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

CYLCOMED

Cyber-security toolbox
for connected medical devices

D1.3 Updated Data Management Plan

Revision: v.2.0

Work package	WP 1
Task	T1.5
Due date	30/11/2025
Submission date	30/11/2025
Deliverable lead	MediaClinics Italia
Version	2.0
Authors	Andrea Scaburri (MCI), Simone Favrin (MCI), Dusko Milojevic (KUL)
Reviewers	Juan Carlos Perez Baun (Eviden) Esteban Alejandro Armas Vega (Eviden)

Abstract	Data Management Plan for CYLCOMED project. This document presents the data management approach followed, guidelines to collect the data and the data collection itself. This version includes the final forms from the whole consortium.
Keywords	Data Management Plan, Cybersecurity, Medical Devices

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V 0.0	23/05/2023	First issue	MCI
V 0.1	29/05/2023	Formatting, executive summary and sec. 2.3 updated	MCI, KUL
V 1.0	31/05/2023	Reviewers' comments and suggestions incorporated	CUB, KUL, MCI
V 1.1	28/08/2024	Intermediate review	MCI
V 1.2	2/12/2025	Issue of final version	MCI
V 1.3	3/12/2025	Added content	KUL
V 1.4	4/12/2025	Final review	EVIDEN
V 2.0	8/12/2025	Implementation of comments and suggestions	MCI, KUL

Disclaimer

The information, documentation and figures available in this deliverable are written by the "CYber security tooLbox for COnnected MEdical Devices" (CYLCOMED) project's consortium under EC grant agreement 101095542 and do not necessarily reflect the views of the European Commission.

Funded by Horizon Europe Framework Programme of the European Union

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	DMP	
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.

Acknowledgments

This document contains the forms and the contribution provided by the partners of the whole CYLCOMED consortium.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary: Data Management Plan

This document represents the final iteration of the Data Management Plan (DMP) for the CYLCOMED project. It groups all the relevant information regarding the data that was used, generated, and managed during the project's lifecycle, concluding at Month 36.

Due to the complex nature of the CYLCOMED project, which involved hospitals and clinical experts alongside cybersecurity and technology companies, the DMP provided crucial common understanding and guidance on data classification, ethical implications, dissemination, and the application of FAIR principles.

The DMP was structured to collect and report information on distinct **data sets** (groups of data with common characteristics, origin, and management requirements). This approach ensured that the diversity of data—from highly sensitive clinical parameters to technical security logs—was categorized in a readable and accessible way.

The core of the document consists of tailored forms detailing:

- Pilot 1 (ICU Equipment): Management of Synthetic Clinical Data and technical logs used to validate the security toolbox in a controlled environment.
- Pilot 2 (Tele monitoring): Management of Pseudonymised Patient Data from paediatric patients, along with the technical logs generated during the real-world validation of the tele monitoring platform, volunteers and technical data to provide integration and feedback to technical partners.
- CYLCOMED Toolbox: Documentation of the Technical Data (logs, alerts, policies) generated by the core security components (e.g., FE4MED, LADS, LuS4MED).

Key Project Outcomes and Compliance

The real-world and simulated pilots served as the focal point for all data generation and usage. The final review confirms that the project successfully delivered a robust framework based on two critical pillars:

- **Ethics and GDPR Compliance:** Data collection in Pilot 2 was fully sanctioned by Ethics Committee Approval. The project implemented a rigorous "Privacy by Design" strategy, involving Data Protection Officers (DPOs) to ensure that all data, especially sensitive patient data, was managed in full compliance with the General Data Protection Regulation (GDPR).
- **FAIR Data Implementation:** The project ensured that all technical outputs and methodologies are Findable, Accessible, Interoperable, and Reusable when possible. While sensitive pseudonymised patient data remains strictly Closed Access to protect privacy, the CYLCOMED Toolbox code, security methodologies, and technical validation logs are the key reusable assets, documented using standards like JSON, Syslog, and OpenAPI to maximize their value for future research and exploitation.

This document serves as the final declaration of the project's commitment to secure and responsible data management, reporting on the execution and final disposition of all project data.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

AI	Artificial Intelligence
ARDS	Acute respiratory distress syndrome
CET	Territorial Ethical Committee
CFREU	The Charter of Fundamental Rights of the European Union
CHD	Congenital Heart Disease
CMD	Connected Medical Device
CP-ABE	Cyphertext-Policy Attribute-Based Encryption
CTI	Cyber Threat Intelligence
CTQT	Clinical Trial Quality Team
CUB	Charité – Universitätsmedizin Berlin
CV	Cardiovascular
CYLCOMED	CYbersecurity tooLbox for COnnected MEdical Devices
D#.#	Deliverable (referred to CYLCOMED proposal)
DMP	Data Management Plan
DPO	Data Protection Office
ECG	Electrocardiogram
ECHR	Convention on Human Rights
eCRF	Electronic Case Report Form
ECtHR	European Court of Human Rights
EHR	Electronic Health Records
ENS	Spain Esquema Nacional de Seguridad
EU	European Union
EVIDEN	Formerly Atos
FE4MED	Functional Encryption for Medical Data
FHUNJ	Fundación para la Investigación Biomédica Hospital Infantil Universitario Niño Jesús
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation
H2020	Horizon Europe 2020 (projects)
HIS	Hospital Information System
ICU	Intensive Care Unit
INOV	Inov - Instituto De Engenharia De Sistemas E Computadores, Inovação

Funded by Horizon Europe Framework Programme of the European Union

IoMT	Internet of Medical Things
IT	Information technology
KUL	Katholieke Universiteit Leuven
LADS	Live Anomaly Detection System
LOMOS	LOg MOnitoring System
LOPDGDD	Organic Law on Protection of Personal Data and Guarantee
LuS4MED	Ledger uSelf for Medical Data
M#	Month of the project
MCI	MediaClinics Italia
MDR	Medical Devices Regulation
MHP	Mediaclinics Health Platform
NMT	NeuroMuscular Transmission
OPA	Open Policy Agent
OPBG	Ospedale Pediatrico Bambino Gesù
OTA	Over The Air
RGB	RGB Medical Devices
RMSE	Root Mean Sqare Error
RPI	Rasberry PI
SaMD	Software as Medical Device
SSI	Synchronous Serial Interface
SSO	Single Sign-On
VC	Verifiable Credential
WP	Work Package
XLAB	XLAB Razvoj Programske Opreme in Svetovanje

Funded by Horizon Europe Framework Programme of the European Union

1 Introduction

This is the final issue of the Data Management Plan section reports the CYLCOMED project essentials, the pilots and the CYLCOMED toolbox.

1.1 Purpose of the Document

This document constitutes the final version of the Data Management Plan (DMP) for the CYLCOMED project (Deliverable D1.3), submitted at Month 36. It updates and supersedes the preliminary DMP (D1.2) issued at Month 6. This report provides a comprehensive overview of how data was generated, collected, processed, and preserved throughout the project's lifecycle, which concluded on November 30, 2025.

In adherence to the Horizon 2020 Open Research Data Pilot (ORDP) and FAIR principles (Findable, Accessible, Interoperable, and Reusable), this document details the final datasets resulting from the two validation pilots, as well as the technical outputs (CYLCOMED Toolbox) and dissemination materials. It serves as a definitive record of the project's data governance strategy, ethical compliance, and long-term preservation standards.

1.2 Project Summary

CYLCOMED strengthened the cybersecurity of Connected Medical Devices (CMDs), in vitro diagnostic devices (IVDs), and Software as Medical Device (SaMD). Addressing the critical infrastructure of the health sector, the project delivered technologically sovereign cybersecurity methodologies, validated through real-world implementation.

The project executed two distinct pilots:

- **Pilot 1 (ICU Environment):** Focused on Neuromuscular transmission (NMT) data in a simulated ICU environment, utilizing Digital Twin technology to validate security without risking patient safety.
- **Pilot 2 (Telemedicine):** Validated the secure remote collection of health parameters (e.g., ECG, blood pressure) from paediatric cardiac patients.

This DMP details the specific data flows, privacy measures (including GDPR compliance and DPO oversight), and the final storage locations for the datasets generated by these pilots.

1.3 Pilots generated data description

This section provides a description of the data life cycle starting from an overview of the data journey and the trials in which data are generated.

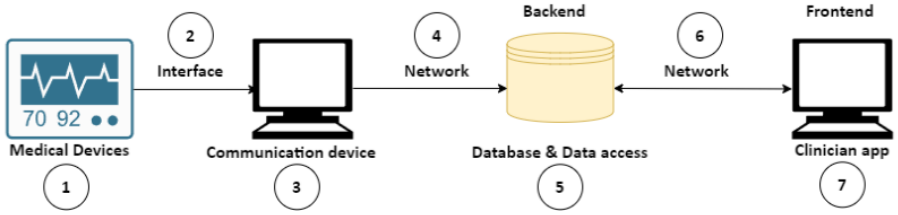

Figure 1: Data journey: general scheme of data generation and transmission (from D3.1 Baseline analysis, requirements and specifications)

Funded by Horizon Europe Framework Programme of the European Union

Data acquired by the CMDs are transmitted through a communication device and then stored in the backend of the used solution (Figure 1), where they can be analysed. Each step of the data journey can follow different specifications depending on the specific scenario.

Generated data can be classified in different categories, due to the nature of CYCLOMED project, particular attention should be paid to patient related data which are normally sensitive data and require additional care compared to technical data.

For the CYLCOMED project, patient related data include, but are not limited to, personal registry, and health-related parameters such as respiratory rate, blood pressure, heart rate, body temperature, Neuromuscular transmission (NMT) data, and blood glucose level.

The non-patient related data that are generated by the CMDs and that were be recorded (e.g., systems logs) are usually not needed to implement security measures (related to privacy and security threats, confidentiality, integrity, and availability of data). The origin of this data can vary: some technical data relate to the integration of the various medical devices and software used in the pilots; some data are related to hardware and software used during the pilot solutions.

1.3.1 Pilot no. 1 - Cyber Security in Hospital Equipment for COVID-19 ICU patients

The first pilot focuses on monitoring and controlling the neuromuscular transmission of COVID-19 ICU (Intensive Care Units) patients using NMTCuff technology and the Vision Air multi-parametric monitor with the CYLCOMED security components.

The data is used to establish the correct drug dosage infusion for each patient, which can vary based on several factors. This pilot was conducted on a simulated patient, without any real patient involvement. The patient simulation using a computerized model allows for testing and development of the platform before being implemented in real-life situations. The security features developed within CYLCOMED to ensure confidentiality, integrity, availability, and interplay with device safety.

Data used:

- Synthetic Patient data including medical history, diagnosis, and NMT (Neuromuscular Transmitter) status
- NMT monitoring data
- Dosage and infusion data

Steps where data is used:

- Monitoring of NMT to establish the correct dosage infusion
- Control of dosage infusion to maintain patient within NMT target limits
- NMT control by Target Control Infusion using NMTCuff technology
- Patient simulation using a computerized model for a digital twin approach

Hardware in Loop/Software in Loop interaction with the Vision Air Monitor and all CYLCOMED security components

Pilot no.1 - Final state

This pilot was developed exclusively as a laboratory project without real patient involvement. A patient simulator was used as a software component of the "Test bench Platform" to generate Synthetic Clinical Data. This setup allowed for the robust testing of the platform's security features, ensuring confidentiality, integrity, availability, and interplay with device safety, before implementation in real-life scenarios.

Funded by Horizon Europe Framework Programme of the European Union

Data Classification and Compliance: The data collected are classified as Synthetic Clinical Data (designed to mimic vital signs and patient history) and Technical Data (security logs, pump status). Since this pilot used simulated data and did not involve real patients, GDPR and the project's ethics requirements for sensitive patient data were not triggered at this stage. However, the data was treated as if it were real sensitive data (via encryption and access control) to validate the CYLCOMED toolbox's capabilities. The data collected includes:

Data Type	Description and Purpose
Synthetic Personal Data (Encrypted)	This data represents vital signs required for clinical functionality (NMT control review):
Vital Signs	Neuromuscular Transmission (NMT), Heart Rate (HR), Oxygen Saturation (SpO2), and Temperature.
Infused Drug Dose	Data on drug administration.
Patient History	Encrypted patient data including medical history and diagnosis (stored to confirm functional requirements).
Technical Data	This data is essential for security features and non-functional requirements
Infusion Pump Status	Status and alarms generated by the infusion pump.
Security Logs	Logs generated from CYLCOMED tools. This encompasses technical log data from tools like FE4MED (logs of encryption/decryption processes) and LuS4MED (logs of the authentication process).

The key vital signs collected are NMT and Dose Infusion values over time. For each simulated patient and day, the expected data size is approximately 300 measures of NMT control data and 5,700 measures of the other vital signs.

Data security is implemented through:

1. Encryption: The (fake) data from the pilot is encrypted by tools like FE4MED for protection when sent to the hospital system and when stored. This ensures protection in transit and at rest.

2. Access Control: Access to the data requires an authentication and authorisation process. Users accessing the hospital services and data must be authenticated via an SSI-based decentralized solution (LuS4MED) and authorized by the C-OPA tool.

Funded by Horizon Europe Framework Programme of the European Union

3. Monitoring: Technical logs generated by security components often adhere to the Syslog standard (RFC 5424). Other technical tools, such as LOMOS and LADS, collect network packets to detect anomalies.

1.3.2 Pilot no. 2 - Cybersecurity for Telemedicine Platforms

Pilot no. 2 focuses on the usage of telemedicine platforms to constantly monitor patients and answer specific medical needs. In this scenario it was used a CMDs (SaMD) to remotely collect health-related parameters from paediatric cardiac patients that are not on hospital premises.

In this pilot we used MediaClinics Health Platform a telemedicine platform (MHP) that collects health-related parameters from patients, including:

- ECG
- Blood pressure
- Heart rate
- Respiratory rate
- Body temperature
- Blood glucose

The security of the platform (already certified as a medical device) was enhanced through the integration of CYLCOMED tools.

In this scenario the data has to guarantee the following properties:

- Accurate and reliable to ensure correct patient monitoring and diagnosis
- Secure and private to protect patient confidentiality and prevent unauthorized access
- Accessible remotely to allow for tele monitoring

Pilot no.2 - Final state and Ethical Compliance

This pilot successfully validated the secure remote collection of health parameters from pediatric cardiac patients (Deployment A, OPBG) and performed tests with volunteers (Deployment A – FHUNJ). Additionally, simulated attacks in a secure VM (Deployment B) were performed.

Data Classification and Ethical/Legal Compliance: The data collected in Deployment A – OPBG (real-world) falls under Special Categories of Personal Data (Health Data) as defined by GDPR Article 9.

- Compliance: All data processing was performed in full compliance with the ethical and legal requirements detailed in Deliverables D2.2 and D2.3 ("Examination of Ethical, Legal and Data Protection Requirements" and "Ethical and Legal Evaluation and Recommendations Report").
- Legal Basis: The processing of data from patients was based on informed consent (GDPR Article 6(1)(a)) obtained by the clinical partner.
- Final Status: All identifiable patient data was pseudonymized immediately upon collection within the secure clinical environment. The Pseudonymized datasets used for the final validation and analysis are stored on the clinical partner's secure server, which is certified for health data storage.

The Volunteer Activity (Deployment A – FHUNJ) was a technical usability trial.

The data collected in Deployment B (simulated) is classified as Technical Data (logs, attack patterns) and does not contain personal or sensitive information.

Funded by Horizon Europe Framework Programme of the European Union

Open Access Statement: Due to the sensitive nature of the underlying data, the raw pseudonymized patient-level data was not made publicly available (In accordance with GDPR, Article 9). However, description of dataset, security performance metrics, and high-level clinical workflow results are available in the relevant Deliverables (D5.3, D6.3).

1.4 CYLCOMED toolbox and dissemination

Due to the nature of the CYLCOMED project, not only the data itself but also other research outputs (such as the tools that are expected from the project and the dissemination itself) should be collected and managed.

1.4.1 CYLCOMED toolbox - package and methodologies

The main output of the CYLCOMED project is the toolbox itself (deliverables D5.1, D5.2 and D5.3) and the risk evaluation methodologies (D4.1, D4.2, D4.3). The data relevant to these outputs is reported in the dedicated forms of this document.

1.4.2 Dissemination and exploitation

Dissemination is a crucial task for H2020 projects and in CYLCOMED a complete work package is devoted to this purpose.

All the deliverables of this WP are strictly related to the DMP essence and the FAIR principles. The main document that shall be considered is D7.1 “Dissemination, Communication, Standardization and Exploitation Strategy and Plan” where information about research outputs (papers, conferences) are reported.

Funded by Horizon Europe Framework Programme of the European Union

2 Data management forms

This section presents an overview of the structure of the data information forms that are collected in this document. The forms are based on the European Commission guidelines for Data Management Plans and comprise three distinct parts:

- Data Summary: General information regarding the dataset's purpose, origin, and classification.
- FAIR Section: Details on how the data was made Findable, Accessible, Interoperable, and Reusable.
- Ethics and Security: Summarizes the ethical compliance, data protection, and security measures implemented.

2.1 Data summary

The standard DMP structure foresees only a common section for the data summary, but due to the different aspects that are involved in CYLCOMED, this section was replicated for each data set that has been identified.

This section is meant to summarize general aspects of the data, and in the CYLCOMED framework it is used to describe more in detail the specific dataset, focusing on the origin of the data and the different purpose of collecting these.

The following key questions **have been answered** for each dataset:

- What data was collected? (Dataset Name)
- With respect to GDPR, how was this dataset classified? (Public, Confidential, Sensitive, or Personal Data)
- Why was it collected? (Purpose and relation to project objectives)
- Which was the final quantity of data collected?
- Which was the source of the data? (Generated, or re-used from another source)

Funded by Horizon Europe Framework Programme of the European Union

2.2 FAIR data Principles in CYLCOMED

FAIR data refers to data that is Findable, Accessible, Interoperable, and Reusable. The following section outlines these principles to enable a common description of the data generated in CYLCOMED.

2.2.1 Findable

In order to make data available for further studies, the first requirements is to allow the possibility to search for it and this can be achieved granting some key aspects:

- **Data comes with identifiers**: Whenever relevant, to make the data findable a unique identifier was assigned to each acquired entry of the dataset, such identifier must be unique and immutable.
- **Data is searchable**: Metadata for each dataset entry was generated following platform-specific conventions and stored in a standard machine-readable format (e.g., JSON) to facilitate automated discovery and access to the technical data and metadata.

2.2.2 Accessible

Indications on how and under which circumstances access was granted are provided for each dataset:

- **Data is accessible and protected:** Accessibility was determined by the type of data considered. Access to sensitive Pseudonymised patient data was strictly limited to authorized healthcare personnel within the secure hospital network. A strong authentication process (possibly involving multi-factor authentication) and Role-Based Access Control (RBAC) mechanisms, validated by the CYLCOMED toolbox (LuS4MED, C-OPA), were implemented to ensure only authorized users had access. The consortium complied with all applicable data protection regulations (GDPR).
- **The authorization process is documented:** If the data is accessible behind authorization, the process to grant access to the dataset was properly documented by each interested partner, and the documentation must be available to those who may need access.

2.2.3 Interoperable

To ensure data interoperability:

- **Standard file formats** were used when possible.
- **Standard terminologies** were used to ensure the data is easily understood and interpreted by researchers in the same application domain.

2.2.4 Reusable

For health-related data, given their sensitive nature, data was made publicly available for reuse. In addition, data were provided in a machine-readable format to enable easy integration with other tools and platforms.

Nevertheless, whenever a data can be reused, it shall be ensured that:

Funded by Horizon Europe Framework Programme of the European Union

- Data is well documented: All reusable datasets were well-documented and properly annotated (including information on data collection procedures and quality control) to enable others to understand and reuse the data in their own research.
- The data format is well defined: The reusable data is available in a machine-readable format to enable easy integration. Data access and sharing guidelines were provided to ensure ethical and responsible use.

2.3 Data security and Ethics

2.3.1 Data security

Data security is one of the core topics for CYLCOMED, and therefore its implications are better described and analysed in the outcome of the project.

To ensure the security of the data, appropriate technical and organizational measures has been implemented to protect against unauthorized access, disclosure, or loss of the data.

We ensured that the data is always transmitted protected. Access to the data has been limited to authorized personnel only, and access control mechanisms was implemented to ensure that only individuals with the appropriate permissions can access the data. We also implemented a robust backup and disaster recovery procedures to ensure that the data is protected against accidental loss or destruction.

Finally, we comply with all applicable data protection regulations and guidelines, including the EU General Data Protection Regulation (GDPR) [3], to protect the privacy and confidentiality of patient data. All hospitals involved had DPOs engaged in project activities, to provide additional oversight for handling sensitive data. This includes ensuring that all personnel handling the data are trained in data protection and privacy best practices, and that appropriate safeguards are in place to protect against unauthorized access or disclosure of patient data.

The GDPR recognises the Data Protection Officer (DPO) as a central figure in the data governance framework and sets out specific conditions for their appointment, position, and tasks. The role of the DPO is critical in ensuring compliance with data protection laws and promoting a culture of data privacy within organisations.

All Hospitals participating in the CYLCOMED project have appointed DPOs, who were internally engaged. For instance, OPBG Hospital's DPO was continuously involved in various stages of the project implementation. These include, inter alia, monitoring the compliance of CYLCOMED's procedures with the current privacy policies, involvement in the preparation of the DPIA, and clinical protocol for the Territorial Ethical Committee. Moreover, the DPO validated the toolbox's GDPR alignment, particularly through pseudo-anonymization and access control logs.

Besides DPO, a DPIA is a critical tool for accountability, as it helps 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 the Regulation. A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing, and help manage the risks to the rights and freedoms of data subjects resulting from the processing of personal data.

A Data Protection Impact Assessment (DPIA) was carried out as part of the toolbox's integration into hospital settings and its validation within PILOT2. The DPIA process was

Funded by Horizon Europe Framework Programme of the European Union

initiated to assess the innovative features of the cybersecurity toolbox, ensuring compliance with data protection requirements while evaluating its practical deployment.

2.3.2 Ethics, legal and regulatory aspects

Ethics is regarded as the cornerstone of all projects funded by the European Commission. This can be illustrated through an EC statement which highlights that “ethics is an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence” [7].

Therefore, all research activities carried out under the CYLCOMED was conducted in compliance with fundamental ethical principles and legal requirements that are briefly clarified within this section.

Rights that are fundamental to CYLCOMED data management

All personal data collected for the CYLCOMED project are in accordance with the relevant European Union (EU) legal requirements on data protection, in particular the provisions of the General Data Protection Regulation (GDPR) [3] and take into account the right to privacy and the right to data protection.

The right to privacy is a fundamental human right which can be found in the European Convention on Human Rights (ECHR) [4] as well as in the Charter of Fundamental Rights of the European Union (CFREU) [5] and has been given a broad interpretation by the European Court of Human Rights (ECtHR).

While not specifically mentioned in the ECHR[1], the right to data protection is a separate right codified in Art. 8 CFREU. In order not to infringe upon Art. 8 of the CFREU, the personal data must be “processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”. It also states that “everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified” [6].

These requirements are also included in the GDPR. The GDPR defines obligations for controllers and processors of personal data and gives the data subjects certain rights.

Particularly the main concepts that should be followed are described in Art. 5 of GDPR [3] which lays out the principles which must be taken into account when processing personal data; specifically Data must be processed lawfully, fairly and in a transparent manner in relation to the data subject, which includes the obligation to have an appropriate legal ground for processing and to inform the data subject about the processing.

Data collection approach

Data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, though there exist some exceptions on compatible purposes. Moreover, it's imperative that the data remains not only adequate and relevant, but also strictly confined to what is required for the intended processing purposes. Additionally, maintaining data accuracy should be a priority, and if necessary, regular updates should be implemented to ensure its current relevance.

Data should only be kept in a form which permits identification of data subjects for as long as it is necessary for the purposes for which the personal data are processed. Afterwards it must

[1] *But in the court’s interpretation since the end of the 1970s/beginning of the 1980s implicitly included in the right to privacy.*

Funded by Horizon Europe Framework Programme of the European Union

be anonymised or deleted, with possible exceptions in case of processing solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Data usage

Finally, the data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. OBJ

Funded by Horizon Europe Framework Programme of the European Union

3 Data sets DMP forms

This section collects all the data informative forms. Here is reported a list of the identified dataset:

3.1 **Pilot 1 - NMT controller CMD**

3.2 **Pilot 2 – Hospitals environment**

- 3.2.1 Deployment A – Paediatric patients
- 3.2.2 Deployment A – Volunteers
- 3.2.3 Deployment B – Virtual Machines for integration

3.3 **CYLCOMED Toolbox**

- 3.3.1 FE4MED
- 3.3.2 Dashboard
- 3.3.3 LADS
- 3.3.4 Lus4Med
- 3.3.5 C-OPA33
- 3.3.6 LOMOS
- 3.3.7 Risk Management Tool

Funded by Horizon Europe Framework Programme of the European Union

3.1 Pilot 1 - NMT controller CMD

Data Summary		
Data set	The pilot was developed as a laboratory project without real patients. A patient´s simulator was used as a SW component of the "Test bench Platform". As is well known, certification of a medical device is a complicated, expensive and time consumable process. For this purpose, the strategy is to incorporate the security features that result from CYLCOMED in a standard external Linux-based board, with enough CPU power so that performance of essential functionalities is not compromised, connected via a serial channel to the medical monitoring device. The medical monitoring functionalities must be preserved from cybersecurity hazards and constitute the legacy of the device. Besides, the infusion pump controller functionality also be embedded in the external board. It communicates with other medical devices such as the infusion pump tree, and the HIS (hospital Information System) via Ethernet, to report on the Vital signs of evolution of the patient. This gateway functionality was performed following the security recommendations mandated by the regulatory norms. This strategy was followed using a legacy device (Vision Air Equipment), and the focus was to achieve an implementation that can be used as a module for legacy devices in the Intensive Care scenario. The manufacturer of the legacy device had to adapt the external board with an open protocol generated in CYLCOMED. A User Guide for the implementation of the External Board in connection to the Vision Air Multiparameter monitor was developed, including the communication protocol and the specific test actions to verify the proper integration.	
Is the data being re-used?	No	
Data classification:	Synthetic Clinical Data (designed to mimic personal data) and Technical Data. No real personal data was generated. Synthetic Clinical Data: Patient data including medical history, diagnosis, Vital signs (NMT, HR, SpO2, Temperature), Infused drug dose Technical: Infusion pump status and alarms, Log generated from CYLCOMED tools.	
What is the purpose of data generation?	The purpose is to store data of NMT control and other vital signs for later review by clinical staff	
What is the expected size of the data that you intend to generate?	The data size can vary depending on the clinical needs. The application is intended for UCI patients and we can use the standard monitoring time. The main data are the data from NMT control and the mean data size for each patient and day is 300 measures of NMT control data (Neuromuscular Transmission value and Relaxant dose rate), and 5700 measures of the other vital signs. There can be additional asynchronous data, such as alarm conditions or personal data.	
What is the origin/provenance of the data?	The data are collected from the patients requiring NMT control during UCI stay: For the correct operation of the device in accordance to functional requirements (i.e. NMT control). For the correct operation of the device in accordance to non-functional requirements (i.e. security features). Data is collected from the CYLCOMED tools for generate security alerts.	
To whom might your data be useful (data utility)	Project partners	
	EVIDEN, MARTEL	Security features
	RGB	Functional features
	Others (External entity)	

Funded by Horizon Europe Framework Programme of the European Union

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES
	Searchable metadata	YES
	Metadata Format	JSON
A	Data access	Data accessibility is restricted to authorized personnel
	Documentation	the tool kit has a tutorial with instructions for use of the application
	Data Protection	The pilot was developed as a laboratory project without real patients, so GDPR is not a concern at this stage
I	Data Standardization	YES (The data is provided in JSON format, which is a standard machine-readable format for logs and structured data.)
	Data Exposure	NO (Interoperability is primarily focused on the internal security components of the CYLCOMED toolbox and the legacy device. External interoperability beyond the test environment was not intended for the raw dataset.)
R	Data documentation	ES (Documentation is provided in the Pilot Final Phase Report (D6.3) and the CYLCOMED final toolbox package (D5.3)
	Data format	JSON

Data security and Ethics	
Data security	The data was encrypted (via FE4MED) and access was controlled (via LuS4MED/C-OPA) to validate the CYLCOMED security toolbox. While the data is synthetic, it mimicked the end-to-end security process, including pseudonymization/encryption requirements.
Ethics	The pilot was developed as a laboratory project without real patients, with only synthetic data involved.

Funded by Horizon Europe Framework Programme of the European Union

3.2 Pilot 2 – Hospitals environment

3.2.1 Deployment A – Paediatric patients

Data Summary		
Data set	Clinical data on 12 patients monitored from remote Data generated from wearable sensors	
Is the data being re-used?	NO	
Data classification:	Personal and Technical data	
What is the purpose of data generation?	These data are used for monitoring the clinical characteristics and changes over time to inform appropriate and timely treatments. Data is also used to monitor unauthorized access or other potential cybersecurity threats in the monitoring system. Data are used for training the algorithms in the cybersecurity toolbox	
What is the expected size of the data that you intend to generate?	Clinical data consists of 30 variables collected for 12 patients. Data from wearables includes ECG, cardiac frequency, respiratory rate, oxygen saturation, weight, body temperature, blood pressure. While ECG, cardiac frequency and respiratory rate are continuously monitored as the wearable device is switched on, the other measures are taken once daily. The expected monitoring time was 8 weeks	
What is the origin/provenance of the data?	Electronic Health record for clinical data; wearable devices for monitoring data	
To whom might your data be useful (data utility)	Project partners	
	Clinical data	OPBG
	Monitoring data	Tool developers
	Other	
	NO	

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES
	Searchable metadata	Metadata are not provided
	Metadata Format	See above
A	Data access	Data access is not permitted to unauthorized personnel outside the hospital due to compliance to GDPR
	Documentation	Data documentation is included in the protocol and in the paperwork of the clinical trial
	Data Protection	All participants in the clinical study signed an informed consent. All procedures regarding data management are GDPR compliant
I	Data Standardization	Clinical standards have been used as for the electronic health record
	Data Exposure	Data not accessible
R	Data documentation	The health parameter data type was documented using the OpenAPI standard, which is reachable only to authorized users upon request.
	Data format	The underlying data format is application/Json, for some health parameter we support export in standard formats, in particular:

Data security and Ethics	
Data security	All data are stored in a secure server on premise within the hospital (OPBG). Access is restricted to authorized personnel through private credentials
Ethics	For personal and health data, a review of ethical requirements is performed both by D2.2 and by the Ethics Committee of the hospitals involved. All participants in the clinical study signed an informed consent. All procedures regarding data management are GDPR compliant

Funded by Horizon Europe Framework Programme of the European Union

3.2.2 Deployment A – Volunteers

Data Summary		
Data set	Volunteers for usability feedback Clinical data access is not permitted to unauthorized personnel outside the hospital due to compliance with GDPR except to MCI staff for technical support.	
Is the data being re-used?	NO	
Data classification:	Technical Data, Personal data is not used in the project.	
What is the purpose of data generation?	Test CYLCOMED toolbox and provide feedback	
What is the expected size of the data that you intend to generate?	32 variables for various days.	
What is the origin/provenance of the data?	Pseudo-anonymized volunteers interacted with the platform to provide feedback.	
To whom might your data be useful (data utility)	Project partners	
	Clinical data	
	Monitoring data	

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES
	Searchable metadata	These field are available for search through API: Type of measure Timestamp Patient identifier (internal to the telemedicine platform)
	Metadata Format	application/Json
A	Data access	The data was stored in a secure server that is accessible only through an authentication process. A role-based access control (RBAC) mechanism was implemented, to limit users' access permission to the specific data required for their work. It was ensured that access to the data is audited and monitored to prevent and detect unauthorized access or use.
	Documentation	Appropriate documentation was provided to help authorized users understand the data and how to use it.
	Data Protection	See data access
I	Data Standardization	Data were stored in machine-readable format (JSON) and it was used standard clinical terminologies. Unit of measurement were stored together with the value.
	Data Exposure	Data were exposed using REST APIs (Application Programming Interfaces) to allow authorized users to access the data and integrate it with other applications and systems each access to the data was traced and available for further inspections.
R	Data documentation	Health parameter data type was documented using the OpenAPI standard, which is reachable only to authorized users upon request.
	Data format	The underlying data format is application/Json, for some health parameter we support export in standard formats, in particular: ECG can be exported in SCP format

Data security and Ethics	
Data security	Stored on proivate servers
Ethics	All clinical, pseudo-anonymized data is deleted

Funded by Horizon Europe Framework Programme of the European Union

3.2.3 Deployment B – Virtual Machines for integration

Data Summary		
Data set	VM logs	
Is the data being re-used?	NO	
Data classification:	Technical Data	
What is the purpose of data generation?	Test tool integration. Log data is used to monitor unauthorized access or other potential cybersecurity threats in the monitoring system. Log data are used for training the algorithms in the cybersecurity toolbox	
What is the expected size of the data that you intend to generate?	Data size was 32 variables for around one week of simulated data	
What is the origin/provenance of the data?	Synthetic data	
To whom might your data be useful (data utility)	Project partners	
	Clinical data	N/A (Synthetic data)
	Monitoring data	Technical partners for integration purposes

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES
	Searchable metadata	These field are available for search through API: Type of measure Timestamp Patient identifier (internal to the telemedicine platform)
	Metadata Format	application/Json
A	Data access	The data was stored in a secure server that is accessible only through an authentication process. A role-based access control (RBAC) mechanism was implemented, to limit users' access permission to the specific data required for their work. It was ensure that access to the data is audited and monitored to prevent and detect unauthorized access or use.
	Documentation	Appropriate documentation was provided to help authorized users understand the data and how to use it.
	Data Protection	See data access
I	Data Standardization	Data were stored in machine-readable format (JSON) and it was used standard clinical terminologies. Unit of measurement were stored together with the value.
	Data Exposure	Data were exposed using REST APIs (Application Programming Interfaces) to allow authorized users to access the data and integrate it with other applications and systems Each access to the data was traced and available for further inspections.
R	Data documentation	Health parameter data type wasdocumented using the OpenAPI standard, which is reachable only to authorized users upon request.
	Data format	The underlying data format is application/Json, for some health parameter we support export in standard formats, in particular: ECG can be exported in SCP format

Data security and Ethics	
Data security	Since the beginning of the project, data security is granted through standard protection measures such as restricted access via authentication, and data encryption at rest through proper database configuration.
Ethics	N/A

Funded by Horizon Europe Framework Programme of the European Union

3.3 CYLCOMED Toolbox

3.3.1 FE4MED

Data Summary		
Data set	Pilot 1| tool FE4MED – Data provided by CMD from RGB Pilot 2| tool FE4MED – Data provided by CMD from MCI Tool FE4MED only processes data	
Is the data being re-used?	The personal data processed by FE4MED are not generated by FE4MED, but by the CMDs. In both pilots the data are encrypted for protecting them when are sent to the hospital system and when are stored. Beside this the FE4MED tool generates technical data (logs data) of the encryption, decryption processes for training an AI model. This model was used to analyses the data generated in the encryption/decryption processes and detect anomalies.	
Data classification:	The data generated in Pilot 1 was related to the patient's vital signs such as heart rate, temperature and oxygen saturation taken each minute during several days while the patient stay at the Intensive care unit. Also, NMT measures were taken every few seconds or minutes. Regarding Pilot 2 questionnaire's answers, filled by the patient or the family, are collected from the MCI mobile app. The FE4MED encrypts these data. Pilot 1 is expected to generate data files ranging Mb size. Pilot 2 is expected to generate files ranging Kb size.	
What is the purpose of data generation?	The source of the data are fake data generated by the CMD (infusion pumps) provided by RGB in Pilot 1, or by the CMD (mobile phone of MCI Hub) provided by MCI in Pilot 2.	
What is the expected size of the data that you intend to generate?	The personal data processed by FE4MED are not generated by FE4MED, but by the CMDs. In both pilots the data are encrypted for protecting them when are sent to the hospital system and when are stored. Beside this the FE4MED tool generates technical data (logs data) of the encryption, decryption processes for training an AI model. This model was used to analyses the data generated in the encryption/decryption processes and detect anomalies.	
What is the origin/provenance of the data?	The data generated in Pilot 1 was related to the patient's vital signs such as heart rate, temperature and oxygen saturation taken each minute during several days while the patient stay at the Intensive care unit. Also, NMT measures wil be taken every few seconds or minutes. Regarding Pilot 2 questionnaire's answers, filled by the patient or the family, are collected from the MCI mobile app. The FE4MED encrypts these data. Pilot 1 is expected to generate data files ranging Mb size. Pilot 2 is expected to generate files ranging from Kb size.	
To whom might your data be useful (data utility)	Project partners	
	RGB & MCI	RGB and MCI as providers of CMDs and hospital backend infrastructures, ensures that the encrypted patient's data reach the Hospital Staff as end users (Doctors & Nurses, and admin staff).
	EVIDEN and XLAB	The logs provided by FE4MED tool are used for monitoring normal and anomalous behavior during the patient's data management.
	Others (External entity)	
	Cybersecurity providers	The generated logs (which doesn't contain personal or sensitive data) can help to develop cybersecurity tools for mitigate threats.

Funded by Horizon Europe Framework Programme of the European Union

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES.
	Searchable metadata	Log files from FE4MED are created with module name plus a timestamp as unique identifier. Pilot files are generated with a unique identifier name.
	Metadata Format	For FE4MED files, at this moment is not expected to include metadata, but was analyses the way to do it, if it is required.
A	Data access	Metadata provided for the given datatype.
	Documentation	For FE4MED files, it is not expected to include metadata.
	Data Protection	FE4MED files are only accessed by the consortium members, e.g., partners involved in the IA training.
I	Data Standardization	For encrypted pilots' data, only allowed users are able to decipher data.
	Data Exposure	The documentation related to the data and the operation of FE4MED is provided in WP5, WP6 and WP3 deliverables, e.g., D5.1, D5.2, D5.3, D6.3 among others.
R	Data documentation	FE4MED files doesn't collect personal information, only data of encryption/decryption processes. FE4MED encrypts data from pilots. In the case of Pilot 1 the data to be encrypted are fake data. In the case of Pilot 2, FE4MED only process (encrypt/decrypt) data collected by the MCI mobile app*.
	Data format	FE4MED log files follows Syslog standard. The pilots' data files to be encrypted follow the JSON standard for exchanging data.

Data security and Ethics	
Data security	The data generated by FE4MED tool and the pilots' data are sent through SSL connections to the LOMOS tool and the FE4MED server on hospital infrastructure, respectively. The pilots' data was encrypted to be sent to the hospital system. Encryption ensures protection in transit and at rest. Additionally, only users are able to decipher the encrypted data.
Ethics	For accessing hospital services and data, the users need to be authenticated through an SSI-based decentralized solution (LUS4MED) and authorized by an authorization tool (C-OPA).

3.3.2 Dashboard

Data Summary		
Data set	Pilot 1 & Pilot 2 — Dashboard (visualizes data from LADS & LOMOS). In both pilots, the Dashboard shows alerts from LADS and LOMOS; it does not display personal data.	
Is the data being re-used?	NO.	
Data classification:	Technical data (see 1.2)	
What is the purpose of data generation?	Collect outputs from connected tools to present security alerts and context to users in a simple, user-friendly way.	
What is the expected size of the data that you intend to generate?	Varies by pilot; the tool does not collect patient data, only machine-generated information.	
What is the origin/provenance of the data?		
To whom might your data be useful (data utility)	Project partners	
	OPBG, FHUNJ, CUB, RGB	As project stakeholders and use case providers, the data collected and showed in the dashboard was useful for them in order to validate the tools
	XLAB, MCI	As tool providers, the data collected was useful to better understand the behavior of their systems and solutions.

Funded by Horizon Europe Framework Programme of the European Union

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES. The data collected from each tool connected to the Dashboard is stored with a unique identifier and a timestamp.
	Searchable metadata	There is no metadata added in what the dashboard collects and store
	Metadata Format	There is no metadata added in what the dashboard collects and store
A	Data access	Only partners of the consortium can access the data shown via the dashboard GUI.
	Documentation	All the information related to deployment, configuration and use of the tool is described in deliverables D5.1, D5.2 and D5.3.
	Data Protection	The Dashboard does not collect or store personal data. GUI access requires user credentials.
I	Data Standardization	The data is received in Syslog1 and Json2 format standard. The dashboard does store the data in Json format standard.
	Data Exposure	The data can be accessed through the web GUI of the tool
R	Data documentation	The format, structure and standard related to the data and the Dashboard tool information is provided in the different WPs deliverables such as D5.1, D5.2 and D5.3. The public deliverables and data are available through the web of the project
	Data format	As it was mentioned before, the standard used are: RFC5424 and RFC8259.

Data security and Ethics	
Data security	The data is received through an encrypted channel (SSL) and to see the data on the GUI, the user can access using username/password credentials.
Ethics	The data received from the connected tools into the Dashboard, only contains technical data, no personal data are collected.

Funded by Horizon Europe Framework Programme of the European Union

3.3.3 LADS

Data Summary		
Data set	Pilot 1 & Pilot 2 — LADS (Live Anomaly Detection System) network telemetry and anomaly outputs. LADS processes machine-generated network data (no patient data).	
Is the data being re-used?	No	
Data classification:	Personal / Technical data (see 1.2)	
What is the purpose of data generation?	Collect and analyses network telemetry to detect anomalous behavior (e.g., low-rate/slow-read DoS). Produce explainable alerts and summaries for operators and the Dashboard.	
What is the expected size of the data that you intend to generate?	Variable; depends on traffic volume and capture scope.	
What is the origin/provenance of the data?		
To whom might your data be useful (data utility)	On-premises LADS sensors deployed in the project Pilots	
	Project partners	
	OPBG, FHUNJ, RGB	Validate detections in pilot environments.

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES, LADS use timestamps to store the telemetry in the csv files that generates
	Searchable metadata	N/A.
	Metadata Format	N/A
A	Data access	Consortium-restricted (on-prem file storage; Dashboard views).
	Documentation	Capture scope, schema, deployment and ops in D5.1, D5.2, and D5.3.
	Data Protection	LADS does not collect personal data. Csv files are stored on secured hosts.
I	Data Standardization	Flow-like records and anomaly outputs in JSON (RFC 8259) and CSV; message transport via AMQP (RabbitMQ)
	Data Exposure	Local files for connected components
R	Data documentation	Formats, fields (e.g., src/dst IP/port, proto, RMSE, feature impacts), and workflows described in WP5 deliverables.
	Data format	JSON/CSV with ISO/RFC timestamps

Data security and Ethics	
Data security	On-prem processing; encrypted transport (TLS for management/AMQP where applicable)
Ethics	No payload/content inspection; only technical telemetry (headers/flows)

Funded by Horizon Europe Framework Programme of the European Union

3.3.4 Lus4Med

Data Summary		
Data set	Pilot 1 & Pilot 2| tool LuS4MED – Generates and validates Verifiable Credentials (VCs). In both pilots LuS4MED generates technical files (log files of the process not including personal or sensitive data)	
Is the data being re-used?	NO	
Data classification:	Personal / Technical data	
What is the purpose of data generation?	VCs are created for user authentication purposes on the hospital infrastructure.	
What is the expected size of the data that you intend to generate?	Log files are generated for tracking tool processes.	
What is the origin/provenance of the data?	Is expected to generate log data files ranging between Kb and Mb size.	
To whom might your data be useful (data utility)	VCs are generated based on the user's data provided by the hospital system. Every time a user tries to authenticate to the hospital service through LuS4MED, this tool collects data of the process, but not personal data.	
	Project partners	
	RGB & MCI	RGB and MCI as providers of hospital backend infrastructures, ensures controlled access to the services and data.

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	YES
	Searchable metadata	Log files from LuS4MED are created with module name plus a timestamp as a unique identifier.
	Metadata Format	For LuS4MED files, at this moment is not expected to include metadata,
A	Data access	For LuS4MED files, at this moment is not expected to include metadata,
	Documentation	LuS4MED files are only accessed by the consortium members, e.g., partners providing hospital infrastructure (RGB and MCI).
	Data Protection	The documentation related to the data and the operation of LuS4MED is provided in WP5, WP6 and WP3 deliverables, e.g., D5.1, D5.2, D5.3, D6.3 among others.
I	Data Standardization	LuS4MED log files don't collect personal information, only data from the authentication process. VCs are transmitted through secure channels.
	Data Exposure	LuS4MED log files follows Syslog1 standard. VCs follow W3C VC2, DIF3, OIDC4 standards.
R	Data documentation	LuS4MED files are shared only with RGB and MCI platforms.
	Data format	The format, structure and standard related to the data and the LuS4MED tool information is provided in WP5, WP6 and WP3 deliverables, e.g., D5.1, D5.2, D5.3, D6.3 among others.

Data security and Ethics	
Data security	The VCs and the log files (if needed) are sent through secure connections (e.g., SSL).
Ethics	The log files generated by the LuS4MED tool only contain technical data, no personal data are collected there. The VC only contains the minimal information needed for user authentication into the system.

Funded by Horizon Europe Framework Programme of the European Union

3.3.5 C-OPA

Data Summary		
Data set	Pilot 1 - Hospital Equipment	
Is the data being re-used?	No, C-OPA only works to enforce policies for access to CYLCOMED components, specifically FE4MED	
Data classification:	Technical data	
What is the purpose of data generation?	The only data generated is the access control policies and the access control logs. Policies are user curated with the purpose of defining access control to protected CYLCOMED services; logs are for analytical purposes (e.g. threat detection)	
What is the expected size of the data that you intend to generate?	Policies should take no more than a few MBs per protected service, depending on complexity. Logs depend on the amount of access the services get, and the verbosity of the logs.	
What is the origin/provenance of the data?	Policies are written by designated administrators. Logs come from C-OPA, referring to the decisions made by the policy agent.	
To whom might your data be useful (data utility)	Project partners	
	RGB	Writing policies, verifying logs for integration

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	Yes, both policies and logs are stored and represented in a way that can be searched through (policies are named, logs follow a defined JSON format)
	Searchable metadata	Policy names and descriptions.
	Metadata Format	Decision Logs; JSON per decision, partially customizable
A	Data access	application/Json
	Documentation	Policies are authored and accessed only by designated administrators that can access the place they are stored in, same with the logs (access to the C-OPA agent API).
	Data Protection	Documentation of C-OPA's API and configuration for handling policies and accessing logs.
I	Data Standardization	End users don't access the logs or policies; these are intended for system administrators.
	Data Exposure	Policies use C-OPA's own programming language (Rego), logs are standard JSON
R	Data documentation	Logs API, or plain text files. Policies written in .rego files
	Data format	C-OPA documentation and configuration

Data security and Ethics	
Data security	Policies and logs are stored securely, only accessible by admins of the system (no exposure to external users).
Ethics	Poorly written policies might expose protected services to unintended parties. Admins need to ensure policies are robust.

Funded by Horizon Europe Framework Programme of the European Union

3.3.6 LOMOS

Data Summary		
Data set	| tool: LOMOS # - Log monitoring system	
Is the data being re-used?	NO	
Data classification:	Technical data (see 1.2)	
What is the purpose of data generation?	The tool that does not generate or collect data. The tool uses data that is being produced by other tools or user applications in the project, analyses it and produces warnings in case any anomalies in the data are detected.	
What is the expected size of the data that you intend to generate?	It is generally difficult to assess as it depends on the use case. For the training LOMOS model, a normal amount of data (log lines) would be around 100.000 to 1.000.000 log lines. For inferencing LOMOS requires at least 1000 log lines.	
What is the origin/provenance of the data?	We are using data from partners' tools, like the MCI Health Platform Reverse Proxy. We generate anomaly scores in the JSON format that are then visualized in Grafana and CYLCOMED Dashboard and include some basic information (e.g. timestamp, source, anomalous log line).	
To whom might your data be useful (data utility)	Project partners	
	XLAB	Tools providers

FAIR principles (**F**indable, **A**ccessible, **I**nteroperable, **R**eusable)		
F	Identifiers are unique and immutable	Each anomaly score as the output data of LOMOS inference is unique as it refers to the single log line that LOMOS detected as suspicious
	Searchable metadata	Yes, by these parameters: timestamp, anomaly score.
	Metadata Format	JSON
A	Data access	The data is accessible only to the project consortium.
	Documentation	The principles of the operation of the system are well documented in the LOMOS documentation. They help the end-user understand how to use or even customize the results of the LOMOS to improve their system
	Data Protection	LOMOS does not collect personal data, only non-personal data generated by other tools or applications. The authors of the applications should be the ones informing the users.
I	Data Standardization	L OMOS output (anomaly score) is in standard JSON format which can be easily converted to other standards needed by the rest of the toolbox.
	Data Exposure	Via the agreed output method and LOMOS API-2.
R	Data documentation	Structure of the LOMOS output data (anomaly score) is documented in the LOMOS documentation. The structure of the input data should be documented by the tool and application providers.
	Data format	JSON data format is used for anomaly scores.

Data security and Ethics	
Data security	Input data (logs) and output data (anomaly score) are stored in LOMOS containers on a machine or VM where LOMOS runs. Access to the machine is regulated with IAM tool.
Ethics	Not applicable

Funded by Horizon Europe Framework Programme of the European Union

3.3.7 Risk Management Tool

Data Summary		
Data set	Pilot 1 and 2 risk management data based on publicly available CYLCOMED deliverables	
Is the data being re-used?	NO	
Data classification:	Technical data – data related to risks and controls associated with the project pilots. The risks and controls were based on publicly available data.	
What is the purpose of data generation?	For risk management. The data was generated to help understand how the risk management framework and the tool could be used to manage CMD risks.	
What is the expected size of the data that you intend to generate?	Give an approximate quantification, it could be related to the number of patients	
What is the origin/provenance of the data?	N/A This tools used only synthetic data generated to test it's capabilities	
To whom might your data be useful	Project partners	

Data security and Ethics	
Data security	Communications through SSL encrypted connections.
Ethics	N/A

Funded by Horizon Europe Framework Programme of the European Union

Conclusions

The successful completion of the CYLCOMED project at Month 36 marks the delivery of a fully validated and ethically sound data management framework. This final Data Management Plan (DMP, D1.3) confirms that the project achieved its goal of strengthening Connected Medical Device (CMD) cybersecurity while rigorously maintaining patient privacy. The core outcome is the demonstration that FAIR data principles and GDPR compliance are a particularly crucial and complex aspects when dealing with health applications and cutting-edge security toolbox.

Key Data Management Outcomes

As of Month 36, the project has successfully established a robust data management framework that balances the critical need for cybersecurity research with the stringent requirements of patient privacy and GDPR compliance. The Data Management Plan has evolved from a preliminary strategy into complete summary.

Ethical Compliance and Data Minimisation Achieved

All data collection processes were subject to rigorous governance. For the real-world validation (Pilot 2, Deployment A), all data collection involving pseudonymised paediatric patients was conducted under strict ethical approval from the relevant Hospital Ethics Committees. Furthermore, the project successfully utilized a Digital Twin/Simulator approach (Pilot 1), generating Synthetic Clinical Data which minimized the need for processing real sensitive data while comprehensively validating the technical solution's functional and security requirements.

GDPR and Security: Privacy by Design Implementation

The project demonstrated that cybersecurity tools (the CYLCOMED Toolbox—including FE4MED, LADS, and LOMOS) can be integrated into legacy systems without compromising data integrity.

The involvement of Data Protection Officers (DPOs), legal offices and data stakeholders throughout the project lifecycle ensured that "Privacy by Design" was not just a concept, but an implemented reality, particularly through:

- Pseudonymisation: Implementing processes to immediately pseudonymise patient data upon collection.
- Access Control: Utilizing the LuS4MED (authentication) and C-OPA (authorization) tools to enforce Role-Based Access Control (RBAC), ensuring only authorized clinical staff could access protected services and data.
- Security Monitoring: Generating non-personal technical logs (e.g., Syslog's, network telemetry) from all toolbox components for threat detection, thereby achieving security goals without inspecting patient content.

FAIR Implementation Final Status

The project successfully applied the FAIR principles to all research outputs, differentiating between highly sensitive patient data and reusable technical outputs:

- Findable: Metadata for all public deliverables, research articles, and technical log datasets have been fully indexed and catalogued, ensuring the project's outputs can be discovered via standard search parameters.
- Accessible: While sensitive pseudonymised patient data remains strictly restricted (Closed Access) to protect privacy (GDPR Article 9), the underlying methodologies, technical logs, and aggregated results (non-personal data) have been made Open Access where legally possible, typically via the project website and the EU repository.
- Interoperable: The use of standard data formats (e.g., JSON/CSV) and established clinical and security protocols (Syslog RFC 5424, SCP for ECGs, OpenAPI for

Funded by Horizon Europe Framework Programme of the European Union

documentation) ensures the CYLCOMED solutions can communicate effectively and be integrated into other technical infrastructures.

- Reusable: The CYLCOMED Toolbox source code, the detailed validation methodologies (D6.3), and the comprehensive Risk Management Framework (D4.3) provide a foundation for future research and commercialization efforts in Medical Device security, representing the project's primary reusable output.

Final Data Disposition and Archiving

Following the project's conclusion, all datasets generated and processed have a defined long-term disposition:

- Sensitive Personal Data (Pilot 2, Deployment A):
  This pseudonymised data is being handled in strict accordance with the hospital retention policies and the specific consent forms signed by the participants. Access, retention, and final deletion timelines are governed by the clinical partner's Data Protection Officer.

- Technical Data and Synthetic Data (All Pilots):
  All technical logs, security alert data, and the Synthetic Clinical Data generated during Pilot 1 are retained by the technical partners for a minimum of five years (as required by the H2020 grant agreement) for verification, future research, and exploitation activities.
  Documentation supporting the final Toolbox is archived in the EU repository.

Funded by Horizon Europe Framework Programme of the European Union

References

[1] Regulation (EU) 2016/679 (General Data Protection Regulation)

[2] EU Grants: Data Management Template (HE): V1.0 – 05.05.2021

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

[4] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950

[5] Charter of Fundamental Rights of the European Union, OJ C 202/2, 7.6.2016, p. 389-405.

[6] Article 8, 2 of the Charter of Fundamental Rights of the European Union.

[7] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

Funded by Horizon Europe Framework Programme of the European Union

Appendix A - New Dataset form - template

This table is a template for the analysis of FAIR data within the CYLCOMED project. For each data type generated during the project involved partners shall fill in a copy of this table.

Data set	**Data set name/ context**
Is the data being re-used from another project / source?	*NO / YES if this data is coming from another project / source please describe the source and why we are using it.*
Data classification:	*Personal / Technical data (see 1.2)*
What is the purpose of data generation?	*Why do we collect this type of data?*
What is the expected size of the data that you intend to generate?	*Give an approximate quantification, it could be related to the number of patients (e.g., we expect to collect X measures for each patient every day, and the study will end in a month)*
What is the origin of the data?	*From whom or what are we collecting/generating the data*
To whom might your data be useful (data utility)	Project partners
	Others (*External entity*)
	Why does it need access to this data?

FAIR principles		
***F**indable*	Identifiers are unique and immutable.	*YES / NO if not, please explain why.*
	Searchable metadata	*Metadata provided for the given datatype.*
	Metadata Format	*Format of metadata (e.g., application/Json)*
***A**ccessible*	Data access	*Describe accessibility of the data, specifying if restriction.*
	Documentation	*Describe the documentation provided together with the data, and how it is supposed to help the user in data consumption.*
	Data Protection	*Describe compliance with regulations such as GDPR and how end-users (if any) will be informed before data collection.*
***I**nteroperable*	Data Standardizatio n	*Is any standard being used? Is the terminology in line with domain standards?*
	Data Exposure	*How the data will be made accessible to other systems (if possible).*
***R**eusable*	Data documentation	*Describe how the data will be documented, and how to access such documentation.*
	Data format	*Describe the data format if any standard is used, refer to it. This field should be compiled using the MediaType notation (rfc6838).*

Data security and Ethics	
Data security	Any relevant information about how we protect this data.
Ethics	Any relevant information about the possible ethical issues related to this data.

Funded by Horizon Europe Framework Programme of the European Union