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

D6.2 Pilots initial phase report

Version: v.1.1

Work package	WP 6
Task	Task 6.2
Due date	30/11/2024
Submission date	30/11/2024
Deliverable lead	MCI
Version	1.1
Authors	Simone Favrin (MCI), Andrea Scaburri (MCI), Marco Mosconi (MCI), Ricardo Ruiz Fernandez (RGB), Ricardo Nolasco (RGB), Juan Carlos Perez Baun(ATOS), Esteban Alejandro Armas Vega (ATOS), Panagiotis Kapsalis Alberto Eugenio Tozzi (OPBG), Alvise Mattana (OPBG), Hrvoje Ratkajec (XLAB), João Rodrigues (INOV), Andrés G. Castillo (FHUNJ), Santiago Bollain (FHUNJ).
Reviewers	Dietmar Frei (CUB), Orhun Utku Aydin (CUB)

Abstract	This derivable describes the main activities performed to start the first phase of Pilot 1 and Pilot 2. This document provides a detailed analysis of the integration status of each tool within every pilot. The challenges encountered and the next steps are outlined in the concluding section of the document.

Keywords	Pilots, tools, implementation, validation

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V 0.0	19/09/2024	Issue of toc for discussion and comments	S. Favrin, A. Scaburri
V 0.1	29/10/2024	Revised and finalised toc	S.Favrin, R. Ruiz
V 0.2	07/11/2024	Contribution of partners defined	S.Favrin, R. Ruiz
V 0.3	18/11/2024	Collection of all partners contributions	All Authors
V 1.0	19/11/2024	First complete version for internal review	S. Favrin, A. Scaburri, M. Mosconi
V 1.1	27/11/2024	After internal review	S. Favrin, A. Scaburri

Disclaimer

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

Funded by Horizon Europe Framework Programme of the European Union

ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Funded by Horizon Europe Framework Programme of the European Union

Executive summary

CYLCOMED project involves two pilots, the first one is named “Cybersecurity in Hospital Equipment for COVID-19 ICU patients” (here in after, Pilot 1) and the latter, which is based on a telemonitoring platform, is named “Cybersecurity for Telemedicine Platforms” (here in after, Pilot 2).

Pilot 1 scenario represents a frequent one in the healthcare landscape, where a legacy device that can be improved with new modules (in CYLCOMED, it is an infusion pump and a new controller), it also needs to raise the cybersecurity levels. A key aspect of this pilot is the development and implementation of robust cybersecurity measures to safeguard patient data and equipment security. This includes integrating security features to mitigate risks such as unauthorized access and data breaches.

Pilot 2 instead covers a completely different scenario: patients outside the hospital that need to be monitored remotely. This scenario, as opposed to pilot 1 that refers to an on premise, legacy, physical device, involves a software as a DM, specifically MPH, a telemonitoring platform which is used to monitor paediatric cardiac patients. Therefore, Pilot 2 aims to enhance cybersecurity for telemedicine platforms, prioritizing patient data protection and medical device reliability.

In CYLCOMED, pilots are executed in two main tasks: “T6.2 Pilots implementation and toolbox integration” (Briefly, implementation) and “T6.3 Pilots validation”. The main focus of these tasks is to provide a framework for tool integration in the available medical devices and eventually improve also the development of the tools to make the use easier (Implementation) and to investigate the actual capabilities, the limitation, and to capture the essence of the end users feedbacks to further improve the tools (Validation). The implementation task focuses on setting on and running the CYLCOMED project pilots by developing and integrating the end-user applications with the toolbox components.

The overall goal is to bridge technology and healthcare, strengthening telemedicine security and ensuring practical and effective tools for everyday use; to achieve this ambitious result, the first phase of pilot development focused on integrating the toolbox in the two different MDs and understanding specific problems, limitations and difficulties.

The integration task is dealing with different aspects in the two Pilots, characteristics of the two scenarios: Pilot 1 is developing a HIL/SIL test bench platform to evaluate controller performance and associated risks in a controlled environment. The platform includes a controller, infusion pump, patient model, and HIL/SIL interface tool. The test bench is currently under development, with recent progress including the development of a backend app that mimics a Hospital Information System and the integration of cybersecurity tools. The verification plan involves creating test cases, executing them on the HIL/SIL platform, and analyzing the results. Pilot 2 focuses on the implementation of a telemonitoring system, integrating the CYLCOMED Toolbox into a real-world hospital setting. The consortium faced challenges due to evolving regulations. OPBG addressed this by conducting interdisciplinary consultations and updating study documents to align with the new requirements. OPBG successfully obtained ethical approval from the Territorial Ethical Committee, enabling the deployment of the CYLCOMED Toolbox and monitoring devices. A patient screening process was conducted to identify suitable participants for the initial validation phase.

Here is a brief overview of the current status (development and integration) of each tool in the CYLCOMED toolbox. The following list presents a brief overview of the development and integration status of each tool designed for the two pilots.

- LADS and LOMOS: These tools are being integrated to analyze network traffic and system logs, respectively. They have been successfully tested in the virtual environment and ready to be installed on the hospitals’ hardware.

Funded by Horizon Europe Framework Programme of the European Union

- Connected Medical Devices and Services Management Tools: The OTA Mechanism is being used to deploy applications to medical devices. In accordance with the consortium agreement, this tool has been implemented solely in Pilot 1.
- LuS4MED and FE4MED: These tools are being integrated to provide identity/authorization functionalities and to protect patient data through encryption, respectively. The final validation tests are still ongoing for both.
- CYLCOMED Security Dashboard: This dashboard is under development to visualize the outputs of various tools. To finalize the development of this tool, the technical partners need to reach an agreement on data standardization (This point is close to being resolved).
- In addition, it has developed and implemented the CYLCOMED Risk Management tool designed as a platform to identify and manage risks associated with connected medical devices (CMDs). This tool is being used to assess and mitigate risks associated with the NMT signal simulator, external module, infusion pump in Pilot 1 and to address evolving regulatory requirements and data privacy concerns in Pilot 2.

In Pilot 1 the validation process currently focuses on technical aspects, including setting up an automated test bench and defining test cases. Non-technical validation involves interaction with healthcare professionals to ensure the relevance of the developed solutions. In Pilot 2, the validation process involves a wide approach, including stakeholder interviews and analysis of system performance and impact on clinical workflows.

The project as a whole faced both technical and regulatory challenges; particularly, some legal and ethical concerns were partially unexpected and, even though it diluted the implementation time, the need to improve the toolbox from these perspectives has been hugely beneficial to provide value to the project.

An example of this can be found in the deployment changes that were required in Pilot 2, from cloud applications to on premises installation. Also, the possibility to understand the reasons behind these requests, improved the knowledge of the whole consortium, allowing to design a better product with added value.

From the mere technical point of view, the tools have successfully addressed specific challenges: starting from LADS, the initial training using synthetic data could have an impact on detection accuracy, and also the complexity of accessing the system within hospital security protocols. The integration of LuS4MED required additional development and testing to adapt to different authorization systems (C-OPA and OpenID Connect). FE4MED encountered challenges in developing two distinct encryption modules for different environments (Raspberry Pi and Android). As already mentioned above for Pilot 2, due to evolving regulatory frameworks it has been necessary to face additional challenges, including updating documentation, data management planning, and ethical considerations (DPIA and Ethical Committee approval).

In conclusion, the CYLCOMED project has made significant progress in addressing regulatory, ethical, and technical/operational challenges. The collaboration between technical experts and healthcare professionals has been instrumental in ensuring the project's alignment with both legal requirements and clinical needs. The next step involves validating the systems in real-world settings to gather valuable insights for further refinement and improvement.

Pilot 1 will continue to focus on extending RGB's CMD without interfering with its certification. Clinician involvement will be crucial in collecting feedback and refining the system. The connected medical device integrity solution may play a central role in the integration of the different tools. Pilot 2 is progressing towards the installation phase, where the MCI's telemonitoring platform and cybersecurity measures will be set up in the hospital. After successful system testing and the Site Initiation Visit (SIV), already planned, patient recruitment and data collection will start, marking the official launch of the pilot.

Funded by Horizon Europe Framework Programme of the European Union

Table of contents

Funded by Horizon Europe Framework Programme of the European Union

List of figures

Funded by Horizon Europe Framework Programme of the European Union

List of tables

Funded by Horizon Europe Framework Programme of the European Union

Abbreviations

AI	Artificial Intelligence
API	Application programming interface
ARDS	Acute respiratory distress syndrome
ATOS	Atos Spain
CMD	Connected Medical Device
CP-ABE	Cipher Policy-Attribute-Based Encryption
CPU	Central Processing Unit
CUB	Charité – Universitätsmedizin Berlin
CYLCOMED	CYbersecurity tooLbox for COnnected MEdical Devices
D#.#	Deliverable (referred to CYLCOMED proposal)
DNS	Domain Name System
DPIA	Data Protection Impact Assessment
EU	European Union
FE4MED	Functional Encryption for Medical Data
FHUNJ	Fundación para la Investigación Biomédica Hospital Infantil Universitario Niño Jesús
GDPR	General Data Protection Regulation
GDPR	General Data Protection Regulation
HIL	Hardware In Loop
HIS	Hospital Information System
IAM	Identity and Access Management
IBM	International Business Machines Corporation
ICU	Intensive Care Unit
INOV	Inov - Instituto De Engenharia De Sistemas E Computadores, Inovação

Funded by Horizon Europe Framework Programme of the European Union

IT	Information technology
IVDR	In Vitro Diagnostic Medical Devices
KPI	Key Performance Indicator
KUL	Katholieke Universiteit Leuven
LADS	Live Anomaly Detection System
LuS4MED	Ledger uSelf for Medical Data
M#	Month of the project
MCI	MediaClinics Italia
MD	Medical Device
MDD	Medical Devices Directive
MDR	Medical Devices Regulation
MHP	Mediaclinics Health Platform (Telemedicine platform)
NMBAs	N-nitroso-n-methyl-4-aminobutyric acid)
NMT	Neuromuscular transmission
OEM	Original Equipment Manufacturers
OPBG	Ospedale Pediatrico Bambin Gesù
OTA	Over-the-air
RGB	RGB Medical Devices
SIL	Software in Loop
SSI	Self Sovereing Identity
V&V	Verification and validation
VPN	Virtual Private Network
WP	Work Package
XLAB	XLAB Razvoj Programske Opreme in Svetovanje

Funded by Horizon Europe Framework Programme of the European Union

1 Objectives of the Report

This report focuses on the groundwork for the CYLCOMED project's pilot studies, highlighting the steps taken to prepare for their implementation. Rather than diving into the finer technical details, covered in other deliverables, it explores the broader aspects that have been carefully considered to make the pilots effective and relevant.

The CYLCOMED project is about tackling real-world challenges in CMDs cybersecurity. A key part of this effort involves two pilot studies designed to evaluate the CYLCOMED toolbox in diverse scenarios. These pilots go beyond testing individual tools, they're built to capture a wide range of perspectives from clinicians, IT staff, administrators, and even patients, ensuring the solutions are practical and impactful across the board.

This report details the design and preparation of the pilots, explaining how they were shaped to address both the technical and clinical aspects of digital healthcare. The involvement of multiple stakeholders ensures that every aspect of the pilots reflects real-world needs and challenges. This phase lays a strong foundation for the next steps, where the pilots will be deployed and tested in real and controlled environments.

Further details about the outcomes of the pilots and their testing will be provided in upcoming report D6.3, considering T6.2 and T6.3 development, offering a complete picture of CYLCOMED's journey toward improving cybersecurity in digital healthcare.

1.1 Purpose and coverage of the Report

This report refers to the first 24 months of the project, focusing on all the activities done from final aspects of the preparation of the pilots to the first activities in the pilots.

It encompasses both the technical aspects that were faced and the validation process that is under development.

1.2 Brief recap about the pilots

This section is a presentation and a brief recap of CYLCOMED's pilots, with the purpose to clarify the importance of these pilots to demonstrate and improve CYLCOMED's toolbox and capabilities.

Funded by Horizon Europe Framework Programme of the European Union

1.2.1 Pilot 1: Hospital Equipment

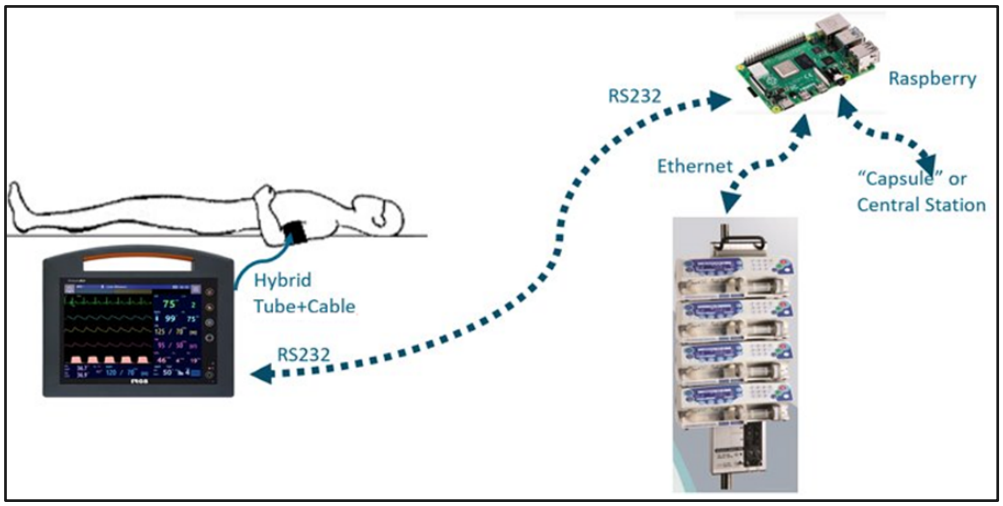

Figure 1: Schematics for control system

In Pilot 1 of the hospital equipment pilot, the central objective is to address the critical issue of cybersecurity within hospital equipment deployed in Intensive Care Units (ICUs). This initiative is particularly focused on patients suffering from acute respiratory distress syndrome (ARDS) symptoms, a condition that poses significant challenges in terms of patient care and management.

Pilot 1 places a specific emphasis on the strategic use of neuromuscular blocking agents (NMBAs) to optimise patient outcomes, especially for those with severe hypoxemic ARDS who require mechanical ventilation support. By leveraging NMBAs effectively, the project aims to enhance ventilatory system support, reduce mortality rates, and facilitate the recovery process for these critically ill patients.

The Vision Air monitor makes it possible to monitor different physiological parameters. The automatic control of physiological parameters is based on the adjustment of the infused dose of the drugs used to regulate the controlled parameter, so a key component is the infusion pump used to administer the drugs to the patient. For this purpose, we will use the AITECS infusion pump tree that allows the control of several infusion pumps for developments.

Figure 2: Equipment

1. Introduction of the necessary parameters to carry out the control
2. Options to control the evolution of the control session

Funded by Horizon Europe Framework Programme of the European Union

3. Screen presentation of control evolution
4. Alarms management such as alarms related to the infusion pumps

The pilot 1 core focus is on cybersecurity measures to enable secure operation of hospital equipment in ICU setting. Furthermore, the project aims to develop and implement cutting-edge cybersecurity measures to safeguard the integrity and confidentiality of patient data and ensure the secure operation of hospital equipment in ICU settings. By integrating robust security features into the equipment, the project endeavours to mitigate potential risks such as unauthorised access, data breaches, and device tampering, thereby enhancing overall patient safety and data protection.

The control algorithms and management of the infusion pump tree will be executed from an external processing module linked to the monitor, ensuring seamless exchange of information for data input and display through the user interface. This integration supports the project's core focus on Neuromuscular Transmission (NMT) control via Target Control Infusion, employing sophisticated techniques to monitor and adjust neuromuscular blockade levels with precision, tailored to the specific needs of each patient.

Overall, Pilot 1 of the hospital equipment project represents the possibility to introduce a strong focus on cybersecurity aspects, not worse the capabilities of intensive care settings, patient care optimization, and innovative approaches to NMT control through Target Control Infusion.

While essential clinical functionalities must be guaranteed, the main task in CYLCOMED has been to prepare the test benching platform and to initiate validation to ensure that the clinical requirements are also complied with when SW cybersecurity components are integrated.

1.2.2 Pilot 2: Telemonitoring

Pilot 2 of the CYLCOMED project is a cornerstone in advancing cybersecurity for telemedicine platforms, focusing on protecting sensitive patient data while ensuring the reliability of connected medical devices. The pilot is split into two deployments: one in real-world hospital settings and another in a controlled, simulated environment.

Deployment A takes place in hospitals, involving paediatric cardiac patients and leveraging existing certified medical devices and infrastructure. The tools are seamlessly integrated into clinical workflows while adhering to strict ethical guidelines to prioritise patient safety and privacy. Dedicated equipment is provided to participating hospitals, pre-configured with the necessary software. This phase allows for real-time monitoring of log and network data to detect potential cyber threats. It also encourages collaboration between technical teams and clinicians, refining the tools based on practical challenges and user feedback encountered in everyday clinical scenarios.

Deployment B shifts to a virtual environment to evaluate the full CYLCOMED toolbox without involving real patients or hospital systems. This controlled approach ensures a comprehensive examination of the tools' scalability, robustness, and cybersecurity features. The focus includes addressing specific scenarios like ambulance transit and utilising AI-driven threat detection to analyse vulnerabilities. It also allows the usage of simulated cyber-attacks on known vulnerabilities in order to perform a laboratory level assessment of the detection tools proposed by the toolbox. This environment enables rigorous testing of tools while maintaining a safe and flexible setup for experimentation.

Two sub-pilots (preparation of these is still under development, being strictly related and dependent from the major scenarios) complement these efforts: one trains AI models for detecting advanced threats within hospital systems, and the other focuses on anomaly detection during patient transport, emphasising the secure handling of sensitive data. Together, these deployments and sub-pilots highlight CYLCOMED's commitment to bridging cutting-edge technology with real-world healthcare needs. The insights gained from Pilot 2 are

Funded by Horizon Europe Framework Programme of the European Union

expected to not only strengthen telemedicine security but also ensure the tools are practical and effective for everyday use in healthcare, setting a new standard for safety and efficiency.

Funded by Horizon Europe Framework Programme of the European Union

2 Activities for Pilot Studies

Summarise the preparatory work done in advance of the pilots; It includes efforts to integrate cybersecurity tools into medical devices and the steps taken to prepare for pilot execution. General description of Task 6.2 (integration of tools into MDs) and Task 6.3 (validation of tools in the scenarios) is reported here.

2.1 Task 6.2: Integration and technical aspects

This task focuses on implementing the project pilots, which involves developing end-user applications and integrating them with the CYLCOMED toolbox components. The process will occur in two phases: during the first round, the initial solution will be evaluated by stakeholders and the technical team. Feedback from this evaluation will then be used to refine and enhance the solution in the second round.

The CYLCOMED Toolbox development and integration is progressing as planned. The individual tools, such as LADS, LOMOS, LuS4MED, and FE4MED, have undergone significant development milestones, ensuring they are ready for deployment and integration into Pilot 1 and Pilot 2.

Each tool has been tested in isolated environments and validated for core functionality; to ensure a smooth deployment, several key agreements were established during the project General Assembly in March 2024:

- A dedicated machine or VM with internet access (via VPN or similar) has been configured for initial deployments.
- Deployment environments have been isolated from hospital networks to safeguard data and infrastructure integrity.
- Specific hardware (PCs with GPUs) has been provisioned for hospitals like OPBG and FHUNJ to support model training for tools like LADS and LOMOS using hospital-specific datasets.

Additionally, testing phases have been defined and are being followed systematically.

Initial virtual environments (Phase 1) are completed, and hospital deployments (Phase 1.1) is underway for Pilot 2.

Hospital stakeholders, not only clinicians but also IT specialists and clinical engineers, had a crucial and propositive role in adapting and preparing the CYLCOMED Toolbox for the deployment.

During the WP5 weekly meetings, hospital partners actively participated in discussions and decision-making processes regarding the integration and development of the toolbox. Their feedback has been invaluable in shaping the following adaptations:

- *Hardware*: Dedicated PCs and servers have been provided to ensure the seamless deployment of the toolbox within each hospital's premises.
- *Deployment Protocols*: Tools must be installed in isolated and secure environments to minimise risks and ensure data integrity.
- *Monitoring* and Maintenance: Hospitals have committed to assigning dedicated personnel to oversee the tools, monitor their performance, and report any issues to technical partners such as MCI and the respective tool developers.

At the moment of the report, all the tools have all been released in their first version.

Funded by Horizon Europe Framework Programme of the European Union

2.1.1 CYLCOMED Toolbox: software tools status

This section presents an overview of the tools developed during CYLCOMED and the current status, providing context for the tools purpose and its readiness to be used in the pilots.

LOg MOnitoring System (LOMOS)

Description and main functionalities:

Log Monitoring System (LOMOS) is harnessing state-of-the-art Natural Language Processing (NLP) architectures to detect anomalies in system and application logs that could indicate a security threat.

Traditional log monitoring solutions often depend on rule-based (manual) analysis of time series data. In contrast, LOMOS utilises advanced Natural Language Processing architectures to model log streams and understand their typical operating conditions. This enables the creation of a monitoring system that doesn't rely on manually defined rules or human intervention, but instead uses a behavioural model to automatically identify deviations that suggest abnormal situations, such as potential security threats.

Our method automatically examines system or application logs, providing valuable insights into the current and past status of monitored assets. It uses deep learning methods, such as Mask Language Modelling, common in self-supervised NLP, and Hypersphere Volume Minimization, mapping normal samples to their representations. These approaches are used in LOMOS to calculates anomaly scores for sequences of log templates, using NLP models for the IDs linked to these templates. LOMOS does not rely on manual pre-processing of raw logs from unstructured data and aims to identify patterns in logs and anomalous behaviour.

Current status:

At present, LOMOS is fully developed and ready for deployment in the first round of pilot validation. It has already been integrated with LADS, a network anomaly detection system, as both systems use the same data source and type (logs from pilot applications). In the first round of pilot validation, LOMOS will be deployed within the hospital environments to validate its functionality in relevant scenarios.

Challenges faced during the development and deployment:

Primary challenges during the development were the identification and preparation of suitable data for AI model training. In this phase, we used synthetic data from Amazon Web Services (AWS) as a provider of cloud services for Pilot 2. To provide the necessary model accuracy, reliability and trustworthiness in the relevant environment, it would be necessary to retrain the model using the pilot application deployed in the hospital premises which entails adhering to the hospital's Clinical protocol with its security measures (limited access to the machine where the pilot application is deployed). MCI as the Pilot 2 owner will provide the necessary support in accessing the application and setting up training and inferencing processes.

The activities for the Pilot 1 were also focused on the log preparation and identification of potential anomalies, specifically for IAM components (LuS4MED and FE4MED) used in this pilot.

Live Anomaly Detection System (LADS)

Description and main functionalities:

The Live Anomaly Detection System (LADS) is a state-of-the-art AI-powered solution designed to monitor and analyse network traffic in real-time, identifying potential anomalies that could signal cyberattacks or network malfunctions. As part of the CYLCOMED toolbox, LADS is

Funded by Horizon Europe Framework Programme of the European Union

responsible for providing robust anomaly detection capabilities that support the overall security of connected medical devices (CMDs) and their associated infrastructure.

- *Real-Time Anomaly Detection*: Identifies deviations from normal network behaviour to highlight potential cyber threats or issues.
- *Explainability*: Provides insights into the detected anomalies, helping to understand the root cause of unusual behaviour.
- *Integration with Other Tools*: Works in tandem with other CYLCOMED components, such as LOMOS, to enhance the overall cybersecurity posture.
- *Scalable Deployment*: Can be deployed in diverse environments, including hospital premises, leveraging Docker and Kubernetes for scalability.

Current status:

LADS is fully developed and ready for deployment in the first round of pilots. It has already been integrated with LOMOS, allowing both systems to collaborate in monitoring and analysing network logs and events. LADS will be deployed within the hospital environments during the first pilot phase to validate its functionality in real-world conditions.

Challenges faced during the development and deployment:

One of the primary challenges during LADS development was training the AI model using synthetic data. While effective for initial development, this approach may lead to detection issues in real-world environments where network traffic patterns differ. Retraining the model to improve accuracy could be logistically challenging, as the server hosting LADS will be deployed within hospital premises and subject to strict security protocols, limiting direct access.

To overcome this, MCI will support us during the pilots if needed. Their assistance ensures that updates to the AI model can be performed securely and efficiently without disrupting hospital operations, maintaining both system performance and operational integrity.

Connected Medical Devices and Services Management Tools

Description and main functionalities:

This component is tasked with minimising the attack surface in medical devices, and its innovation lies in establishing a secure channel between the OTA Mechanism Management Server, repositories hosting medical applications, and the target medical devices (Fleet of Medical Devices). Specifically, the OTA Mechanism Management Server conducts vulnerability scanning on application updates it receives, checking for security breaches in a passive device partition. If the application successfully passes the vulnerability scanning phase, it can then be deployed in the active device partition.

The main entities in the Architecture of OTA Mechanism are the following:

- Fleet of Medical Devices: Virtual or physical medical devices where the OTA Mechanism will establish a persistent communication with them.
- Mender Server: This is a microservices oriented solution which is being used to perform over the air updates. Key components of the Mender Server are the following microservices:
    - Messaging System: Internal messaging system used.
    - Storage: Object Storage to store artefacts.
    - Device Inventory: Service which manages list of devices.
    - Device Authentication: Service that manages the device authentication.
    - User Administration: User Administration, registration, and credentials. o API Gateway: Proxy Service.
- Workstation: It is the intermediate component that checks for application updates and generates application artefacts (is the generated package that contains the application

Funded by Horizon Europe Framework Programme of the European Union

updates and patches). The artefact is the Mender object which triggers the installation of new applications or the updates on existing applications to the fleet of devices.

Self-Sovereign Identity solution (Lus4MED)

Description and main functionalities:

The Lus4MED is a decentralised authentication solution based on Self-Sovereign Identity (SSI) where the user has the control over their data and identity credentials. In the context of the CYLCOMED project this solution is used to authenticate the user accessing the patients' data. LuS4MED comprise two components:

- The Agent for integrating the SSI technology with the Hospital Information System (the service provider) playing the roles of issuer (on behalf of the hospital) and verifier of the credentials.
- A Mobile App where the user stores the credentials issued by the Agent. This app facilitates the interaction of the user with the hospital front-end during the sign-up and login processes.

More technical details of this solution and the interaction with both pilots are provided in section 5.1 of D5.1 [1].

Challenges faced during the development and deployment:

The main challenge faced during the implementation and integration of this component is the different authorization solution used in each pilot. For pilot 1 the Agent needs to be integrated with the C-OPA (described below) an authorization component based on policies developed by Martel. In pilot 2 the integration is made with the MCI legacy system based on OpenID Connect. Also, it has been necessary for the LuS4MED adoption to the latest specifications. The final integration of this component with pilots is expected during the fourth quarter of 2024.

Authorisation solution C-OPA

Description and main functionalities:

This component acts as a proxy that sits in front of the FED4MED component. It is made of 3 elements:

1. *Envoy Proxy*: it takes the incoming requests, and either lets them through or rejects them after forwarding them first to OPA for evaluation.
2. *OPA*: It evaluates the requests against a series of security policies, written in a high-level declarative language called Rego. The current policies primarily check for two things: the validity of the JWT security token provided with the request, and whether the credentials provided permit the request (e.g. roles).
3. *Policy Store*: Where the policies are stored and pulled by OPA. Policies are generally bundled, and OPA is configured to pull them periodically.

Current status:

A web GUI is also being developed that could be used to write and bundle policies in a more structured manner.

Currently, the main development challenge is integrating with the FED4MED component, as well as the definition of the policies themselves, as it requires defining both the validation of the security tokens being sent alongside the requests as well as how roles and client IDs are reflected in the policies.

A full C-OPA implementation with basic policies are currently ready to be implemented and further developed within the pilots' more specific use cases.

Funded by Horizon Europe Framework Programme of the European Union

Data Protection solution (FE4MED)

Description and main functionalities:

The FE4MED component is a data encrypting solution for protecting data when shared and being stored. It is based on the cryptographic scheme Cyphertext-Policy Attribute-Based Encryption (CP-ABE). The patient data are encrypted using policies based on attributes. FE4MED provides a fine-grained access control over the data, which means that only those users holding the right attributes are able to decrypt the data.

Current status:

The FE4MED presents a modular architecture providing two main elements:

- The FE4MED server comprises 3 modules:
  - The Key generator module creates the key pair private and public keys, and the decryption key based on attributes.
  - The Decryptor module decrypts the data using the user specific decryption key.
  - The storing module for storing the keys in a Key vault and a DB for storing policies, attributes and configuration parameters.
- The encryptor module for encrypting patients' data. This module is provided in two versions:
  - A module provided as a docker image for being deployed on a Raspberry PI (RBPI), for encrypting data from the connected medical devices (CMDs), used in pilot 1.
  - An android library for being included into the mobile MCI Hub for encrypting data from the patients, used in Pilot 2.

A graphical user interface could be developed for configuration purposes, if needed.

More technical details of this solution and the interaction with both pilots are provided in section 5.3 of D5.1 [1].

Challenges faced during the development and deployment:

The main challenge faced during the development and integration of this components has been the fact that two different versions of the encryption module have been implemented for each pilot. Namely, a service to be deployed on the RBPI and an android mobile library for being used into the MCI Hub. Currently the FE4MED server and the encryptor module docker images have been integrated with the pilot 1 infrastructure managed by RGB. In the case of pilot two the integration process started with the FE4MED server, and the encryption android library has been delivered for complete the integration.

Connected Medical Device integrity

Description and main functionalities:

As stated in D6.1, section 2.2.3, Pilot 1 will challenge the CYLCOMED toolbox by extending the RGB's CMD without interfering with its certification.

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

- Table 5 of D6.1 provides a description of "to be integrated" CYLCOMED tools.
- With regards to licensing, in D7.3 in M18 RGB defines the exploitation strategy and current plans.

Security dashboard

Funded by Horizon Europe Framework Programme of the European Union

Description and main functionalities:

The CYLCOMED Security Dashboard serves as a centralised platform for collecting, correlating, and visualising security events and data generated by the CYLCOMED toolbox. Its primary purpose is to provide real-time situational awareness of threats, vulnerabilities, and calculated risk exposures associated with connected medical devices (CMDs). By integrating various tools within the CYLCOMED framework, the dashboard delivers a 360-degree view of cybersecurity, facilitating efficient decision-making for hospital IT and security teams.

- *Data Collection and Ingestion*: Collect security events, logs, and alerts from the various tools in the CYLCOMED toolbox, including LADS and LOMOS.
- *Data Analysis*: Analyze collected data to detect potential threats and calculate associated risk levels.
- *Visualisation*: Provide user-friendly visual representations of security metrics, detected threats, and actionable insights for hospital IT staff.
- *Alerting*: Generate real-time alerts and notifications when specific anomalies or risks are detected.
- *Integration*: Enable seamless interaction with other tools in the CYLCOMED framework for a cohesive cybersecurity ecosystem.

Current Status:

The development of the CYLCOMED Security Dashboard started in month 19 of the project. As of today (month 24), significant progress has been made:

- The design and architecture of the dashboard have been completed, incorporating modular and scalable principles to ensure seamless integration with the toolbox.
- A data persistence layer has been implemented to securely store events and alerts.
- Development of the data analysis and visualisation layers is underway, leveraging frameworks such as ELK Stack for real-time processing and visualisation.
- Initial API designs have been prepared to enable data ingestion from the tools.

Challenges faced during the development and deployment:

However, the dashboard is not yet ready for the first round of pilots. It is expected to be fully operational in time for the second round of pilots, and efforts are being made to accelerate progress to possibly make it available earlier.

While the individual development of the dashboard has progressed without significant challenges, the integration phase may encounter issues with inconsistent data formats. This challenge can be effectively addressed by defining a standard data schema (e.g., JSON) for all tools and providing transformation scripts or middleware to ensure alignment and compatibility of outputs.

2.1.2 CYLCOMED Toolbox: Risk management tool

The CYLCOMED risk management tool was designed taking into account the risk management frameworks most widely used in the industry, by the partners, and when considering connected medical devices. It was designed to be general enough to encompass emerging technologies, like 5G, Blockchain, Cloud services, Artificial Intelligence, and IoT, where the CMDs are included. It was also designed to enable the adoption of any benefit-risk scheme currently used in healthcare.

It currently supports four main roles:

1. *User Manager:* responsible for enrolling new members to access the risk management tool

Funded by Horizon Europe Framework Programme of the European Union

2. *Organization Manager:* responsible for creating standards and controls to be used to manage the risks
3. *Asset Manager:* responsible for creating assets and assigning vulnerabilities, threats and benefits to the assets
4. *Risk Manager:* responsible for creating the risks, performing risk analysis and evaluation, carrying out the benefit-risk analysis and assigning risk treatment

For each asset, a set of vulnerabilities and threats will be registered, and the risks will emerge from the combination of vulnerability-risk pairs. These risks will be evaluated following some criteria (to be determined during the pilots). Risks that are intolerable must undergo a benefit-risk analysis process, where the benefits of the CMD must be weighed against the risks. Then, an assessment of what controls should be implemented to mitigate the risks takes place, and it should mitigate them to an acceptable level, and the benefits must outweigh the risks.

In the scope of the CYLCOMED project, the assets to be considered are the connected devices and the controls will be the cybersecurity protections offered by the CYLCOMED Toolbox. The CYLCOMED Toolbox is a set of tools that will contribute to mitigate and/or eliminate risks, ideally enabling the CMDs to have the most benefits possible, while eliminating all the risks.

2.2 Task 6.3: Validation and pilots' management

This task focuses on validating the pilots through a step-by-step process. Validation will occur in multiple rounds to provide feedback and guidance for Task T6.2, ensuring the development aligns with stakeholder expectations. It takes a multidisciplinary approach, including hospital-based studies to confirm that Task T6.1's design is followed while addressing non-technical aspects such as societal, legal, economic, ethical, and practical considerations. For pilots involving sensitive data, publicly available or synthetic data may be used to maintain privacy standards while providing a real-like environment to evaluate the CYLCOMED toolbox.

Validation process (Task 6.3) is currently focusing on providing feedback to technical partners, through selected meetings and continuous discussions. The involvement of clinical partners is proving to be invaluable in understanding the capabilities of CYLCOMED in the real context, achieving not only a technical improvement but also maximizing the actual possibilities of exploiting these capabilities

The Pilots validation aims to ensure the CYLCOMED system complies with required specifications, standards, safety, performance, and regulatory requirements by conducting a thorough evaluation of both technical and non-technical aspects.

Technical Aspects

The technical validation focuses on:

- *System Functionality*: Ensuring the telemonitoring system and cybersecurity tools perform according to design specifications.
- *Integration*: Verifying seamless integration with hospital IT infrastructure and workflows.
- *Reliability and Performance*: Assessing stability, uptime, response times, and resilience under various conditions.
- *Interoperability*: Confirming compatibility with existing hospital systems, medical devices, and communication protocols.
- *Safety Compliance*: Ensuring adherence to clinical safety standards to mitigate risks for patients and staff.
- *Regulatory Compliance*: Validating alignment with local, national, and international medical device regulations.

Clinical and non-software aspects

Funded by Horizon Europe Framework Programme of the European Union

Non-technical validation encompasses:

- *Social Aspects*:
  - Stakeholder Impact: Evaluating the system's influence on workflows, relationships, and trust, particularly the doctor-patient relationship.
  - Adoption and Acceptance: Understanding perceptions and attitudes of staff and patients toward the system.
- *Legal Aspects*:
  - Data Privacy and Consent: Ensuring compliance with GDPR and other relevant data protection regulations.
  - Ethical Compliance: Addressing informed consent processes and ensuring equitable access.
- *Economic Aspects*:
  - Cost-Effectiveness: Assessing resource use and return on investment.
  - Budget Compliance: Ensuring alignment with hospital financial strategies.
- *Ethical Dimensions*:
  - Fairness and Inclusivity: Preventing disproportionate impacts on specific demographics.
  - Transparency: Clarifying data usage and decision-making processes.

Stakeholder-Centred and Questionnaire based approach: to address non-technical aspects, a targeted questionnaire method engages six key hospital stakeholders:

- *Clinicians*: Focus on data privacy, consent processes, and the doctor-patient relationship.
- *Supply Chain Managers*: Address challenges in procuring resources for research and innovation.
- *Cybersecurity Managers*: Oversee technical integration and procedural safeguards.
- Data Protection Officers: Ensure compliance with hospital data protection policies and regulatory frameworks.
- *Clinical Trial Center Staff*: Provide guidance on legal and ethical requirements for CYLCOMED implementation.
- *Clinical Engineers*: Evaluate the safety, functionality, and performance of the tools.

Comprehensive Assessment Goals

By involving these stakeholders, the validation ensures a holistic approach that extends beyond technical functionality to include social, legal, ethical, and economic factors. This ensures the CYLCOMED system is not only technically sound but also well-suited for real-world healthcare settings.

2.3 Pilot 1 - Hospital Equipment: activities performed

As indicated in section 4.1. and more specifically in subsection 4.1.1. of D5.4, the demonstrator under development consists of a HIL/SIL test bench platform that will support the control algorithm development and controller implementation. It will make use of specific tools provided by partners, in order to evaluate:

- the controller´s performance level regarding robustness of the controller in the presence of noise injection and different levels of patient's sensitivity to the drug
- the risks associated with the application and the components to be included to mitigate such risks, both from a safety as well as a security viewpoint.

The system includes the following HW components:

- the controller

Funded by Horizon Europe Framework Programme of the European Union

- the Infusion pump´s tree
- the PC software containing the patient model
- the HIL/SIL interface tool

Pilot status:

According to the CYLCOMED project proposal, this pilot is being carried out at laboratory level. Currently, the verification platform is under development. The latest works are related to the presentation of the backend App that mimics the Hospital Information System. Some cybersecurity tools have been integrated, and some others will be in the following weeks, as it is described in this same section. Once the integration is completed, the Verification Plan shall be executed as a test plan execution flow, that will consist of the following steps, as indicated in section 4:

- Test Plan, Test Case and Test Case parameters, which will be created in the Test Case Services Provider TCSP.
- HIL/SIL gets a Test Plan from the Requirements tool (e.g., functionality like IBM Rational Quality Manager). Every Test Plan consists of several Test Cases, every Test Case contains a set of different parameters.
- HIL execute sequentially all the Test Cases.
- HIL initiates the Neuromuscular Transmission –NMT- model developed, with a configuration file that contains the patient´s model set of parameters (e.g., change of patient's sensitivity to drug, or noise injection).
- The NMT patient´s model sends to the controller the value of the simulated NMT value.
- The Controller calculates the new relaxant dose value to inject and sends it to the Infusion pump and to the HIL Manager Tool.
- The HIL Manager Tool sends the dose to the NMT model that simulates the NMT reaction to the dose.
- This closed loop is one in sequence, for a predefined amount of time, e.g., 2 hours. When the test case finishes, the NMT model writes the result of the execution in a file that is read by the HIL software.

2.3.1 Details of integration (T6.2) in Pilot 1

Technical meetings have taken place on a regular basis in order to prepare the verification platform. Consistently with the state of the test bed, which is in a state of almost-readiness, the progress of the verification strategy is progressing successfully.

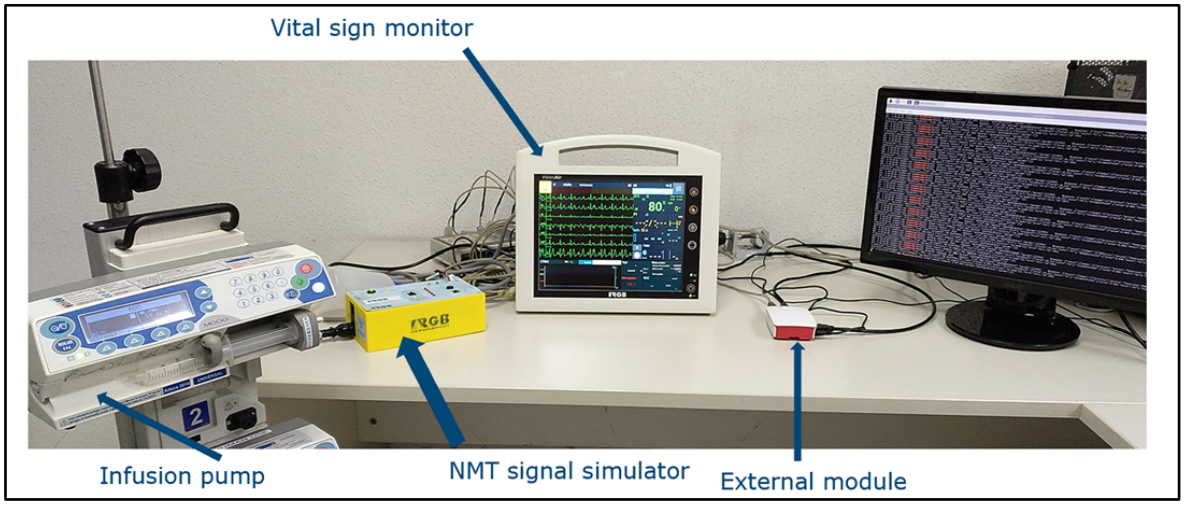

Figure 3: Pilot 1 Test Bench Platform

Funded by Horizon Europe Framework Programme of the European Union

As indicated in section 4.1 of D5.1, it is expected that when all the Test Cases finish their execution, HIL/SIL interface tool can upload the Test Results to the Test Case Service Tool (acting as a Quality Manager).

In order to make tests of different types of patients and trial configurations, a Test Case Manager has been developed that allows us to introduce variables such as gender, age, sensitivity to the drug, etc.

The Test Case Manager will statistically evaluate the time series of state variables outputs from the Patient Model. Special care is taken for moments when neuro-muscular blockade is less intense than required. Unexpected movements by the patients may interfere in the surgical process and must therefore be suppressed by providing an adequate level of NMT. A secondary goal is to minimise the total drug consumption of rocuronium, which beyond its economical relevance, it also may shorten the time needed for total recovery.

In addition, the Pilot 1 will integrate the SW components from other CYLCOMED partners on cybersecurity. RGB has studied the potential benefit of new support for V&V tasks related to safety analysis, specification quality analysis, traceability management, and compliance management. Although RGB successfully performs these activities nowadays, the use of different methods and tools could lead to, e.g., a higher efficiency.

Section 4 of Deliverable D3.1 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 in the Appendix C in D3.1.

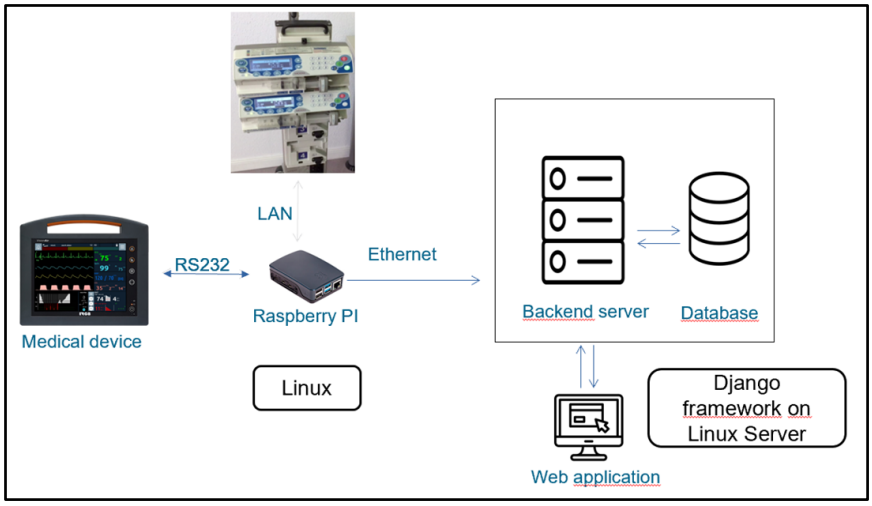

Figure 4: Pilot 1 Architecture

2.3.2 Software Tools integration in Pilot 1

In this section, the integration status of each individual tool utilized in pilot 1 is described.

Live Anomaly Detection System (LADS) and Log Monitoring System (LOMOS)

The integration of LADS and LOMOS into RGB's Pilot 1 is currently underway. A series of meetings have been held between the key stakeholders (RGB, EVIDEN, XLAB) to establish a timeline that facilitates the integration of LADS and LOMOS into Pilot 1 as quickly as possible. During these discussions, the structure of the pilot's deployment was also defined, following a hybrid approach. Since Pilot 1 operates within a laboratory environment, it does not involve the use of real data or deployment within critical infrastructures (such as hospitals), which simplifies the deployment process and enables subsequent monitoring and improvements to LADS and LOMOS within the Pilot 1 environment.

Funded by Horizon Europe Framework Programme of the European Union

As planned, LADS will be deployed as a service that analyses network traffic entering through RGB's backend server into the internal network. Additionally, it will monitor traffic originating from the internally deployed Raspberry Pi. The results generated by LADS will then be sent to the CYLCOMED Dashboard, where they will be displayed alongside outputs from other tools deployed in the pilot.

Regarding LOMOS, the plan is that LOMOS will consume system and application logs coming from the RGB's backend server. As this server doesn't have the necessary hardware capability to train the LOMOS model (it lacks powerful GPU), LOMOS will be deployed at XLAB premises, and a secure connection will be established to the server to transfer logs (using Filebeat) from the server to the LOMOS Elasticsearch database at XLAB. Similar to LADS, the inferencing results generated by LOMOS will then be sent to the CYLCOMED Dashboard, where they will be displayed alongside outputs from other tools deployed in the pilot.

Connected Medical Devices and Services Management Tools

In this Pilot, the OTA Mechanism component is responsible for deploying the RGB applications to target medical devices. RGB Medical devices are RPI4 devices and our tool is fully compatible with this type of devices.

Until now we have installed the OTA Mechanism in two dedicated instances, first instance for the Mender Server that manages the connections with the devices, application artefacts and deployments to target devices.

The Artefact generation that takes docker compose files and transform them to artefacts (files ending in .mender format). We have tested the RGB apps' fresh installation to more than one RGB devices and the RGB apps updates, from v1 to v2, to the same devices.

Self-Sovereign Identity solution Lus4MED

The first release of the LuS4MED component has been delivered for starting integration in this pilot. The Agent is provided as a docker image, to be deployed on the hospital infrastructure. The integration of this component is different depending on the pilot. In this particular case, the LuS4MED will be integrated with the C-OPA authorization solution (described next) into the Hospital Information (HIS) System created by RGB. Several meetings have been scheduled for exchanging information and agreeing on the integration process. Detailed specifications for interacting with the LuS4MED Agent are being provided to RGB as front-end developer of the HIS infrastructure, in order to interact with the LuS4MED component. Also, these specifications are being delivered to Martel as implementer of the C-OPA authorization solution for the interaction with the LuS4MED Agent. The finalisation of the full integration will be performed during the last quarter of 2024.

Authorisation solution C-OPA

C-OPA is currently capable of taking requests towards the FED4MED service and processing some basic policies that check for the validity of a JWT token, and the presence of some simple defined "roles" within the token. Full integration with more defined policies is underway.

Data Protection solution FE4MED

Regarding the integration with pilot 1, several releases of the FE4MED server and the Encryptor module have been delivered, deployed, tested and integrated with the infrastructure created by RGB. The Encryptor module has been deployed on the RBPI encrypting the patients' data collected from the connected medical devices. The process of encryption in the RBPI and decryption on the RGB infrastructure have been completed and tested successfully, with a smooth collaboration between both partners ATOS and RGB. Several face-to-face and online meetings have been scheduled, where ATOS presented to RGB the functionalities of the FE4MED tool and suggest a JSON structure of the data to be encrypted, and to share the

Funded by Horizon Europe Framework Programme of the European Union

specifications (Rest API) provided by the FE4MED server and the Encryptor module. The integration process was developed in two phases:

- Deployment of the Encryptor module in the RBPI and deployment of the abe-toolbox service (the service containing the basic functionalities of the FE4MED server) for testing the complete encryption/decryption processes.
- Deployment of the FE4MED server on the HIS infrastructure for completing the integration with the front-end and back-end of the HIS system.

During this integration process some minor bugs have been detected and fixed. An additional FE4MED server endpoint was requested to implement, for deleting policies.

Connected Medical Device integrity [RGB]

Besides the integration of Cybersecurity SW components, already mentioned in this section, the external module includes functional requirements that are in an advanced stage of development.

In particular:

- User interface including controller functionalities
- Communication protocol to incorporate new required information such as alarms
- Alarms management
- Connectivity to Infusion pump tree as an external OEM component
- Connectivity to backend server

CYLCOMED security dashboard

As mentioned in the previous section, the Dashboard is currently in the development phase and is about to begin integration with other tools. However, similar to LADS, the Dashboard will be deployed as a service, receiving results from the tools deployed in Pilot 1 on an external server. This approach simplifies the management and updating of the system, ensuring efficient and streamlined operation.

2.3.3 Risk assessment tool in Pilot 1

In Pilot 1, the risk management tool will be used to document the risk analysis, evaluation and controls implemented to mitigate the risk of the NMT signal simulator, external module, infusion pump and vital sign monitor. These elements will be documented as assets in the RMT and the vulnerabilities, threats, risks definition, evaluation and controls for mitigation will be documented in the RMT. The benefit-risk analysis will be performed, with an appropriate Benefit-risk evaluation method. According to MDR and ISO 14971, the residual risks that have unacceptable levels must be mitigated, reducing the risks to acceptable levels. These controls can come from the CYLCOMED Toolbox, but it is not limited to it, as some controls might include design changes, blocking USB ports, etc.

2.3.4 Details of Validation (T6.3) in Pilot 1

Most of the validation process that has currently been done, focuses on the technical aspects.

Specifically, the first need is to set up an automated test bench platform where we can perform a large number of automated tests. The modules within the simulation infrastructure are the following:

- Test Case Manager (TCM)
- Rocuronium Controller (CNT)

Funded by Horizon Europe Framework Programme of the European Union

- Patient Model for Rocuronium (PATMOD)
- Infusion pumps (PUMP)
- NMT (NeuroMuscular Transmission) TOF/PTC Sensor (SENSOR)

These modules are provided by RGB, and they interoperate using a protocol constructed on the designated platform REDIS using REDIS database for message broadcasting as well as data storage capabilities.

The experimental test bench was intended to work in two main regimes:

- fully simulated - all participants are simulated, including CNT
- hardware in the loop - CNT is real, Pumps&Sensors are optionally real or simulated

TCM implementation purposes are to:

- maintain library of defined test cases
- perform automated testing, i.e. run simulation experiments
- summarise experiments and test cases (store outputs in any technical way files, databases and output statistical results from the experiments)

The non-technical validation for this pilot is currently being taken care through interaction with FHUNJ; although Pilot 1 is not going to be tested on real patients, RGB's basic medical device is going to start being certified at the Niño Jesús hospital and that is why the hospital's anesthesiologists are closely following the development that CYLCOMED is adding to the device to analyse how it can improve the device's cybersecurity in the operating room.

2.4 Pilot 2 – Telemonitoring platform: activities performed

This section describes the used medical device, the goals of the pilot, and the preparatory activities conducted to set up the pilot.

2.4.1 Details of integration (T6.2) in Pilot 2

During the initial phase of the CYLCOMED pilots, OPBG has overseen the implementation of the virtual clinic and the integration of the CYLCOMED Toolbox on-site. This phase was influenced by recent amendments to national legislation, which imposed more stringent requirements for ethical oversight and redefined the classification of systems comprising medical devices and associated digital monitoring platforms. The updated regulatory framework necessitated a comprehensive reassessment of the CYLCOMED Toolbox and monitoring devices as an integrated "system," with particular emphasis on their combined functionality and compliance with ethical, privacy, and legal standards. To address these complexities, OPBG engaged in interdisciplinary consultations with experts in ethics, law, and data privacy to refine the study objectives and align them with the revised legislative definitions. Subsequently, the team systematically updated key study documents, including the protocol, informed consent forms, and economic feasibility analyses, ensuring compliance with the enhanced requirements.

Following rigorous preparation, OPBG submitted the revised documentation to the Territorial Ethical Committee (Comitato Etico Territoriale, CET). Despite the heightened complexity resulting from the regulatory updates, the CET approved the on-site implementation of both the CYLCOMED Toolbox integrated platform and the associated monitoring devices. This regulatory approval represented a critical milestone, facilitating the practical deployment of the virtual clinic and advancing the CYLCOMED pilot toward its operational phase.

Funded by Horizon Europe Framework Programme of the European Union

In parallel with these preparatory activities, OPBG conducted a patient screening process to plan the enrollment of participants in the initial validation phase of the pilot. The inclusion of these patients enables OPBG to identify key blockers of clinical implementation of cybersecurity tools at point-of-care, validate the system's functional and operational parameters within a controlled clinical environment, offering critical insights into its efficacy, safety, and alignment with stakeholder expectations. Data management flow, and clinical operation has been implemented and processed as a clinical trial in Good Clinical Practice (GCP), with a focus on quality improvement of care and feasibility, therefore adhering to the highest scientific and regulatory standards while ensuring the pilot's translational relevance.

Pilot 2 Virtual Machine pilot status

During the initial stages of Pilot 2, MCI set up a virtual machine in its development environment dedicated to the technical partners in order to host and test CYLCOMED's tools before their deployment in hospital premises.

In addition to the virtual machine, a shared repository was established on the GitHub platform to simplify the version control and file sharing.

The virtual machine was shared to the various partners through a dedicated VPN. Furthermore, the use of a virtual machine allowed for a clearer definition of the supportive/necessary elements for the different tools (third-party software, libraries, etc.), thus creating a clean procedure to configure the definitive environment used in hospitals.

The majority of the tools have been tested and are ready for installation on the servers destined for hospitals (Lomos, Lads, Fe4Med, Lus4Med). The maintenance of the virtual machine is scheduled towards the end of the project to allow the potential modifications/updates to the tools or validation of the Dashboard.

Pilot 2: Hospital deployment status

The servers dedicated for the hospitals' pilots have been configured according to the installation procedure based on the requirements identified during the activities carried out on the virtual machine shared by the partners.

MCI has started the installation of the final version of each tool into the different servers and it has tested the overall configuration.

MCI has also collaborated with the information systems of each hospital to configure essential network aspects, such as the use of VPN and DNS.

Activities related to Pilot 2, conducted in recent months, focused on verifying the project's ethical, privacy, and engineering requirements and on achieving an ethics committee approval. Key milestones included obtaining approval from the territorial ethics committee, finalising contracts between the hospital and technical partners, setting up the telemonitoring platform and cybersecurity toolbox, and organising patient enrolment logistics. The telemonitoring phase is scheduled to begin in the last week of November 2024.

More in detail: The engineering, privacy, and ethical requirements for the project were thoroughly reviewed in collaboration with relevant stakeholders at OPBG. In parallel, a comprehensive data flow and associated data management plan were established to ensure proper handling and protection of patient information throughout the project.

A detailed protocol was drafted, shared with all involved stakeholders, and reviewed multiple times to ensure its alignment with regulatory standards. This process was followed by the preparation of additional documentation required for submission to the ethics committee. After submitting the protocol in June 2024, three rounds of revisions were requested by the committee before final approval was granted on the 24th September 2024.

Funded by Horizon Europe Framework Programme of the European Union

Following the approval, a formal notification of study initiation was sent to the Ministry of Health, ensuring compliance with all legal and regulatory obligations.

In addition, all contracts with technical partners - namely XLAB and MCI - were drafted, reviewed, and signed, formalising the collaboration for the technical execution of the project.

As part of the preparations, the engineering requirements for the telemonitoring devices were thoroughly evaluated to ensure they met the necessary standards. Additionally, logistics related to patient enrolment and management of the telemonitoring devices were successfully set up, laying the groundwork for the upcoming telemonitoring phase.

2.4.2 Software tools integration in Pilot 2

In this section, the integration status of each individual tool utilized in pilot 2 is described.

Live Anomaly Detection System (LADS) and Log Monitoring System (LOMOS)

As detailed in Section 2.1.1 of this document, LADS and LOMOS are fully prepared for deployment and use in the Pilot 2 environment. The integration and deployment process followed the approach outlined during a General Assembly held in Rome, where it was decided to initially deploy the tools in a virtual environment managed by MCI.

This allowed for the integration process to address and resolve most challenges prior to deploying the tools on the servers that will be installed inside the hospitals.

In this controlled virtual environment, LADS and LOMOS were successfully deployed and tested over several months, demonstrating their functionality and effectiveness during the first project period review. Currently, LADS and LOMOS are ready and awaiting local deployment in the hospitals once the first round of the pilot begins.

As noted in the previous section, the primary challenge faced is the remote management of the service, necessary for the effective control over AI model training and inferencing. However, thanks to the support and collaboration of MCI, we are confident this issue will be effectively mitigated without major difficulties.

Connected Medical Devices and Services Management Tools

The Over The Air (OTA) update mechanism is a tool dedicated for embedded medical devices, since pilot 2 does not include any sensor capable of OTA updates this tool will not be demonstrated (please refer to Pilot 1 if interested in investigating how the consortium is planning its evaluation).

Self-Sovereign Identity solution Lus4MED

A first release of the LuS4MED component has been delivered for starting integration into this pilot. The Agent is provided as a docker image, to be deployed on the MHP infrastructure. The integration of this component is different depending on the pilot. In this particular case, the LuS4MED will be integrated with the authorization legacy system (based on OpenID Connect) into the MHP. Several meetings have been scheduled for exchanging information and agree the integration process. Detailed specifications for interacting with the LuS4MED Agent are being provided to MCI as front-end developer of the MHP infrastructure, in order to interact with the LuS4MED component. Also, these specifications are being delivered to MCI as manager of the authorization solution for the interaction with the LuS4MED Agent. MCI started to deploy the LuS4MED in their infrastructure for starting the initial tests. The finalisation of the full integration will be performed during the last quarter of 2024.

Data Protection solution FE4MED

Funded by Horizon Europe Framework Programme of the European Union

With respect to the integration in Pilot 2, the last version of the FE4MED server is being used for the integration into the MCI Health Platform (MHP). The mobile encryption module has been finalised and tested on ATOS infrastructure. This module is provided as an android library to be integrated into the MCI Hub, the mobile phone provided to the patient's environment. Several online meetings have been scheduled, where ATOS presented to MCI the functionalities of the FE4MED tool and suggested a JSON structure of the data to be encrypted, and to share the specifications (Rest API) provided by the FE4MED server and the Encryption module.

The integration process is planned in two phases:

1. Deployment of the FE4MED server and the Encryptor module service used for pilot 1 (bear in mind that the two flavours of encrypting module provide the same endpoints and functionalities) on the MHP for testing the complete process of encryption and decryption, with the aim to avoid additional delays during the integration between the different components.
2. Include the encryption android library into the MCI Hub and test the encryption of the patient's data. This step will be performed during the last quarter of 2024.

The main challenge to be faced during the integration of this component will be the use of the new encryption android mobile module. In this regard, ATOS is providing information for using the library, namely, how to add this library to the project and an example of a call to the library.

CYLCOMED security dashboard

As outlined in previous sections, the CYLCOMED Dashboard is currently in its development phase, nearing readiness for integration with other tools. Like the approach taken with LADS, the Dashboard's deployment strategy involves leveraging a virtual environment managed by MCI for its initial integration and testing. This allows for a controlled environment where challenges can be identified and addressed before moving to the more complex deployment scenario within hospital infrastructures.

While the Dashboard is not yet fully integrated or deployed, we are confident it will be ready (as is established within the project GANTT) in time for the second round of pilots, providing essential functionalities for comprehensive threat analysis and management.

2.4.3 Risk assessment tool in Pilot 2

The feedback gathered during the initial design of the risk assessment tool, and the demo phase, particularly from OPBG's ethical, legal, and clinical experts, significantly influenced the refinement of the tool. By addressing the regulatory redefinition of a "system" as both a medical device and its associated digital platform, the development team was compelled to reevaluate the tool's integration, data processing workflows, and compliance with privacy laws.

This required enhancements in the Risk assessment tool's algorithm to account for modular functionalities that could operate within stricter data privacy frameworks, ensuring scalability and adaptability. The interdisciplinary discussions also helped identify gaps in the user experience and data handling, driving iterations that better aligned the tool with clinical workflows and patient safety standards.

Deployment Model	Advantages	Challenges
On-Premises Deployment	Enhanced control over sensitive patient data, crucial for compliance with stringent privacy laws.	High initial costs for hardware and ongoing maintenance.

Funded by Horizon Europe Framework Programme of the European Union

	Customizable to align with specific hospital IT infrastructures.	Resource-intensive, requiring in-house IT expertise.
	Reduced latency for real-time monitoring and decision support.	Limited scalability compared to cloud-based solutions.
Cloud-Based Deployment	Scalability to manage growing patient volumes and larger datasets	Potential vulnerabilities in data security and compliance with privacy regulations.
	Lower upfront costs and reduced reliance on local IT infrastructure	Dependence on internet connectivity, which may impact reliability.
	Easier integration with other digital tools and external datasets	Perceived lack of control over data storage and processing location

Table 1: Advantages and Challenges in different deployment

Based on our findings, the decision to maintain an on-premises deployment ultimately depends on balancing privacy concerns, operational needs, and cost-efficiency. For institutions like OPBG, where the sensitivity of patient data is paramount, on-premises deployment may provide superior control and compliance with legal standards. Furthermore, the ability to optimise latency and tailor the system to specific clinical workflows offers tangible benefits in high-stakes environments like virtual clinics.

However, if future iterations of the toolbox emphasise scalability and interoperability across multiple sites or if data privacy laws evolve to support hybrid or secure cloud solutions, transitioning to a cloud-based infrastructure may provide a more sustainable path forward. A detailed cost-benefit analysis and long-term strategic goals should guide the final decision, ensuring that the deployment of our cybersecurity model aligns with both clinical and regulatory priorities.

Moreover, the risk management tool, together with the benefit-risk scheme, enables the evaluation, in a single platform, of several categories of risks, e.g., cybersecurity, privacy, interoperability and performance risks. It can also address the compliance with standards and regulations, like the ISO 27001, GDPR, MDR/IVDR among others. The benefit-risk scheme enables the comparison between the benefits and risks of on premise and cloud deployment of tools. The generalisation made to the benefit-risk scheme enables the evaluation of the benefits and risks of, not only therapeutics, but also to include other aspects of the solution, such as connection to the cloud, type of deployment, existing controls, and so on.

2.4.4 Details of Validation (T6.3) in Pilot 2

The CYLCOMED validation framework is designed to take a comprehensive approach, bringing in a wide range of stakeholders to help refine the telemonitoring system. Its main goal is to ensure sensitive patient data is well-protected while meeting all relevant data protection and cybersecurity standards. To do this, the process actively involves clinicians, nurses, IT staff, patients, and administrators to understand how the system impacts daily workflows and overall patient care. By comparing their experiences before and after the system is implemented, the team can pinpoint areas for improvement and develop practical guidelines for introducing similar technologies in other hospitals.

A big part of the process involves semi-structured interviews. These conversations happen in two stages: first, to hear stakeholders' expectations and concerns before the system is deployed, and later, to gather feedback on how it worked, what challenges came up, and what

Funded by Horizon Europe Framework Programme of the European Union

benefits it brought. Participants include experts like cybersecurity specialists, clinical engineers, and data protection officers.

The feedback collected is analysed with a focus on cybersecurity, ethics, clinical workflows, and compliance. This helps fine-tune the system's risk prediction tool while addressing real-world issues. The ultimate aim is to create a solution that's practical, secure, and fits seamlessly into healthcare environments.

Funded by Horizon Europe Framework Programme of the European Union

3 Challenges and Lessons learnt

The lessons learned from the CYLCOMED project offer valuable insights into the challenges and innovations that come with introducing advanced cybersecurity and telemonitoring systems into healthcare. With regulations constantly changing and patient data needing the highest level of protection, these pilot projects highlight both the obstacles and the opportunities that arise when trying to integrate new technologies into healthcare.

They emphasise the need for close collaboration between different fields of expertise, the ability to adapt to evolving legal requirements, and the importance of involving all relevant stakeholders from the start. In this section, we reflect on the hurdles faced during the development and testing of these systems, sharing insights that could help guide future projects. We also touch on key issues like ethics, data privacy, and the complexities of merging medical technology with everyday healthcare practices. By learning from these experiences, we hope to provide a roadmap for others looking to take on similar projects, pointing out the challenges to expect and the strategies that can help overcome them.

The main challenge faced during the development and integration of LADS was the initial training used synthetic data, which may not fully reflect real-world network conditions and potentially affect detection accuracy. Additionally, since LADS is deployed within hospital premises with strict security protocols, accessing the system for retraining is logistically complex.

Similarly, LuS4MED (Self-Sovereign Identity Solution) encountered challenges adapting to different authorization systems in the pilots: C-OPA for Pilot 1 and MCI's legacy OpenID Connect for Pilot 2. Adjustments to integrate LuS4MED with both environments required additional development and testing efforts.

For FE4MED (Data Protection Solution), the need to develop two distinct encryption modules—one for Raspberry Pi in Pilot 1 and an Android library for Pilot 2—introduced complexity. Each module had to be tested and deployed separately for its respective infrastructure, and additional features like a delete policy endpoint were implemented during integration.

Despite these challenges, all tools have progressed significantly, with functionality demonstrated in testing environments, and are on track for full integration during the pilots.

3.1 Main challenges faced in Pilot 1 implementation

The pilot will evaluate the degree of compliance to requirements from a functionality point of view, when cybersecurity tools are integrated. Therefore, in accordance with section 2.2.2. of D6.1, test cases will be carried out to verify that the incorporation of non functional SW components do not alter the correct operation of the medical system.

3.2 Main challenges faced in Pilot 2 implementation

The CYLCOMED project is a unique clinical study, characterised by high complexity and innovative elements. It focuses on a vulnerable patient population, increasing the need for careful ethical oversight. The study involves the integration of a high number of medical devices, requiring extensive validation and ensuring smooth interoperability in a clinical setting. Additionally, artificial intelligence is used to manage and analyse data, adding complexity in terms of data processing and transparency. The project also includes a robust cybersecurity toolbox to protect sensitive patient information, demanding thorough assessments for privacy

Funded by Horizon Europe Framework Programme of the European Union

compliance. These combined factors have intensified scrutiny from regulatory bodies and ethics committees.

3.2.1 Clinical protocol approval

Here follows a list of the different processes that implied an extension of the time needed to achieve expected results.

- Establishment of data flow and related data management plan.
- Protocol drafted, shared, and reviewed, along with additional documents required for submission to the ethics committee, such as the informed consent form, data management plan, protocol synopsis, list of all manual medical devices, and medical device notification by the Ministry of Health, and others.
- DPIA (Data Protection Impact Assessment) process initiated to evaluate the innovative aspects of the cybersecurity toolbox. The first step was to determine how many DPIAs were necessary for this trial, considering the use of six tools. The responsibility for this task and the subsequent analysis were clearly defined. In conclusion, a mandatory DPIA was deemed necessary.
- Internal feasibility assessment at OPBG: In this step, we evaluated the feasibility of conducting the study at the hospital, considering aspects such as integration in the clinical routine, management, space, staff, technology, and other resources.
- Update of national regulations for clinical trial submission: The changes in national regulations required modifications to the documents submitted and to the Ethics Committee process.
- Submission to the ethics committee: Three rounds of revisions were requested by the ethics committee, and the protocol was finally approved in September 2024.
- Notification of study initiation sent to the Ministry of Health, including the production and completion of all required documentation and oversight by the responsible staff for this submission.
- All contracts with technical partners (XLAB and MCI) required to be drafted, reviewed, and signed.
- Evaluation of the engineering requirements of the telemonitoring device: During the study, the CE certification of the device expired. It was necessary to contact each medical device manufacturer to obtain updated certifications.
- Set-up of patient enrolment logistics and telemonitoring device management.

3.3 Legal and ethical considerations

Regulating cybersecurity, especially in the context of medical devices, is a complex challenge due to the specialised and fragmented nature of the legal framework [2] . The complexity of cybersecurity technology, such as the proposed CYLCOMED technology, arises from the intersection of various EU legislative frameworks and their potential applicability. Consequently, this complexity is compounded by the need to navigate both medical device regulations and cybersecurity laws [3] . When it comes to the legal requirements for the cybersecurity of medical devices, the EU laws establish a set of different requirements enshrined in the Medical Devices Regulation (MDR), In vitro Diagnostic Medical Devices (IVDR), the Cybersecurity Act (CSA), the Network and Information Systems Directive (NIS2), the General Data Protection Regulation (GDPR), the Radio Equipment Directive (RED) and recently adopted Artificial Intelligence Act (AI Act). The EU cybersecurity landscape evolves at a fast pace. While medical device stakeholders operate in an already complex legal environment, new legislative initiatives bring additional layers of complexity and uncertainty. The proper guidance is essential to facilitate compliance with numerous legal requirements scattered across various regulations. However, as these legal acts have been extensively

Funded by Horizon Europe Framework Programme of the European Union

discussed in the D2.2 Examination of Ethical, Legal and Data Protection Requirements, they will not be subject to further analysis in this deliverable.

Next, CYLCOMED pilot 2 encompasses the real-world deployment in the form of an observational clinical study within existing hospital ecosystems, providing the integration of CYLCOMED tools. It will include the participation of paediatric patients with heart failure. It is an established fact that clinical research involving children and young people, ranging from newborn babies to adolescents, has always been perceived as highly challenging, both from ethical and practical standpoints. While remote monitoring technologies, such as telemedicine, present exciting prospects for clinical research, their adoption also introduces novel ethical considerations. The most prominent among these are concerns surrounding privacy and data security. As digital technologies capture and transmit sensitive health-related data, ensuring the confidentiality and integrity of participants#39; information becomes paramount. Children constitute a vulnerable population, and they need special protection when included in clinical research settings. Since children are considered incapable of giving informed consent to participate in research, their assent is regarded as the main ethical requirement defined by the many international documents addressing children's participation in clinical research.

Minors' right to freely express their views is well-established in documents like the UN Convention on the Rights of the Child and the Charter of Fundamental Rights of the European Union. This right is further echoed by international ethical guidelines such as the Declaration of Helsinki, the ICH E6 Good Clinical Practice guideline, and the Council for International Organizations of Medical Sciences CIOMS guidelines, which are often referenced in clinical research protocols. As a result, clinical research protocols emphasise adherence to these ethical principles. However, since these guidelines vary significantly in their content, focus, and requirements, implementing assent in practice becomes complex, leaving ample room for varied interpretations and challenges.

For instance, there is no universally accepted definition of assent. It has different meanings to different people. Surprisingly, none of the ethical guidelines mentioned above provide a definition of assent, leaving the term vague and open to various interpretations. Even scholarly literature rarely attempts to define the assent. Unlike informed consent, which is well-defined in ethical documents, the specifics of what information should be conveyed to children are less clear. None of the ethical documents above provide guidelines on which amount of information should be provided to children and in which ways. The ethical and practical challenges of obtaining assent in clinical research are multifaceted, requiring careful consideration and adherence to established ethical frameworks. While international ethical guidelines strongly advocate for children's assent in clinical research, the lack of a standardised definition and practical framework makes its implementation challenging. [4] The ethical challenges related to the assent are examined in the D2.2 Examination of Ethical, Legal and Data Protection Requirements, and they will not be subject to further analysis in this deliverable.

Funded by Horizon Europe Framework Programme of the European Union

4 Next steps and Conclusions

The upcoming activities for each of the two pilots will be briefly described below.

4.1 Next activities for Pilot 1

Pilot 1 will challenge the CYLCOMED toolbox by extending the RGB's CMD without interfering with its certification.
Clinician involvement and interaction will be essential in the following steps to collect their feedback.
To do so the CMD will interact with CYLCOMED tools through a single board computer, which is the main objective of the connected medical device integrity solution . It will be the core of Pilot 1 around which the other tools will provide their benefits. At the same time, in the upcoming steps, technical validations and feedback will be carried out on the behavior of various tools in a real-world environment.
For this purpose, a simulator of the clinical conditions has been implemented, to study how a parameter influences the control, the scripts that contain the variations of said parameter are grouped in a batch. There are already some functional requirements that will need to be tested, in order to verify that the incorporation of the security SW components does not compromise the essential clinical functionalities of the infusion controller.
For this purpose, we will be using a script file, that will allow to be configured both the patient's characteristics (weight, volume of distribution Vd, EC50 sensitivity to the drug...) and the control characteristics (initial dose, NMT target, duration...).
Additional work is the improvement of the interface at the desktop of the medical profile as well as necessary changes in the back-end server.

4.2 Next activities for Pilot 2

Once all the necessary approvals from the relevant authorities have been secured, the Pilot 2 can move on to the next stage: installing the entire system in the hospital. This phase involves setting up the telemonitoring devices, data management software, and cybersecurity measures to ensure that everything functions smoothly and securely. After the installation, the next step is to conduct a system test, where each part of the setup is carefully checked to make sure it works correctly and is safe for use with patients. Following the successful testing, the study officially begins with the Site Initiation Visit (SIV). This meeting is crucial because it brings together all the staff involved - doctors, nurses, technicians, and company partners - to provide training and guidance. During the SIV, everyone learns how to use the different platforms, manage the devices, and monitor patient data effectively. It also includes instructions on how to educate and assist patients in using the medical devices during the study. The SIV is also an opportunity to set clear roles and responsibilities for everyone involved, ensuring smooth cooperation between the clinical teams and the commercial partners. With everyone trained and the system ready, the study can finally start patient recruitment and data collection, marking the official launch of the Pilot 2.

4.3 Conclusions

This report provides an in-depth look at the development of the CYLCOMED project's pilot phase, highlighting the essential groundwork laid for successful deployment and testing. By addressing key regulatory, ethical, and operational challenges, the project has established a

Funded by Horizon Europe Framework Programme of the European Union

strong foundation for integrating cybersecurity and telemonitoring technologies into clinical environments. The close collaboration between technical experts and healthcare professionals has been critical to ensuring the project stays on track with both legal requirements and clinical needs. As the project moves toward deployment, the next step will be to validate the systems in real-world settings, gathering data that will be crucial for refining and improving the technology. The insights gained from these pilots are expected to not only improve patient care and data security but also provide a model that can be scaled for future innovations in healthcare.

Funded by Horizon Europe Framework Programme of the European Union

References

[1] CYLCOMED-D5.1 CYLCOMED toolbox prototype, Hrvoje Ratkajec editor, 2024

[2] Chowdhury, Nupur, and Ramses A. Wessel. 2012. “Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance?” European Law Journal 18, no. 3: 335-357 - https://doi.org/10.1111/j.1468-0386.2012.00603.x

[3] Biasin, Elisabetta, and Erik Kamenjasevic. 2020,”Cybersecurity of medical devices: regulatory challenges in the EU”; https://dx.doi.org/10.2139/ssrn.3855491

[4] Milojevic, Dusko. “Navigating the Ethical Maze: Children’s Assent in Clinical Research” Blog Post, 22 October

Funded by Horizon Europe Framework Programme of the European Union