcare providers, patients, integrators, operators and regulators. Modification of a medical device, e.g., the installation or enabling of third-party software including software patching, should always be under explicit published guidance of the manufacturer. It is important to understand that any invalidated modification of a medical device or system (e.g., product firewall changes, software patches, security software, utilities, games, music files, other software programs, etc.) can adversely affect system performance or safety in unpredictable ways. For example, it may open doors for easy exploitation of identified vulnerabilities of the medical device.
Layered Defence in Depth Approach	A medical device should be designed in a layered defence in depth approach and therefore should not rely on security controls in the operating environment. Nevertheless, as part of this layered defence in depth approach, there are expectations on the intended operating environment

Funded by Horizon Europe Framework Programme of the European Union

Lifecycle Aspects	Addressing cybersecurity risks at the design stage can help mitigate cybersecurity risks that could contribute to a breach in the confidentiality, a compromise in the integrity and availability of the medical device and its data, or intentional unauthorised access to the medical device and/or the network. Compromised CIA might impact medical purposes as specified in the medical device definition in MDR Article 2. Other than for safety related hazards, whose number is quite stable over time, the security situation for software may change rapidly due to newly emerging security vulnerabilities, or due to new attack vectors. This may lead to the situation that a medical device is considered secure with respect to known vulnerabilities at a specific point in time. However, without any security maintenance that device may become unsecure and possibly unsafe as a consequence due to newly emerging vulnerabilities or due to novel attack methods.
Management of security-related issues (practice)	Processes specified by this practice are used for handling security-related issues of a product.
Minimum IT Requirements for the operating environment (incl. Security Requirements)	Annex I of the Medical Devices Regulations make explicit references to the environment hosting medical devices, highlighting the need for medical device manufacturers to set out the minimum relevant IT security requirements (17.4 MDR/16.4 IVDR) and communicate them effectively to the users (23.4ab MDR/20.4 ah IVDR). The manufacturer shall provide clear documentation of the device's instructions for use, including IT security features/configurations (if applicable), and clear instructions for the IT security controls related to the operating environment, including product specifications, compatibilities, recommended IT security measures, IT environment configuration (e.g. traffic control), etc. Due to frequent changes in the threat landscape, it might be advisable to maintain security information in an electronic form that allows for dynamic updates as needed. **For requirements, check "Basic Principles", "IT security requirements for the operating environment" in pp.20-22 of section 3.6 of MDCG 2019-16**

Funded by Horizon Europe Framework Programme of the European Union

Operating Environment	Operating environment for a medical device is defined as any IT/network asset interacting with the medical device that is not supplied by the medical device manufacturer. Devices operating in the intended use environment should consider that the IT infrastructure of the different healthcare providers has unique and different risk management approaches associated with their networks. Any minimum requirements concerning hardware, IT networks characteristics and IT security measures for the operating environment should be defined on the basis of the following principles: · Any proposed IT security requirement for the operating environment should be based on the risk assessment conducted for the medical device. · The medical device should be as autonomous as possible in terms of IT security and sole reliance on the existence of any IT security requirements on the operating environment should be kept to a minimum and reflect the manufacturer's assumptions on the baseline environment security for the secure operation of the medical device. · The manufacturer's assumptions regarding the IT security of the operating environment shall be clearly documented in the instructions for use and may refer to best practice security standards. · In accordance with the principle of layered security, IT security measures foreseen for the operating environment in general should not serve the purpose of compensating security controls for medical device vulnerabilities, unless there is sufficient justification. In cases where the medical device relies on the operating environment to provide important IT security controls, this should be stated in the accompanying technical documentation.
Operation Security Domain	Protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers, or users
Operator	The operator should follow the manufacturers' published requirements and guidelines regarding security for commissioning, operating and de-commissioning of medical devices. The operator is responsible for the procurement and should ensure that security is maintained during the operation and application of the system (medical device), and particularly not compromised by changes in the environment of by user interaction. • Ensure required level of security for operational environment (network, physical, …); • Provide required infrastructure (network, physical); • Ensure that personnel are properly trained and available in case of security issues;

Funded by Horizon Europe Framework Programme of the European Union

	• Ensure that system is used as proscribed by manufacturer guidelines (e.g., no physical access by unauthorized users, password policies kept, network security measures); • Ensure that prescribed maintenance is done as required, including installation of security patches; • Notify the manufacturer without delay of any suspected security event.
Patients and Consumers	Patients and consumers are encouraged to employ cyber smart behaviour, such as paying attention to privacy, being aware of suspicious messaging, and browsing responsibly. Instruction for Use should include the necessary information so that patients and consumers can be up to date with the latest version of software, protect the device throughout its lifespan, use sufficiently complex passwords, turn off features that are not used, secure the computer or tablet devices, use backups and protection of their healthcare data. This includes ensuring that connected devices, such as computers and mobile devices comply with the operating instructions provided with the medical device.
Penetration testing	Penetration testing is the assessment of the security of a system against different types of attacks performed by an authorised security expert. The tester attempts to identify and exploit the system's vulnerabilities.
Post-market Surveillance System (PMS)	Cybersecurity considerations for medical devices should be part of this PMS system. A PMS system includes actively and regularly collecting user experience from devices on the market (including third party software and hardware components), to review these, and to timely implement necessary corrective action, taking into account the nature and risks in relation to the device. The manufacturer will involve the distributors of the device and, where applicable, the authorised representative and importers of the device in his system, in order to obtain the relevant information from the market. This system will be part of QMS and be supported by the manufacturer's PMS plan (MDR Art.84, IVDR Art.79), which must address a range of information (Medical Devices Regulations Annex III). See definitions of 'Incident' and 'Serious Incident' in next tab. See examples on the distinction between incidents and serious incidents from the point of view of cybersecurity in Annex II of MDCG 2019-16. Data gathered from PMS system must be used to actively update: - the clinical evaluation; - the benefit-risk determination and to improve the risk management; - the design and manufacturing information, the instructions for use and the labelling;

Funded by Horizon Europe Framework Programme of the European Union

	Handling and remediation of cybersecurity incidents and vulnerabilities reported through the post-market surveillance and vigilance systems shall be carried out conforming to the methodologies described in Chapter 3.2 of MDCG 2019-16, with regards to: - Assess the need for reporting serious and non-serious incidents and of carrying-out field safety corrective actions; - Enhancing security capabilities; - Update the original Security Risk Assessment; - Update the Verification and Validation; - Update the original Security Benefit Risk Analysis - Update the Technical Documentation.
Product Risk Analysis for Safety. Safety Risk Assessment.	Security vulnerabilities may affect the product's safety or effectiveness. A product risk analysis for safety should therefore consider the effects of security vulnerabilities to the essential functioning of the product.
Product Security Risk Management Process	During the product security risk management process, the manufacturers need to distinguish two important areas: 1. Safety risk management normally covered in the overall product risk management, and 2. Security risk, which is not associated to safety.
Risk	The combination of the probability of occurrence of harm and the severity of that harm
Safety and Effectiveness	Devices shall achieve the performance intended by their manufacturer and shall be designed and manufactured in such a way that, during normal conditions of use, they are suitable for their intended purpose. They shall be **safe and effective** and shall not compromise the clinical condition or the safety of patients, or the safety and health of users or, where applicable, other persons, provided that any risks which may be associated with their use constitute acceptable risks when weighed against the benefits to the patient and are compatible with a high level of protection of health and safety, taking into account the generally acknowledged state of the art.
Safety and Security	Overall, Annex I section 1 of the Medical Devices Regulations requests that any risks associated with the operation of medical devices must be acceptable so as to enable a high level of protection of health and safety. This can be only achieved through the establishment of an adequate balance between benefit and risk during all possible operation modes of a medical device. To this

Funded by Horizon Europe Framework Programme of the European Union

	end, there is a need to consider the relationship between "safety and security" as they relate to risk.
Secure by Design (practice)	The processes specified by this practice are used to ensure that the product is secure by design including defence in depth.
Secure implementation (practice)	The processes specified by this practice are used to ensure that the product features are implemented securely.
Security update management (practice)	Processes specified by this practice are used to ensure that security updates and security patches associated with the product are tested for regressions and made available to product users in a timely manner.
Security Benefit Risk Analysis	An overall Benefit Risk Analysis is to be executed based on the intended use and possible safety and performance impact using the safety risk assessment, which includes the security-related hazard categories. Risk acceptance criteria should be established by the manufacturer and documented to guide the appropriate measures for mitigating security risks. Those criteria relate to the intended purpose and operational environment.
Security Capabilities / Risk Control Measures	The list of known vulnerabilities and attack vectors is the basis for specifying the security capabilities, depending on the risk management, required for appropriate protection of confidentiality, integrity, availability of data, function and services of the medical device along with the specified product security context. Where there is an impact on safety or effectiveness, manufacturers shall select the most appropriate risk control solution, in the following order of priority: a) Eliminate or reduce risks as far as possible through safe design and manufacture; b) Where appropriate, take adequate protection measures, including alarms, if necessary, in relation to risks that cannot be eliminated; c) Provide information for safety (warnings/precautions/contra-indications) and, where appropriate, training to users.
Security guidelines (practice)	Processes specified by this practice are used to provide and maintain user documentation that describes how to integrate, configure, and maintain the defence in depth strategy of the product in accordance with its product security context.
Security Issues - Restrictive Security	The use of too restrictive security measures that provide a high level of protection may have a safety impact, especially if the security functionalities are not well designed.

Funded by Horizon Europe Framework Programme of the European Union

Security Issues - Weak Security	For example, weak access control may allow malicious modification of the operation of an implanted cardiac device.
Security Management (Practice)	The purpose of the security management practice is to ensure that the security-related activities are adequately planned, documented and executed throughout the product's lifecycle.
Security Risk Assessment/Threat Modelling Techniques	When choosing such security capabilities as protection measures, the manufacturer should consider the device's intended clinical use and intended operational environment when determining the appropriate balance of safety, effectiveness and security. The likelihood of identified security scenarios can be supported through structured scoring systems, e.g., Common Vulnerability Scoring Systems - CVSS (https://www.first.org/cvss/), which may also consider the attacker's gain in relation to the required effort. A scenario whereby an attacker exploits a known vulnerability (identified via a Common Vulnerabilities and Exposures -CVE-identifier) may be considered as "foreseeable" with respect to the product's risk management – notably if the intended operational environment or other mitigation controls do not prevent that type of attack.
Security Risk Management	The discipline of identifying and measuring risks towards safety and effectiveness resulting from the intended use and foreseeable misuse of a medical device and reducing them "as far as possible" to an acceptable level. Specific methods and requirements are used for security risks.
Security Risk Management Plan	The security risk management process has the same elements as safety risk management process, all documented in a security risk management plan. The process elements are security risk analysis, security risk evaluation, security risk control, evaluation of residual security risk and reporting.
Security verification and validation testing (practice)	Processes specified by this practice are used to document the security testing required to ensure that all the security requirements have been met for the product and that security of the product is maintained when the product is used as intended.
Specification of security requirements (practice)	Processes specified by this practice are used to identify the security capabilities that are required for appropriate protection of confidentiality, integrity and availability of data, function and services of the medical device along with the specified product security context. These security requirements can be defined at the product-level, or they may supplement product-level requirements.
Verification / Validation	The primary means of security verification and validation is testing. Methods can include security feature testing, fuzz testing, vulnerability scanning and penetration testing. Additional security testing can be done by using tools for secure code analysis and

Funded by Horizon Europe Framework Programme of the European Union

	tools that scan for open-source code and libraries used in the product, to identify components with known issues.
Vigilance	The manufacturer is responsible for reporting all serious incidents and field safety corrective actions (FSCA) to the CA in accordance with MDR Article 87 or IVDR art 82. Manufacturers are obliged to conduct investigations as soon as they are informed that a serious incident has taken place. As such, a risk assessment of the incident is conducted and if needed, a FSCA will be implemented in order to minimize the risk of the device. The manufacturer will involve the distributors of the device and, where applicable, the authorised representative and importers in the system, in order to obtain the information needed from the market, especially for FSCA or issued field safety notices (FSN) so that to ensure required actions are followed and completed in a timely manner. The manufacturers shall carry out investigations of serious incidents related to a cybersecurity incident in order to provide a comprehensive description of the serious incident, including: a) a description of the serious incident including any relevant information that might impact the understanding or evaluation of the serious incident, i.e., information is compromised or information is threatened; b) a description of the health effects (if applicable), i.e. clinical signs, symptoms, conditions as well as the overall health impact. The reporting tools that are made available to manufacturer enable the use of IMDRF codes to index: - the device problem of the incident; - the related health impact; - cybersecurity related incident root causes; Regarding medical device problems due to cybersecurity related incident root causes, the IMDRF codes available to date include code A110502 (IMDRF Annex A), which is representative for a Computer System Security Problem. This code is further sub-divided into 2 more specific codes on "Application Security Problem" and "Unauthorized Access to Computer System" (see Table 4). Regarding the cybersecurity related incident root causes of medical device problems, the IMDRF codes available to date include code C1007 (IMDRF Annex C) which refers to "Software Security Vulnerability" (see Table 5). In cases where the currently available IMDRF coding system does not provide sufficient level of detail to indicate the cybersecurity causal root of an incident, the manufacturer is requested to propose a new code to be adopted by the IMDRF coding system, in accordance with the relevant procedure for new term request.

Funded by Horizon Europe Framework Programme of the European Union

Vigilance - Trend Reporting	Incidents that have cybersecurity related incident root causes are subject to Trend Reporting under the Medical Devices Regulations. According to trend reporting provisions, manufacturers shall report, by means of the electronic system referred to in Article 92 (IVDR Art. 95), any statistically significant increase in the frequency or severity of incidents that are not serious incidents or that are expected undesirable side-effects that could have a significant impact on the benefit-risk analysis referred to in Sections 1 and 8 of Annex I and which have led or may lead to risks to the health or safety of patients, users or other persons that are unacceptable when weighed against the intended benefits. Within the Trend Report, key obligations of the manufacturers are to specify: - the methodology used for determining any statistically significant increase in the frequency or severity; - how to manage the incidents; - the observation period. Using IMDRF codes to index the cybersecurity medical root causes related to non-serious incidents is desirable and may be implemented into the Trend Report. Use of IMDRF codes is desirable also in the context of periodic post-market surveillance reports and periodic safety update reports as referred to in Articles 85 and 86 of the MDR.

Table 8 : Glossary on current regulation concerning cybersecurity of connected devices

Glossary MDR-IVDR

Term	Definition/Meaning
'CE marking of conformity' or 'CE marking'	A marking by which a manufacturer indicates that a device is in conformity with the applicable requirements set out in this Regulation and other applicable Union harmonisation legislation providing for its affixing.
Accessory for a medical device	An article which, whilst not being itself a medical device, is intended by its manufacturer to be used together with one or several particular medical device(s) to specifically enable the medical device(s) to be used in accordance with its/their intended purpose(s) or to specifically and directly assist the medical functionality of the medical device(s) in terms of its/their intended purpose(s)
Active Device	Any device, the operation of which depends on a source of energy other than that generated by the human body for that purpose, or by gravity, and which acts by changing the density of or converting that energy. Devices intended to transmit energy, substances or other

Funded by Horizon Europe Framework Programme of the European Union

	elements between an active device and the patient, without any significant change, shall not be deemed to be active devices. Software shall also be deemed to be an active device
Adverse event	Any untoward medical occurrence, unintended disease or injury or any untoward clinical signs, including an abnormal laboratory finding, in subjects, users or other persons, in the context of a clinical investigation, whether or not related to the investigational device.
Authorised representative	Any natural or legal person established within the Union who has received and accepted a written mandate from a manufacturer, located outside the Union, to act on the manufacturer's behalf in relation to specified tasks with regard to the latter's obligations under this Regulation.
Benefit-risk determination	The analysis of all assessments of benefit and risk of possible relevance for the use of the device for the intended purpose, when used in accordance with the intended purpose given by the manufacturer
Clinical benefit	The positive impact of a device on the health of an individual, expressed in terms of a meaningful, measurable, patient-relevant clinical outcome(s), including outcome(s) related to diagnosis, or a positive impact on patient management or public health.
Clinical data	Information concerning safety or performance that is generated from the use of a device and is sourced from the following: — clinical investigation(s) of the device concerned, — clinical investigation(s) or other studies reported in scientific literature, of a device for which equivalence to the device in question can be demonstrated, — reports published in peer reviewed scientific literature on other clinical experience of either the device in question or a device for which equivalence to the device in question can be demonstrated, — clinically relevant information coming from post-market surveillance, in particular the post-market clinical follow-up;
Clinical evaluation	A systematic and planned process to continuously generate, collect, analyse and assess the clinical data pertaining to a device in order to verify the safety and performance, including clinical benefits, of the device when used as intended by the manufacturer.
Clinical evidence	Clinical data and clinical evaluation results pertaining to a device of a sufficient amount and quality to allow a qualified assessment of whether the device is safe and achieves the intended clinical benefit(s), when used as intended by the manufacturer.

Funded by Horizon Europe Framework Programme of the European Union

Clinical investigation	Any systematic investigation involving one or more human subjects, undertaken to assess the safety or performance of a device
Clinical investigation plan	A document that describes the rationale, objectives, design, methodology, monitoring, statistical considerations, organisation and conduct of a clinical investigation
Clinical performance	The ability of a device, resulting from any direct or indirect medical effects which stem from its technical or functional characteristics, including diagnostic characteristics, to achieve its intended purpose as claimed by the manufacturer, thereby leading to a clinical benefit for patients, when used as intended by the manufacturer.
Common Specifications (CS)	A set of technical and/or clinical requirements, other than a standard, that provides a means of complying with the legal obligations applicable to a device, process or system.
Compatibility	The ability of a device, including software, when used together with one or more other devices in accordance with its intended purpose, to: (a) perform without losing or compromising the ability to perform as intended, and/or (b) integrate and/or operate without the need for modification or adaption of any part of the combined devices, and/or (c) be used together without conflict/interference or adverse reaction.
Conformity assessment body	A body that performs third-party conformity assessment activities including calibration, testing, certification and inspection
Conformity assessment	Process demonstrating whether the requirements of this Regulation relating to a device have been fulfilled.
Corrective action	Action taken to eliminate the cause of a potential or actual non-conformity or another undesirable situation.
Device deficiency	Any inadequacy in the identity, quality, durability, reliability, safety or performance of an investigational device, including malfunction, use errors or inadequacy in information supplied by the manufacturer.
Distributor	Any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a device available on the market, up until the point of putting into service.
Economic operator	A manufacturer, an authorised representative, an importer, a distributor or the person referred to in Article 22(1) and 22(3).

Funded by Horizon Europe Framework Programme of the European Union

Ethics committee	An independent body established in a Member State in accordance with the law of that Member State and empowered to give opinions for the purposes of this Regulation, taking into account the views of laypersons, in particular patients or patients' organisations.
Field safety corrective action (FSCA)	Corrective action taken by a manufacturer for technical or medical reasons to prevent or reduce the risk of a serious incident in relation to a device made available on the market.
Field safety notice	A communication sent by a manufacturer to users or customers in relation to a field safety corrective action.
Fully refurbishing	The complete rebuilding of a device already placed on the market or put into service, or the making of a new device from used devices, to bring it into conformity with this Regulation, combined with the assignment of a new lifetime to the refurbished device.
Harmonised standard	A European standard as defined in point (1)(c) of Article 2 of Regulation (EU) No 1025/2012
Health institution	An organisation the primary purpose of which is the care or treatment of patients or the promotion of public health.
Importer	Any natural or legal person established within the Union that places a device from a third country on the Union market
Incident	Any malfunction or deterioration in the characteristics or performance of a device made available on the market, including use-error due to ergonomic features, as well as any inadequacy in the information supplied by the manufacturer and any undesirable side-effect.
Informed consent	A subject's free and voluntary expression of his or her willingness to participate in a particular clinical investigation, after having been informed of all aspects of the clinical investigation that are relevant to the subject's decision to participate or, in the case of minors and of incapacitated subjects, an authorisation or agreement from their legally designated representative to include them in the clinical investigation.
Instructions for use	Information provided by the manufacturer to inform the user of a device's intended purpose and proper use and of any precautions to be taken
Intended purpose	The use for which a device is intended according to the data supplied by the manufacturer on the label, in the instructions for use or in promotional or sales materials or statements and as specified by the manufacturer in the clinical evaluation.

Funded by Horizon Europe Framework Programme of the European Union

Interoperability	The ability of two or more devices, including software, from the same manufacturer or from different manufacturers, to: (a) exchange information and use the information that has been exchanged for the correct execution of a specified function without changing the content of the data, and/or (b) communicate with each other, and/or (c) work together as intended.
Investigational device	A device that is assessed in a clinical investigation.
Investigator	An individual responsible for the conduct of a clinical investigation at a clinical investigation site
IT Security Measures	IT security measures may refer to any applicable technical and/or organisational measures for managing IT security risks related to the operating environment
Lay person	An individual who does not have formal education in a relevant field of healthcare or medical discipline
Making available on the market	Any supply of a device, other than an investigational device, for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge
Manufacturer	Means a natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured or fully refurbished, and markets that device under its name or trademark.
Market surveillance	Activities carried out and measures taken by competent authorities to check and ensure that devices comply with the requirements set out in the relevant Union harmonisation legislation and do not endanger health, safety or any other aspect of public interest protection.
Medical Device	Any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: — diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability, — investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,

Funded by Horizon Europe Framework Programme of the European Union

	— providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.
Notified body	A conformity assessment body designated in accordance with this Regulation
Overall Residual Risk	**Evaluate all risks together against medical benefits** (expert judgment, define method and criteria in risk management plan, disclose residual risk)
Performance	The ability of a device to achieve its intended purpose as stated by the manufacturer
Placing on the market	The first making available of a device, other than an investigational device, on the Union market
Post-market surveillance	All activities carried out by manufacturers in cooperation with other economic operators to institute and keep up to date a systematic procedure to proactively collect and review experience gained from devices they place on the market, make available on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions.
Post-market surveillance and vigilance	**Post-market activities**: collect information; review information on relevance for safety; take action where needed
Putting into service	The stage at which a device, other than an investigational device, has been made available to the final user as being ready for use on the Union market for the first time for its intended purpose.
Recall	Any measure aimed at achieving the return of a device that has already been made available to the end user
Reprocessing	A process carried out on a used device in order to allow its safe reuse including cleaning, disinfection, sterilisation and related procedures, as well as testing and restoring the technical and functional safety of the used device.
Risk	The combination of the probability of occurrence of harm and the severity of that harm
Risk Assessment	Describe **intended use**, reasonably **foreseeable misuse**, **characteristics related to safety**; Identify all **hazards** and hazardous

Funded by Horizon Europe Framework Programme of the European Union

	situations; Estimate **severity and probability of risk**; **Evaluate risks against criteria**
Risk Control	Reduce risks: inherent safe design; protective measures; apply state of the art, information for safety; Training. Check for completeness. Benefit-risk balance, definition of "benefit"
Risk Management Plan	All activities must be planned. **Plan must include**: Description of medical device; Authorities and responsibilities; **Criteria for risk acceptability** based on regulations & international standards; Requirements for review
Risk Management Review	**Review before product release**: review of activities so far; ensure overall residual risk is acceptable; ensure methods to collect (post-)production information are in place
Serious adverse event	Any adverse event that led to any of the following: (a) death, (b) serious deterioration in the health of the subject, that resulted in any of the following: (i) life-threatening illness or injury, (ii) permanent impairment of a body structure or a body function, (iii) hospitalisation or prolongation of patient hospitalisation, (iv) medical or surgical intervention to prevent life-threatening illness or injury or permanent impairment to a body structure or a body function, (v) chronic disease, (c) foetal distress, foetal death or a congenital physical or mental impairment or birth defect;
Serious incident	Any incident that directly or indirectly led, might have led or might lead to any of the following: (a) the death of a patient, user or other person, (b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health, (c) a serious public health threat;
Serious public health threat	An event which could result in imminent risk of death, serious deterioration in a person's state of health, or serious illness, that may require prompt remedial action, and that may cause significant morbidity or mortality in humans, or that is unusual or unexpected for the given place and time.

Funded by Horizon Europe Framework Programme of the European Union

Sponsor	Any individual, company, institution or organisation which takes responsibility for the initiation, for the management and setting up of the financing of the clinical investigation.
Subject	An individual who participates in a clinical investigation
System	A combination of products, either packaged together or not, which are intended to be interconnected or combined to achieve a specific medical purpose
Unique Device Identifier ('UDI')	A series of numeric or alphanumeric characters that is created through internationally accepted device identification and coding standards and that allows unambiguous identification of specific devices on the market
User	Any healthcare professional or lay person who uses a device
Withdrawal	Any measure aimed at preventing a device in the supply chain from being further made available on the market

Table 9 : Glossary on MDR-IVDR

Funded by Horizon Europe Framework Programme of the European Union