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

D6.1 Pilot planning and evaluation strategy

Revision: v. 1.0

Work package	WP 6
Task	Task 6.1
Due date	30/11/2023
Submission date	30/11/2023
Deliverable lead	MCI
Version	V. 1.0
Authors	Simone Favrin (MCI), Marco Mosconi (MCI) Pietro Di Maggio (MCI), Marco Carminati (MCI), Andrea Scaburri (MCI) Ricardo Ruiz Fernandez (RGB), Ricardo Nolasco (RGB) Dusko Milojevic (KUL), Andrés G. Castillo (FHUNJ) Juan Carlos Perez Baun(ATOS), Esteban Alejandro Armas Vega(ATOS) Panagiotis Kapsalis (Martell), Tomaz Martincic (XLAB)
Reviewers	Alberto Eugenio Tozzi (OPBG) Orhun Utku Aydin (CUB)

Abstract	Report describing the details of the use cases and the design of each pilot (design, expected integration with CYLCOMED toolbox), and the expected evaluation strategy

Keywords	Use cases, Pilot, Exploitation strategy

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
v0.1	31/07/2023	First Issue	MCI
v0.2	05/10/2023	Content review after Berling Meeting	MCI
v0.3	30/10/2023	Inserted partner contributions	MCI, RGB
v0.3.1	07/11/2023	Inserted partner contributions	MCI, KUL
v0.3.2	27/11/2023	Inserted partner contributions	ATOS, MAR, XLAB
v0.4	28/11/2023	Additional contributions, comments	OPBG, CUB, FHUNJ, RGB, KUL, FHUNJ
v1.0	30/11/2023	Finalised version after internal review	MCI

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 No. 2015/444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No. 2015/444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No. 2015/444*	

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

Executive summary

This document reports a complete overview of the project pilots, from the design to evaluation strategies.

Presentation of context and general aspects of pilot developments are reported, together with insights about the involvement of different stakeholders.

Particular attention is reserved to the interaction between CYLCOMED toolbox and the pilots, reflection about the added values of each tool to the individual scenario.

Evaluation strategies that focus on maximising the outcomes of the pilots are presented, exploiting the diverse representation of healthcare stakeholders of the consortium.

This report is a first part within the broader process of deploying the toolbox in the pilot and it is conceptually connected to the implementation reports.

Table of contents

List of figures

List of tables

Abbreviations

AI	Artificial Intelligence
ATOS	Atos Spain
BGL	BlueGene/L
BP	Blood Pressure
CMD	Connected Medical Device
CP-ABE	Cipher Policy-Attribute-Based Encryption
CPU	Central Processing Unit
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CTR	Clinical Trials Regulation
CUB	Charité – Universitätsmedizin Berlin
CYLCOMED	CYbersecurity tooLbox for COnnected MEdical Devices
D#.#	Deliverable (referred to CYLCOMED proposal)
DDoS	Distributed Denial-of-Service
DMP	Data Management Plan
DNP3	Distributed Network Protocol 3
DoS	Denial-of-Service
EC	European Commission
ENISA	European Union Agency for Cybersecurity
EU	European Union
FBI	Federal Bureau of Investigation
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
GPU	Graphics Processing Unit
H2020	Horizon Europe 2020 (projects)
HDFS	Hadoop Distributed File System
HDT	Human Digital Twin
HIL	Hardware In Loop
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System

IAM	Identity and Access Management
IBM	International Business Machines Corporation
IC3	Internet Crime Complaint Center
ICS	Industrial Control Systems
ICU	Intensive Care Unit
INOV	Inov - Instituto De Engenharia De Sistemas E Computadores, Inovação
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
MAR	Martel GmbH (Associated Entity)
MCI	MediaClinics Italia
MD	Medical Device
MDD	Medical Devices Directive
MDR	Medical Devices Regulation
MHP	Mediaclinics Health Platform (Telemedicine platform)
MitM	Man-in-the-Middle
NIS2	Network and Information Systems Directive
NMT	Neuromuscular transmission
OEM	Original Equipment Manufacturers
OPBG	Ospedale Pediatrico Bambin Gesù
OR	Operating Room
OT	Operational Technology
RGB	RGB Medical Devices
SaMD	Software as a Medical Device
SBC	Single Board Computer (ie. RaspberryPi)
SCADA	Supervisory Control and Data Acquisition
SIL	Software in Loop
SSH	Social Sciences and Humanities
SSI	Self Sovereing Identity
TCI	Target Control Infusion

TCP	Transmission Control Protocol
U.S.	United States
UX	User eXperience
VC	Verifiable Credentials
VPN	Virtual Private Network
WP	Work Package
XLAB	XLAB Razvoj Programske Opreme in Svetovanje

1. Pilot planning and evaluation: overview

The introduction of pilots into the CYLCOMED project represents a pivotal strategy to actively engage real end-users and gain deeper insights into the challenges associated with the implementation of innovative technologies in healthcare scenarios and their integration with existing policies and services.

These pilots are conceived as a shared platform to test and explore critical aspects such as cybersecurity, overall effectiveness, and ethical concerns. By doing so, the initiative aims to facilitate the implementation of solutions into clinical practice, the work of clinicians, enhance the quality of patients' lives, and ensure the safety, security, and privacy of these solutions. The collaborative design of the pilots, driven by a user-centred approach, underscores the commitment to meet the diverse needs of all the stakeholders involved.

The problems addressed and the solutions depicted in this document start from considering how much the healthcare sector is getting increasingly interconnected [1] and therefore more and more vulnerable. Privacy was of course already a concern before digital healthcare services; the difference is that paper copies were usually stored in a single surveilled environment with controlled accesses, while healthcare organisations now need to protect numerous access to sensitive information. Moreover, information is duplicated and distributed, meaning that while previous unauthorised accesses could affect hundreds of patients, a data breach nowadays can potentially expose millions of people's data [2]. For these reasons, health technology solutions need to meet stringent regulations and ethical implications related to security. Recent studies addressed privacy and policy issues, especially due to security issues (attacks, vulnerabilities, weaknesses, and threats) and the related security strategies (detect attacks, stop or mitigate attacks, and react to attacks). The challenge of medical device manufacturers is thus to develop interoperable, secure, and scalable systems, while ensuring security, risk management, and protection of patient's data [3].

Healthcare organisations are usually target because they are a rich source of sensitive information while presenting weak defences: this is both physiological, considering the digital acceleration of the last 10 years, and specific to the sector, considering e.g. the use of personal devices connected to telemedicine platforms, aiming to more continuous monitoring especially for chronic and frail patients. The increased connectivity outside of hospital premises [4], paired with the usual obsolete technology adopted by the organisations [5], particularly the ones operating in National Health Services, and a general lack of awareness on the data protection and cybersecurity threats, makes the healthcare sector a perfect target for malicious attacks. These attacks are commonly performed aiming at direct financial gains (blackmail), but also to put political pressure threatening to disclose sensitive information about public figures (STDs, substance abuse etc) and finally can be used as a political leverage or to spread propaganda or political activism communications and actions [6].

Over the last few years the health sector has experienced a dramatic rise in the number and size of data breaches [7]. This can lead above all to severe harm to the patients' safety and wellbeing; as a consequence, targeted healthcare organisations can experience serious financial and reputational loss.

European legislation made a remarkable step forward with the implementation of GDPR, with the aim of harmonising data privacy laws across Europe and addressing gaps in previous national legislation, mostly released in the 1990s, prior to organisations holding vast electronic data. This new legislation can significantly increase the cost of breaches (due to implemented fines) and is helping to increase awareness around privacy issues and the need for improved cybersecurity.

Cybersecurity threats cannot be 100% prevented, and therefore they need to be conceived and integrated as part of the risk management process of healthcare organisations. A minimum standard for cyber-hygiene must be assessed and implemented: this includes regular, secure

backups (essential to maintain resilience and be able to recover quickly if attacked) and keeping software up to date to ensure security patches are in place. On the confidentiality side of the matter, anonymization of data (including images), disjunction of patients' identity from their medical data, and access limitation access to online patient information must be implemented [8]. Security must be considered a core part of the requirements design and during the whole lifecycle of the product (EHR, telemedicine platforms, connected physical medical devices etc) [3]. Both the integration of security in organisations' culture (recruitment of security specialists, training, awareness raising), as well as an enforcement via inspections from accredited bodies can help in this paradigm shift.

A crucial aspect that needs to be considered about cybersecurity in healthcare is that can only be achieved through a multidisciplinary approach that specifically considers the human factor.

1.1 Purpose of pilots

1.1.1 Cybersecurity

A central and paramount purpose of the pilots within the CYLCOMED project is the advancement of new technologies, particularly in the realm of cybersecurity. This emphasis serves as a safeguard against potential vulnerabilities and ethical concerns that may arise during the adoption of these technologies. The integration of robust cybersecurity measures becomes crucial in ensuring the integrity of healthcare data, protecting against unauthorised access, and mitigating potential risks associated with technological innovations.

1.1.2 Clinical impact

The integration of connected medical devices into clinical settings is an important step in improving patient care. However, the cybersecurity related risks, threats and vulnerabilities that accompany the adoption of connected medical devices need to be addressed. Ensuring the cybersecurity of connected medical devices is mandatory to ensure the privacy and safety of patients. With medical devices that adopt novel technologies like automation, artificial intelligence and telemonitoring the requirements for cybersecurity are also evolving and demand improved protective measures. Importantly, cybersecurity measures need to be tested in real-world clinical scenarios to confirm their effectiveness and relevance. With two clinically driven pilot studies, the CYLCOMED consortium aims to elevate cybersecurity standards within healthcare scenarios, particularly focusing on the safety, and privacy aspects of Connected Medical Devices (CMDs). The unique approach of Pilot 1, dedicated to "Cybersecurity in Hospital Equipment for COVID-19 ICU patients," utilises a digital twins simulation without direct human participation. In contrast, Pilot 2, addressing "Cybersecurity for Telemedicine Platforms," employs an observational study involving the processing of personal data, specifically patient data, within the bounds of stringent compliance with EU data protection regulations.

1.2 General requirements

Building on the insights gained by CYLCOMED Deliverable 3.1 "Baseline analysis, requirements and specifications", the document provides a concise exploration of the overall aspects pertinent to the evaluation phase.

The Connected Medical Device (CMD) requirements defined in D3.1 are scrutinised to discern their implications across different scenarios. This examination encompasses both functional and non-functional requirements, with particular attention to cybersecurity requirements.

Cybersecurity requirements are linked to the results of risk analyses, incorporating methodologies outlined in D4.1 “CMD Risk Management Methodologies” to ensure a comprehensive understanding and application across various scenarios.

- Interoperability: it is a critical aspect, requiring verification of information exchange among medical devices, clinical information systems, and telemedicine platforms. User experience validation becomes imperative, assessing the user-friendliness of cybersecurity tools for both clinicians and IT professionals, with feedback becoming an invaluable asset for final design of the cybersecurity toolbox to be implemented in CYLCOMED.
- Regulatory compliance checks span healthcare regulations, data protection laws, and standards for medical devices, ensuring adherence to necessary certifications and requirements.
- Technical efficacy verification involves assessing the tools' robustness in detecting and mitigating potential cyber threats under diverse conditions.
- Scalability assessments are essential to confirm the cybersecurity solution's adaptability to varied healthcare settings, accommodating different patient loads and technological infrastructures. Establishing a feedback mechanism from clinicians, IT professionals, and stakeholders enables iterative improvements, addressing identified issues.
- Beyond technical aspects, educational impacts are scrutinised, particularly in enhancing healthcare professionals' understanding of cybersecurity risks and best practices.
- Requirements verification ensures the evaluation of the CYLCOMED solution's readiness for wider implementation, navigating the complex landscape of telemedicine with attention to clinical, technical, and ethical considerations.

1.2.1 Legal, ethics overview about the pilots

As human participants will be included in the CYLCOMED project, all the activities of the project will comply with applicable international, EU, and national laws as well as the highest ethical standards, such as the Declaration of Helsinki, which sets the ethical framework for medical research. Although law and ethics are closely intertwined, it is important to establish their relationship at the beginning of this deliverable. While laws stipulate what must, can or cannot be done, ethical notions about good and bad behaviour lie behind these stipulations[9]. According to Rochel, ethics fulfils three important functions, namely: coordinative function, which provides actors with common principles; a red-line function of clarifying practices which should be prohibited; and the gap-filling function of providing justification for specific actions. In doubt regarding the legal norms or where the law has no clear answer, “ethics is used to jump in and address the problematic situation” [10]. New technologies are an example of where the law lags behind and where ethics play a crucial role, paving the way to legal norms.

Indeed, Ethics is regarded as the cornerstone of all projects funded by the European Commission. This can be illustrated through an EC statement, which highlights that “ethics is an integral part of research from beginning to end, and ethical compliance is seen as pivotal to achieve real research excellence” [11]. Therefore, EC requires that all research activities carried out under the Horizon 2020 Framework Programme are conducted in compliance with fundamental ethical principles.

The Horizon 2020 Framework was established by EU Regulation No. 1291/2013 [12]. The rules applicable to participation and dissemination in Horizon 2020 are set out in Regulation 1290/2013/EU [13]. Regulation 1291/2013 lays out the ethical principles with which all actors in Horizon 2020 projects need to comply. It sets out that “all research and innovation activities carried out under Horizon 2020 need to comply with ethical principles set out in this article and with relevant legislation”. Additionally, it obliges all actors in Horizon 2020 projects to pay

particular attention “to the principle of proportionality, the right to privacy, the right to protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the right to ensure high levels of human health protection” [14]. Regarding the research ethics under the Horizon 2020 framework, it is important to emphasise the rules laid down by the four EC guidelines, which have been briefly touched on below.

Guidance on how to complete the ethics self-assessment has been developed by EC, aiming at facilitating the identification of any ethical issues that may arise, including the Ethics Checks and Audit [15]

Ethics and data protection has the objective of ensuring that all projects are guided by ethical considerations and the values and principles on which the EU is founded [16]. It highlights that data protection is the cornerstone for research ethics in the EU, as well as a fundamental human right. It is intimately linked to autonomy and human dignity and the principle that everyone should be valued and respected [16]. The guidance note places particular attention on the research that involves the processing of special categories of data and processing of personal data concerning children, which is the particular case in the CYLCOMED environment. As mentioned above, CYLCOMED Pilot 2, “Cybersecurity for Telemedicine Platforms”, will be conducted as an observational study by processing the personal data of patients, including paediatric patients, whereas no interventional study will be conducted on them. Therefore, it is imperative to test the technologies developed in real-life, operational settings.

The informed consent is also one of the main elements of the guidance note, which states that “Informed consent is the cornerstone of research ethics”[16]. Accordingly, it is essential to clearly communicate to participants the purpose of the study, the nature of their involvement, and any potential risks involved. Only after this information is conveyed to the participants, subject to the condition that information is fully understood by participants in the research, is it allowed to seek and obtain the participants’ express permission to include them in the project[16].

In other words, individuals should not be the subject of a research project without being informed, while their informed consent must meet the minimum requirements stipulated by the GDPR.

Further guidance on “informed consent” is provided by the EC Guidance note on informed consent [17]. This document lays down rules on, inter alia, obtaining the consent of a parent/legal representative and, where appropriate, the assent of the child. For instance, it is imperative that any information addressed to a child is in age-appropriate and plain language that they can easily understand. Besides, it is mandatory to apply the principle of protection by design to research data concerning children and minimise the collection and processing of their data as far as possible. According to the EC Guidance note on informed consent, “Informed Consent is the decision, which must be written, dated and signed, to take part in a clinical study, taken freely after being duly informed of its nature, significance, implications and risks and appropriately documented, by any person capable of giving consent or, where the person is not capable of giving consent, by his or her legal representative; if the person concerned is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation”[17].

It is important to differentiate informed consent as an ethical standard from consent as a legal ground. Therefore, the consent requirements in the GDPR and the informed consent requirement in the Clinical Trials Regulation (CTR) must not be confused. The former presents a legal ground for processing personal data, whereas the latter serves as an ethical standard and fundamental condition under which an individual can be included in an interventional clinical study with a medical product.

Ethics in Social Science and Humanities serves as a crucial guide for social sciences and humanities (SSH) researchers to effectively identify and address ethical considerations when participating in EU Framework Programme research and innovation initiatives [18].

It sets out overarching ethical principles that must be followed whenever research includes humans, which is the case with the CYLCOMED project. These overarching ethical principles in the context of EU-funded research include:

- respecting human dignity and integrity;
- ensuring honesty and transparency towards research subjects;
- respecting individual autonomy and obtaining free and informed consent;
- protecting vulnerable individuals;
- ensuring privacy and confidentiality;
- promoting justice and inclusiveness;
- minimising harm and maximising benefit;
- sharing the benefits with disadvantaged populations, especially if the research is being carried out in developing countries;
- respecting and protecting the environment and future generations [18].

European Code of Conduct for Research Integrity outlines the various professional, legal, and ethical obligations, while also recognising the crucial role of the institution in which the research takes place [19]. For instance, the European Code of Conduct for Research Integrity Article 1 lays down four ethical principles to which the consortium ought to adhere as they lie at the core of ethical research. These are:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources;
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way;
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and their environment;
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring and for its wider impacts.

As the CYLCOMED project seeks to develop complex technical solutions concerning connected medical devices based on personal data processing, most notably sensitive data, the CYLCOMED project must uphold the highest ethical standards to achieve the balance between the research objectives and the means used by project partners to attain these goals. Therefore, it is crucial to ensure that the project does not compromise ethical principles. This will ensure the integrity of the research and maintain the trust and credibility of the proposed CYLCOMED technical solutions. Since Pilot 2, “Cybersecurity for Telemedicine Platforms”, will be conducted as an observational study by processing the personal data of paediatric patients, it will be subject to the review of an Ethical Committee that should review a formal protocol and adherence to ethical standards that are delineated in this section.

Nowadays, healthcare is one of the most targeted sectors concerning cybersecurity incidents. European Union Agency for Cybersecurity (ENISA) Report on the threat landscape [20] reveals that the health sector is the third most targeted sector per number of incidents. Likewise, according to a recent FBI Internet Crime Complaint Center (IC3) report, healthcare and public health were the most targeted critical infrastructure sectors in the U.S. in 2022, with 210 officially reported attacks [21]. Successful cyberattacks may impede hospital operations, because the loss of sensitive patients' data, compromise patient safety and consequently

cause death, to mention just a few severe ramifications of malicious attacks. According to ENISA's Cyber Threat Landscape of the Health Sector in the EU, patient data, including electronic health records, were the most targeted assets from January 2021 to March 2023 [22]. IBM's "Cost of a Data Breach Report 2023" has found that healthcare breach costs have been the most expensive industry for 13 consecutive years, increasing by 53.3% since the 2020 report [23]. Hospitals might be faced with significant financial costs due to patient compensation and regulation fines [24] For instance, The Finnish psychotherapy centre Vastaamo has been fined EUR 608,000 by the Office of the Data Protection Ombudsman for violating the GDPR provisions related to the safe processing of personal data as well as reporting a personal data breach [25]. The increasing digitalisation of healthcare service providers has enabled cyberattack techniques toward them to become more liquid, flexible, and able to exploit all the possible paths of entry rapidly. Cyberattacks on the IT infrastructure of hospitals, electronic health records, or medical devices that have taken place during the COVID-19 pandemic reaffirmed the importance and urgency of ensuring cybersecurity in the healthcare sector [26]

As technology continues to be integrated into healthcare, cybersecurity incidents have become a major challenge for the industry. Medical devices, which were once only set up on hospital premises, can now generate, collect, analyse, transmit, and store vast amounts of data, as well as communicate with each other. Although this increased connectivity has resulted in multiple benefits, such as real-time patient care, monitoring, and a reduction in healthcare costs, it has come at a cost. Every connected medical device increases the attack surface and vectors, making each device a potential entry point for an attack. As a result, preserving data privacy and patient safety has become a challenging task that requires innovative cybersecurity solutions in the complex digital environment.

It is important to note that regulating cybersecurity is a complex task. The same can be said for medical device regulation, which is characterised by regulatory specialisation and fragmentation [27]. Consequently, regulating the cybersecurity of medical devices bears the complexities of both legal frameworks [26]. It is noteworthy to point out that the EU cybersecurity framework comprises several pieces of legislation that cover aspects linked to cybersecurity or some of its elements. When it comes to the legal requirements for the cybersecurity of medical devices relevant to CYLCOMED technical solution, the EU laws establish a set of different requirements enshrined in, for instance, the Medical Devices Regulation (MDR), the Network and Information Systems Directive (NIS2), and the General Data Protection Regulation (GDPR).

1.3 Pilot design: crucial aspects and the CYLCOMED toolbox

The strength of CYLCOMED lies in its consortium's representation of the entire healthcare ecosystem, from manufacturers to end-users. This wide-ranging representation ensures that each project partner benefits from the feedback provided by medical professionals impacts the evaluation schema. This approach, beyond assessing the objective efficiency of the tools, aims to catch the perception of hospital staff, acknowledging the multifaceted nature of technology implementation in healthcare settings.

Even though no clinical trials are foreseen for For Pilot 1, the representation of the end-user is granted also in this scenario through the collaboration with FHUNJ who brings the end-user perspective in the pilot, providing valuable feedback for the improvement of tools.

In the case of Pilot 2, which is an implementation of telemedicine in hospital environments (in particular we will focus on vital signs tele-monitoring), end-users (OPBG, CUB, FHUNJ) actively contribute with their experiential insights. These insights are seamlessly integrated into the formulation of the patient journey and the definition of the clinical protocol, ensuring a holistic approach to technology implementation.

The double nature of the pilots allows to test in the best possible way all the tools expected in the toolbox, in Table 1 is reported the interaction between tools and pilots. Furthermore, deeply involves the end-users, allowing a fundamental exchange of knowledge between the partners.

	Pilot 1	Pilot 2		
		Pilot 2	Sub pilot A	Sub pilot B
AI-based CMD Behavioural Analysis & Log Monitoring				
↳LOG Analysis	☐	☑	☑	☑
↳Network Analysis	☑	☑	☑	☑
Connected Medical Devices and Services Management Tools				
↳Service management tools	☑	☐	☐	☐
↳Ansible playbook scanner	☑	☐	☐	☐
Identity & Access Management and Data Protection for Connected Medical Devices				
↳IAM Single Sign-In solution Lus4MED	☑	☑	☑	☑
↳Data protection solution FE4MED	☑	☑	☑	☑
Connected Medical Device integrity				
↳Connected medical device integrity solution	☑	☐	☐	☐
CYLCOMED Security Dashboard				
↳CYLCOMED Security Dashboard	☑	☑	☑	☑

Table 1: Tools deployment in the pilots.

Additional information about the tools characteristics are reported in Deliverable 3.1.

1.3.1 AI-based CMD Behavioural Analysis & Log Monitoring

1.3.1.1 Log analysis

Any modern software is designed to collect logs of information useful mainly for technical support, bug fixing, monitoring access operations and more. In particular, being MHP (Mediaclinics Health Platform, the MD used in Pilot 2 as we'll describe) a microservices based solution, it generates important quantities of logs of different kinds, in particular:

- network logs, collected by the front facing reverse proxy.
- database errors logs.
- technical information about crashes of the microservices and the app.
- audit logging system, which collects any operation performed on the platform.

Nevertheless, they contain a lot of unused information that CYLCOMED will use to detect anomaly behaviours, and while the tool itself cannot prevent threats, it can detect them and fire alerts. The tool analyses log sequences (sequences of events).

The tool is able to detect changes in the distribution and order of events (e.g., a brute force attack results in many unsuccessful login attempts). It can also detect unknown events whenever a log message does not match any of the known log templates (e.g., a network error log that was not present in the training data).

1.3.1.2 Network analysis

The CYLCOMED Network Analyzer or LADS (Live Anomaly Detection System) is an anomaly-based network intrusion detection system tailored for operational technology (OT) environments. It focuses on monitoring network traffic and identifying deviations from established behavioural patterns, specifically in industrial control systems (ICS) and SCADA environments. LADS leverages advanced deep learning algorithms to detect both known and unknown (zero-day) threats, ensuring robust protection against a wide range of network-based attacks.

Both pilots will benefit from the capabilities of this tool in different ways:

1. Operating in such a critical environment as the one proposed in pilot 1, detecting anomalies on the network to which the SBC connects is critical, in fact the little hardware capabilities of these boards can be easily overcome by network based attacks.
2. Tele monitoring platforms leverage the public internet (protected in various ways such as using a VPN, virtual private network) and therefore may be subject to various network attacks.

Main Threats Addressed by LADS:

- Network Intrusions and Anomalies: For ICU and Telemedicine platforms, LADS can detect unusual network behaviours, flagging potential intrusions or anomalies in communications.
- Unauthorised Access and Reconnaissance Activities: The tool can identify unauthorised access attempts in the network by analysing the network behaviours, crucial for maintaining secure operations.
- Man-in-the-Middle (MitM) Attacks: By monitoring network traffic, LADS can identify patterns indicative of MitM attacks, crucial for secure data transmission.
- Protocol-Specific Attacks: It can detect misuse or abnormal usage of common OT protocols, such as ModbusTCP [REF MODBUS] and DNP3, particularly relevant in scenarios involving complex medical equipment.
- DoS and DDoS Attacks: LADS can identify and alert on Denial-of-Service attacks that could cripple critical healthcare infrastructure.

Expected Impacts on the Platform:

- Increased Infrastructure Security: LADS will enhance the security of the network infrastructure by providing real-time monitoring and anomaly detection.
- Complexity and Integration Requirements: Implementing LADS could increase the complexity of the existing network and require integration with current systems.
- Need for Skilled Personnel: Effective operation and interpretation of LADS data might require skilled cybersecurity personnel.
- Operational Overhead: Continuous monitoring and analysis of network traffic might add to the operational overhead but are essential for robust security.

1.3.2 Connected Medical Devices and Services Management Tools

The management tools aim to provide secure management of connected medical devices.

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

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

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

1.3.3 Identity & Access Management and Data Protection for CMDs

1.3.3.1 IAM Single Sign-In solution Lus4MED

The LuS4MED (Ledger uSelf for Medical Data) asset is a tool for adopting the Self-Sovereign Identity solution in the health domain, providing a user-centric access control to data where the user is in full control of their identity and data. In the CYLCOMED project LuS4MED can be used to mitigate different identity threats, in the context of data protection and access control.

The main threats LuS4MED can help to mitigate are:

- Identity theft can be minimised leveraging the decentralised approach of the SSI solution, because the user has more control over their personal and sensitive information and how to share these data.

- Generation of malicious identity, as the SSI solution uses cryptographic mechanisms for securing the verifiable credentials (VC) the user manages.
- Data leaks. The user-centric approach permits a minimisation and a selective disclosure of data.
- Unauthorised access. The use of VC instead of passwords, the use of cryptographic techniques and the decentralised nature of SSI avoid malicious actors the access to personal data.

Expected Impacts on the Platform

- Technical integration complexity. The integration of SSI solutions with legacy systems could be technically complex, but the use of LuS4MED diminishes this complexity allowing a seamless integration.
- Wallet Security. The access of attackers to the device can allow the access to the digital wallet and compromise the SSI system.
- Regulatory compliance. SSI integrated systems must comply with the current regulation (e.g., GDPR and EU digital services Act).
- User experience can be affected when using digital identities. Lus4MED design mitigates this impact including UX design principles.

1.3.3.2 Data protection solution FE4MED

The FE4MED (Functional Encryption for Medical Data) tool is intended for privacy-friendly secure data exchange among devices and healthcare providers in cross platform and even cross-border settings. FE4MED is based on novel encryption schemes such as the Cipher Policy-Attribute-Based Encryption (CP-ABE). CP-ABE is a type of encryption scheme using attributes to control access to encrypted data. In CYLCOMED project FE4MED can be used to mitigate various security threats, in the context of data protection and access control.

The main threats FE4MED can help to mitigate are:

- Unauthorised access to encrypted data, restricting data access.
- Data leakage by controlling the access to personal and sensitive data, diminishing the risk of data leakage.
- Loss of confidentiality, the encrypted data are accessible only to those users with specific attributes, based on the access policies, in case the encrypted data are caught by unauthorised parties.
- Insider menace can be mitigated enforcing access policies based on attributes.

On the other hand, affects negatively by:

- Complex integration depending on the legacy systems the hospitals have in place.
- Performance overhead as the CP-ABE encryption/decryption process can take more time than expected compared to other basic encryption schemes.
- Attributes management by the hospital need to be carefully treated, when setting attributes and access policies.
- Computational resources can be affected in comparison with other basic access control solutions.

1.3.4 Connected Medical Device integrity

Modification to legacy medical devices is generally very complex both from a technological point of view and from a compliance perspective. By introducing an external controller component we aim to reduce such complexity.

This approach is at core of Pilot 1 (as we'll describe in the upcoming sections) where it will be applied the infusion pump CMD (connected medical device) by RBG, enabling it to integrate with a much broader audience of tools, and therefore leverage on the benefits of the CYLCOMED toolbox.

The component will be deployed on a SBC (single board computer) and act as the infusion pump controller as well as a local server to serve readings coming from the CMD itself. This component will run in Docker containers on the SBC itself allowing for independence from the SBC manufacturer and allowing isolation between the other tools.

Benefits:

- Software isolation, docker can isolate the process and govern the resource access (network, connected devices, storage etc.)
- Ease of software update
- Independence from SBC manufacturer

1.3.5 CYLCOMED Security Dashboard

The CYLCOMED Dashboard serves as a centralised security information and event management tool within the CYLCOMED framework. Its primary function is to aggregate, analyse, and display security data from various sources across the CYLCOMED Framework. This tool is instrumental in providing real-time visibility into the security posture, highlighting potential threats, and aiding in prompt and effective incident response.

It will be a valuable tool for the IT technicians of the MDs manufactures and of the HIS (Hospital Information System) to understand the overall status of the telemedicine platform and the security threats.

Main Threats Addressed by CYLCOMED Dashboard:

- Data Breaches and Unauthorised Access: The Dashboard can correlate events and logs to detect unauthorised access attempts to the telemedicine platforms and ICU equipment, a critical aspect in safeguarding patient data.
- Network Anomalies and Intrusions: By integrating with network monitoring tools, the Dashboard can highlight unusual network behaviours, flagging potential security breaches or intrusions.
- Insider Threats: Through analysing user behaviour and access logs, the Dashboard can help in identifying suspicious activities that might indicate insider threats.
- Compliance Violations: The Dashboard can assist in monitoring and ensuring compliance with healthcare regulations, like GDPR and HIPAA, by tracking access and data handling.

Expected Impacts on the Platform:

- Enhanced Situational Awareness: The Dashboard will provide a centralised view of the cybersecurity state across the telemedicine and ICU platforms, offering enhanced situational awareness.
- Operational Complexity: Implementing a Dashboard that aggregates and correlates data from multiple sources will increase the complexity of the system architecture.
- Training Requirements: Staff may require training to effectively interpret and respond to the insights provided by the Dashboard.

Resource Allocation: The Dashboard could require computational resources for data processing and storage, and network resources for data aggregation.

1.4 Evaluation strategy overview

Given the inherent complexity of the CYLCOMED project, a single evaluation tool wouldn't fit the diverse aspects, therefore different evaluation tools are required.

For each pilot two major approaches can be outlined: a technical and a "clinical" evaluation. The technical evaluation refers to aspects that are not strictly related to the healthcare application itself but are of interest for the tool developer, who gains insights about the tools real behaviour.
Under the "clinical" evaluation term, all the aspects that involve users are considered, from usability to functional requirements. Both these evaluation aspects will cooperate and provide valuable feedback to the tools' developer.

The technical evaluation is planned involving a comparative analysis of the tools against the predefined requirements in D3.1. Functional assessments will be conducted through acceptance tests, validating the functionality and operational efficacy of the implemented tools.

The acceptance and perception of end-users (where possible, it will also involve the patients and not only the medical professionals) constitutes a critical dimension of the evaluation. To capture this impact, a structured approach employing questionnaires is adopted.

These questionnaires serve as valuable tools for soliciting qualitative feedback, highlighting the user experiences and perceptions.

This comprehensive evaluation approach addresses crucial non-technical aspects such as usability, perceived value, societal implications, and legal and ethical considerations.

While technical aspects such as ease of integration and performance are indispensable for evaluating the outcomes of Work Package 5 ("Cybersecurity Toolbox Design and Implementation"), equal weight is accorded to non-technical aspects. These include considerations such as usability, the value perceived by users, societal implications, and legal and ethical dimensions. The recognition of this evaluation scope underscores the commitment to understand the effects and the efficacy of the CYLCOMED toolbox when deployed in healthcare frameworks.

Each pilot has selected proper evaluation methodologies with their stakeholders, the result of this activity is reported in this document.

1.4.1 CYLCOMED tools evaluation: technical aspects

In this section we highlight key metrics that will measure the impact of each tool of the CYLCOMED toolbox.

Tool	**Technical**	**Clinical**
Log analysis	Accuracy, Efficiency	
Network monitoring and analysis	Accuracy, Response time, Performance impact, Protocols coverage, Incident reduction rate, Compliance with standards	
Connected medical devices and service management tools	Performance, Efficacy	
IAM, Single sign-on solution	Performance	Usability
Data Protection solution	Performance	Usability
Connected Medical Device integrity	Accuracy, Performance	
CYLCOMED security dashboard	Accuracy, Response time, Efficiency, Usability, Compliance with regulations	Usability

Table 2: Metrics for the measurement of the impact of the tools

1.4.1.1 Log Analysis

The following metrics will be monitored in order to evaluate the technical impact of the log analysis tool:

- Accuracy: the tool will be tested against some labelled public data (e.g. of public available dataset are BGL [30], HDFS [31].
- Efficiency: to assess the efficiency and impact on the existing infrastructure of the instrument it'll also be important to measure the throughput in logs/second.

About efficiency, the tool will require the usage of a dedicated infrastructure (GPUs) to train the anomaly detection models, while this is mandatory for the training phase, the inference will not have such requirement lowering the costs on hospital premises.

1.4.1.2 Network monitoring and analysis

The following metrics will be monitored in order to evaluate the technical impact of the LADS tool:

- Detection Accuracy: Measure the accuracy of LADS in detecting true security incidents versus false alarms.
- Response Time to Anomalies: Assess how quickly the system responds to detected anomalies.

- Network Performance Impact: Monitor if LADS deployment impacts the overall performance of the network.
- Coverage of Protocols: Evaluate the range of OT protocols that LADS successfully monitors and detects anomalies in.
- Incident Reduction Rate: Track the reduction in the number of network-related security incidents over time.
- Compliance with Security Standards: Assess how well LADS aligns with industry-standard cybersecurity practices and regulations, particularly in healthcare.

1.4.1.3 Connected Medical Devices and Services Management Tools

The following metrics will be monitored in order to evaluate the technical impact of the tool:

- Performance: Number of medical devices that can be monitored by one instance
- Performance: number of Over The Air (OTA) updates performed simultaneously by one instance
- Efficacy: Number of medical devices monitored during the pilot
- Efficacy: Number of OTA updates performed during the pilot

1.4.1.4 IAM Single Sign-in solution Lus4MED

The following metrics will be monitored in order to evaluate the technical impact of the Lus4MED tool:

- Performance, identity verification operation speed: time for verifying the user's identity using SSI solution.
- Performance, registration/login process time: Measuring the time for generating credentials by the issuer system and spending time for authenticating users when SSI solution is in place.

1.4.1.5 Data Protection solution FE4MED

The following metrics will be monitored in order to evaluate the technical impact of the FE4MED tool:

- Performance, encryption/decryption speed: taking time measures of encryption/decryption operations: key generation, data encryption and data decryption.
- Performance, computational overhead: consider the system performance and the resources consumption during the encryption/decryption process.

1.4.1.6 Connected Medical Device integrity

NMT CONTROL

Once the correct operation of the patient simulator has been verified, we will apply it to evaluate the NMT control strategy. To assess the effectiveness of the strategy, several controls will be performed by varying the patient parameters of Vd and Cp50.

We have refined the control strategy based on past experience on control theory used in the case of other Vital Signs. The objective is to maximise the time in which the patient's NMT

remains at the programmed target value. We have used the “bolus” approach -instead of a continual dose infusion.

The “optimal bolus” dose strategy is based on finding the bolus dose that, applied repeatedly, ensures that the patient's NMT remains at the target value.

Obviously, the specific “Optimal Dose” value is varying during the control process, since the patient is subject to changes such as sensibility to the drug. To assess the effectiveness of the strategy, several controls will be performed by varying the patient parameters of Vd and Cp50.

1.4.1.7 CYLCOMED security dashboard

The following metrics will be monitored in order to evaluate the technical impact of the dashboard:

- Event Correlation Accuracy: Evaluate the accuracy of the Dashboard in correlating events to actual security incidents.
- Time to Detect and Respond: Measure the time taken from event occurrence to its detection and the subsequent response initiation.
- Incident Resolution Efficiency: Track the efficiency in resolving security incidents identified by the Dashboard.
- User Engagement and Usability: Monitor how frequently and effectively the security teams interact with the Dashboard.
- Regulatory Compliance Adherence: Evaluate the effectiveness of the Dashboard in maintaining and demonstrating compliance with relevant regulations.

2. Pilot 1: Cybersecurity in Hospital Equipment for COVID-19 ICU patients

2.1 Description of the pilot

Pilot 1 relates to a muscular relaxation infusion controller, which is a medical device that measures at regular intervals the level of relaxometry of the patient, and according to this value and previous ones, determines the new dose infusion to be given. The system has the means to control the infusion pump as well as alarms management in order to automatically maintain the levels of relaxation within pre-established target values.

A prototypical implementation of the testbench and autonomous intelligent controller will be implemented to test the functionality and performance of the controller under laboratory conditions.

This baseline implementation includes a monitor and controller, with external OEM infusion pump tree; a target Neuromuscular Transmission level profile is set up for the operation. The target control infusion SW component computes at regular intervals the new drug dose (with e.g. relaxant drug "Rocuronium") to be infused . The patient´s model determines the patient´s NMT level achieved. The patient is modelled using traditional compartmental analysis in which the interpersonal variability is considered (RGB). This NMT value is transferred via a serial channel to the infusion controller. The main focus has been on validation and verification of the HiL (Hardware-in-the-loop) system in virtual test platforms with the tool landscape for this purpose provided by RGB and Cylcomed partners for the implementation of security tools. HiL tests have been performed in the laboratory, with the concept of continuous improvement in mind. In parallel, a Virtual Platform for the autonomous infusion pump controller has been built, to explore the different control strategies and testing its autonomous mode.

The long-term objective (outside CYLCOMED time frame) is to incorporate this feature as a software component, incorporated in an external module that interoperates with a CE-certified monitoring equipment (VISION AIR) for preventing Acute Respiratory Distress of Covid-19 ICU patients.

Pilot 1 does not involve real patients, it's a proof of concept, and it is performed within a controlled laboratory environment. However, it addresses the real needs of Medical Equipment in an “on-premises" scenario. In CYLCOMED, several cybersecurity features will be tested.

A test bench platform using digital twins will be used for this pilot. Cybersecurity protection features, when integrated as software components into the Medical Equipment, could potentially alter the functionalities of the demanded essential requirements. One of the reasons is that the Medical Equipment could have CPU performance limitations when dealing with additional lines of code to cope with. In other cases, the security APP (such as User´s authentication) itself might not be ergonomically feasible to be implemented in a real-life context. Therefore, it is necessary to set up a kind of Digital twin that can test the functional (safety) and non-functional (security) performance of the system, trying to mimic the ICU real conditions.

Even though it is not expected to carry out any clinical tests, the hospital “Niño Jesús”(FHUNJ) will support in providing their feedback from the medical user perspective.

Medical application itself (functional aspect of the development)

Anesthesiology has three main objectives:

- Analgesia. The intended effect is to reduce or eliminate a patient's pain via analgesic type of drugs.

- Immobilisation. The intended effect is to avoid the intentional or unintentional patient's movement during surgery via relaxant type of drugs.
- Unconsciousness. The intended effect is to reduce or eliminate the patient's consciousness so that the patient does not witness or otherwise sense the surgical procedure. This is done via hypnotic type of drugs.

In order to achieve these purposes, anesthesiologists use three different types of drugs.

RGB is working on a line of controllers for the regulation of vital signs in the operating room by means of drug infusion.

An intelligent infusion controller for Vital Signs is a medical device that monitors the specific Vital Signs Parameter (e.g., Blood Pressure BP or Neuromuscular transmission NMT) to be regulated and infuses at regular intervals an updated drug dose value, to achieve a specific target value for the physiological value under control.

The medical use case is concerned with the manipulation of relaxant drugs such as Rocuronium, and its ability to provide new and breakthrough technology to cope with a better control of muscle relaxation status in the patient. Since each patient is unique, no single dosage of a relaxant is likely to be appropriate for all patients. In addition, providing an under or over-dosage of an anaesthetic is highly undesirable. At recovery time, the patient is provided an antidote for the drug, and again, the more relaxed the patient is, the more antidote is required. This has several drawbacks for the patient. So the rule for dose infusion is "not too little, not too much".

The development of this autonomous controller would facilitate the work of the anesthesiologists and increase patient safety through better control of the Neuromuscular Transmission values. For this development, the verification and validation of the controller prior to any clinical investigation with real patients is essential, so a virtual test bench platform with a complete test plan is required for this.

CYLCOMED Pilot 1 on NMT (Neuromuscular Transmission) or Relaxometry Controller by means of Drug Infusion is, by itself, a technological break-through in line with Robotic and Automation of tasks within the O.R. (Operating Room) and I.C.U. (Intensive Care Unit). RGB, as the Use Case provider, is working on a family of controllers with innovative functionalities to be incorporated on a multiparameter monitor. The objective in Pilot 1 is to develop a Digital Twin HiL/SiL testbench platform that will allow the system to be verified under laboratory conditions.

2.2 Scenario details

Section 4 of Deliverable 3.1 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.

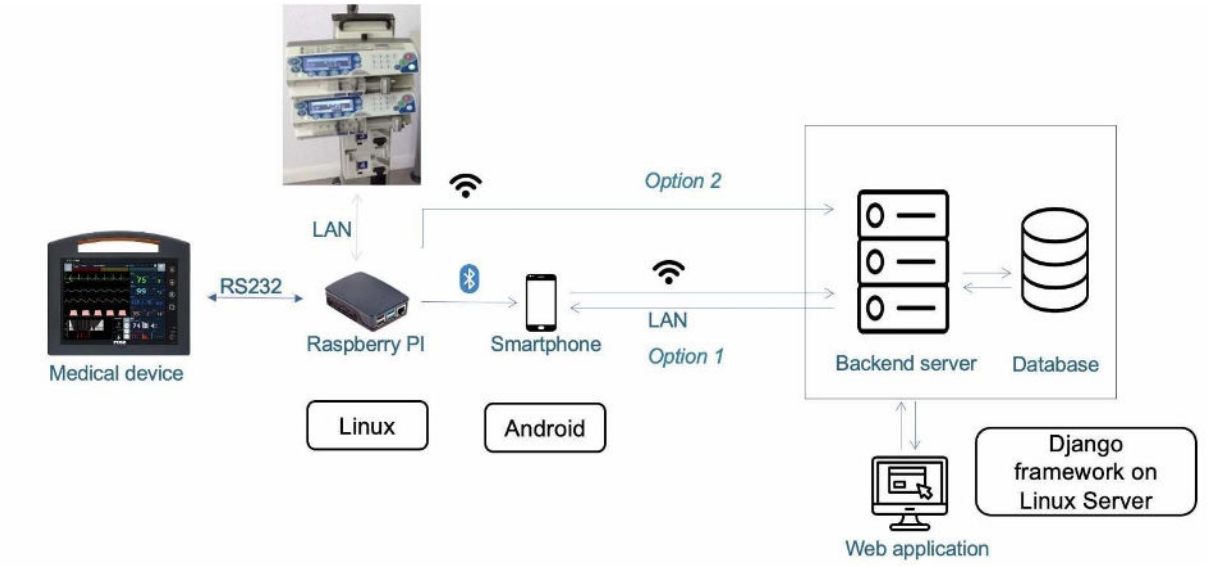


Figure 1: Pilot 1 Architecture

On top of that, a high-level view of the technical architecture that will be implemented in the pilots is also considered, because some requirements are deeply related to them.

2.2.1 Risk and threats

CYLCOMED addresses new challenges for medical devices, posed by their use in the context of novel cybersecurity risks and threats to be studied in relation to this particular use case scenario. However, let us not forget that the ultimate goal is that the compliance with the safety functional specifications are not altered by the incorporation of cybersecurity components.

For safety analysis, we need to identify hazards that can lead to serious injury and fatality to the patient in the Medical Use Case.

The VisionAir® is the trade name of the multi-parameter monitor designed by RGB Medical Devices; It refers to physical Equipment, not a system. The VisionAir® equipment incorporates, among others, the technology NMTCuff® for consciousness sensing purposes. Vision Air has been certified as a multi-parameter monitor in the past June 2023 (see Appendix).

NMTCuff® technology is a unique software plus hardware solution developed by RGB and is continually evolving.

The feature to be incorporated in CYLCOMED is a NMTCuff® software component to be designed by RGB that acts as a closed loop algorithm and determines the Optimal dose to be infused to achieve a certain NMT target in a TCI (Target Control Infusion) strategy.

Since work will be carried out at laboratory level, RGB will simulate the patient's behaviour using models to mimic the behaviour of the patient subject to a certain infusion profile of a relaxant drug.

The way to do it is by using a Pharmaco-Kinetics/Pharmaco-Dinamics (PK/PD) model, with 3 compartments. We expand the idea of digital twin to include not only physical objects and systems but also people themselves with the concept of a Human Digital Twin (HDT) which is

a representation of an individual that accurately captures and simulates their physiological, behavioural, and physical traits in a digital setting and provides insights into human performance, well-being, and behaviour.

We designed an NMT Patient Model for the relaxant drug called Rocuronium (PATMOD) that simulates the response of the patient to the amount of drug that is infused by the controller. The dynamics of the models is designed using a docker based tool developed by RGB following a 3-compartmental model that can be described as follows:

- The drug (namely Rocuronium) is injected intravenously into the central compartment, representing the blood in the body - contained primarily in the arteries and veins and the directly influenced tissues and organs, such as brain, heart, liver, kidney etc.
- The second compartment represents the group of tissues that are indirectly affected by the amount of drug in the central compartment, i.e., mainly the muscles.
- The third compartment represents the group of tissues that can store a certain amount of drug, but the exchange with the central compartment is rather slow, i.e., mainly the fat.

The effect site for the drug rocuronium is basically at the interface between nerves and muscles.

Result of the risk analysis

The examples below show the way that risk analysis will be evaluated. We will restrict the contents to the security requirements already described in D3.1 plus a few functional examples as indicated in the following table.

NMT component	Req No.	Req. Type	Description
Sensing	UC1-NMT 01	Functional	Within X distance of range from the NMT target level, the sensing component shall identify overshooting or undershooting conditions.
Sensing	UC1-NMT 02	Functional	Time between NMT samples must take into consideration perturbations due to noise or patient condition or evolution.
Sensing	UC1-NMT 03	Functional	The sensing component shall perform as required in all situations. Patient behaviour has a Fuzzy nature.
Sensing	UC1-NMT 04	Functional	The sensing component shall perform as required in the face of defined component failures arising within the system.
System	UC1-NMT 05	Design Constraint	All data samples shall represent discrete NMT levels.
System	UC1-NMT 06	Design Constraint	All data samples should include common types of patients.
System	UC1-NMT 07	Design Constraint	Noise or unexpected patient´s behaviour shall be considered.
System	UC1-NMT 08	Design Constraint	The format of each data sample shall be representative of that which is captured using sensors deployed on the RGB NMT monitor.
System	UC1-NMT 09	Design Constraint	Each data sample shall assume sensor data is representative of current NMT values.
System	UC1-NMT 10	Design Constraint	The data samples shall include a sufficient range of levels belonging to the particular relaxometry category.
System	UC1-NMT 11	Design Constraint	The data samples shall include examples with acceptable levels of certitude giving partial view of noise and patient´s behaviour.
System	UC1-NMT 12	Design Constraint	The data samples shall include a sufficient range of patient´s configurations reflecting the e.g. adaptability level of the patient to the drug.
Predict/ Control	UC1-NMT 13	Functional	Controller behaviour should be reasonably proximate to the target for more than X% of the operation time.
Predict/ Control	UC1-NMT 14	Functional	Distance to target shall not be greater than X% at all times.
Predict/ Control	UC1-NMT15	Functional	All sources of failure present in the data samples must be correctly identified.
Sensing	UC1-NMT16	Non-Functional	The sensing system shall use redundancy with the patient´s model to protect the patient from potential threats on sensors.
System	UC1-NMT 17	Non-Functional	Adversarial training shall be used during design to increase their robustness against adversarial conditions.
System	UC1-NMT 18	Non-Functional	Input data should be filtered during operation to remove features (such as addition of specific noise), which renders the data malicious and adversarial.

Table 3: Risk analysis example

The table below compiles in a simple way the results of the risk analysis for each requirement. It summarises the distribution of the risks based on its levels of severity and probability.

The cells of the table in red colour identify the zones of unacceptable risk and the cells of the table in yellow colour identify the zones of acceptable risk, according to what has been established in the risk management plan.

		SEVERITY				
PROBABILITY		*Minimum 1*	*Minor 2*	*Moderate 3*	*Major 4*	*Maximum 5*
Extremely high	*5*					
High	*4*					
Average	*3*					
Low	*2*					
Extremely low	*1*					

Table 4. Risk analysis, severity vs probability

After the application of the risk control measures described for each particular risk, each one of the identified risk levels must be reduced to exit the “red” category.

2.2.2 Pilot 1 technical details

Identifiers

Being pilot 1 a simulated experiment every simulation experiment must have a unique identifier.

TCM (Test Case Manager) should:

- define all circumstances of an experiment
- generate an UNIQUE identifier ID for the experiment in the form “vm.TESTCASE.NUMBER”, where TESTCASE is an identifier of a group of experiments and NUMBER is some unique number of the experiment
- create a data structure (REDIS command in the form “hset ID key value” for all defined attributes/keys)
- publish START command into ID channel (“publish ID START”)
- clock individual cycles of the simulation (controlling mtime and cycle attributes)

For every experiment vm.TESTCASE.NUMBER, there must be:

- a data record in REDIS called vm.TESTCASE.NUMBER (see the following section with information about the contents of this data record)
- a communication channel called vm.TESTCASE.NUMBER; note: channels are so very temporal and each one is intended for a single simulation experiment

Participants will be activated by sending messages via vm.TESTCASE.NUMBER channel. Order of activations should be:

- TCM
- CNT
- PUMP
- PATMOD
- SENSOR
- TCM, ..., and the cycle repeats

Assume a set of participants { A, B, C, ... } in a distributed system. Each participant is allowed to:

- publish a message M (string content) into a channel CH,
- become a subscriber of any channel CH,
- become a generic subscriber of channel description using formatting letters *, ?, etc

The participant gets registered for receiving all messages published in channelA and also for all messages published in channels with names matching the pattern vm.*

All participants subscribing vm.tc.1 (or p-subscribing vm.*) will receive a message "start".

Technically, they receive a tupple (channelID, message), so they know from what channel the message comes.

Participating in the infrastructure

Participants are supposed to p-subscribe the pattern "vm.*".

TCM is going to run a new experiment in test case called TC. This new experiment will be identified by string "vm.TC.1" for example.

TCM fills vm.TC.1 data record in REDIS with all relevant attributes depending on particular test case (using hset commands)

Then, TCM publishes the test case (publish vm.TC.1 start)

All participants are notified about new simulation experiment vm.TC.1 which is about to start.

TCM fires the first iteration of the simulation by calling CNT (publish vm.TC.1 CNT)

"CNT" message activates CNT. Then, CNT is supposed to:

- load the experiment data structure (REDIS: hgetall vm.TC.1)
- decide about anesthesia (initial bolus, infusion flow)
- activate next in the queue, i.e. the pump.

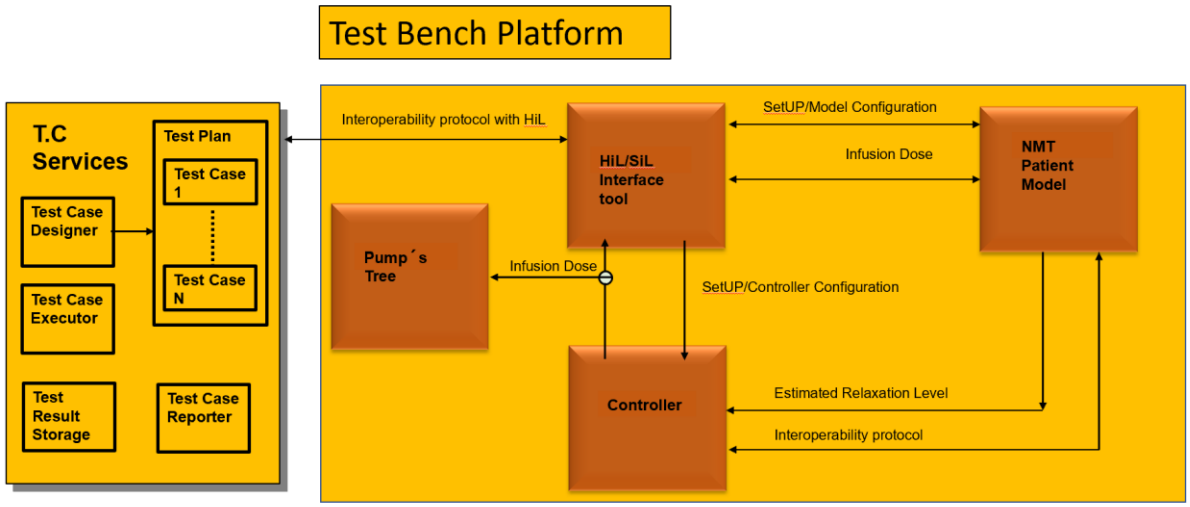


Figure 2: Experiment bench platform

CNT executes to REDIS (hset vm.TC.1 bolus some-value / hset vm.TC.1 infusion some-value / publish vm.TC.1 PUMP)

PUMP gets activated. It does its part (on the vm.TC.1 data record) and calls PATMOD out (publish vm.TC.1 PATMOD)

PATMOD gets activated. The model computes patient's response in TOF/PTC units and outputs all data (hset vm.TC.1 TOF 100 / hset vm.TC.1 PTC 12 / publish vm.TC.1 SENSOR)

SENSOR gets activated. It does its part (like adding noise to the TOF/PTC values) and ends up the cycle by calling TCM (publish vm.TC.1 TCM)

TCM is the last element in the loop. Again, the loop is:

TCM → CNT → PUMP → PATMOD → SENSOR → back to TCM

TCM gets activated. Regarding the experiment specification, TCM decides the next move (to terminate the experiment, next cycle, etc). To start the next cycle, TCM increases the model time to some T2 new value and increments the cycle counter (hset vm.TC.1 mtime T2 / hset vm.TC.1 cycle C2 / publish vm.TC.1 CNT)

To terminate the current simulation experiment vm.TC.1, TCM should publish (publish vm.TC.1 end)

Briefly, an activated component can hget/hset access the central data record called vm.TC1.123 ,for instance:

- CNT sets bolus/infusion attributes and provides so its control above the infusion process
- PUMP can alter bolus/infusion attributes (an eventual model of noise in the infusion)
- PATMOD computes pharmacokinetics/dynamics of the infusion and updates its attributes
- such as TOF, PTC, LinearCM, Cinp (will be described below)
- SENSOR samples outputs from PATMOD and can add some simulated noise. Not implemented yet. SENSOR publishes publish vm.TC1.123 TCM passing the activity token back to TCM.

The different documents provided by BUT include more information and instructions for the use and interoperability by using REDIS database.

The complete technical specifications of the testbench are available in appendix A.

2.2.3 CYLCOMED toolbox involved in the pilot

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.

	Pilot 1
AI-based CMD Behavioural Analysis & Log Monitoring	
↳LOG Analysis	☐
↳Network Analysis	☑
Connected Medical Devices and Services Management Tools	
↳Service management tools	☑
↳Ansible playbook scanner	☑
Identity & Access Management and Data Protection for Connected Medical Devices	
↳IAM Single Sign-In solution Lus4MED	☑
↳Data protection solution FE4MED	☑
Connected Medical Device integrity	
↳Connected medical device integrity solution	☑
CYLCOMED Security Dashboard	
↳CYLCOMED Security Dashboard	☑

Table 5: Recap of the CYCLOMED tools to be integrated and evaluated in Pilot 1

2.3 Pilot purposes

Cybersecurity Toolbox is a major outcome, but training needs will be considered for technicians/clinicians, bridging the gap so that novel IT components are well understood, i.e. The target is producing cybersecurity training materials which are specifically oriented to the context of healthcare stakeholders' use of novel technologies mentioned in previous points.

2.3.1 Pilot expected outcomes

We need 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)
- 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)

2.4 Evaluation strategy

RGB is developing the proposed digital twin approach as a computerised model simulating the interaction with intended patients. H. Niño Jesús (FHUNJ) confirmed interest in participating in this scenario.

In particular, in section 4.1.7. “Device integrity checks tools” of CYLCOMED D3.1, it is described as the preferred implementation of the Medical Equipment to be evaluated in Pilot 1.

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

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

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

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

2.4.1 System simulations

The test described below will be carried out either alone or in the presence of running cybersecurity software, so that we can evaluate the interaction of the APP with the system under normal performing conditions.

To verify the correct behaviour of the Digital Twin, the simulator will be run with different patient configurations. In these tests, an initial dose of relaxant will be applied to the patient and the system will be allowed to evolve (without applying additional doses) until complete recovery. The tests will be carried out in series where a single parameter of the simulation is varied, in order to verify that the effects of said parameter are consistent with clinical experience.

Volume of Distribution (Vd)

When the drug is injected into the patient, it is dispersed in a volume known as the “volume of distribution” and is expressed in ml/kg.

It will be evaluated the evolution of concentration of the drug in plasma (CP) and the neuromuscular transmission (NMT), depending on the different Vd of the patient.

Cp50

Cp50 is the plasma concentration which would, at steady state, produce 50% depression of NMT response. This means that the lower the Cp50, the more sensitive the patient is to the

drug. We will analyse how neuromuscular transmission (NMT) evolves depending on the different Cp50 of the patient, and ascertain that the recovery time increases with a lower Cp50. This is consistent with the actual behaviour of patients, since the patient who is more sensitive to the drug (<Cp50) needs less drug plasma concentration to have the same effect on NMT and therefore takes longer to recover. the NMT.

Initial Dose

We will study the evolution of plasma drug concentration (CP) and how the neuromuscular transmission (NMT) evolve as a function of different initial drug doses.

The higher the dose, the higher the concentration in plasma and therefore the longer the drug remains in the patient, prolonging his recovery.

2.4.2 CYLCOMED tools evaluation: technical aspects

All technical metrics individuated in the CYLCOMED toolbox evaluation are applicable to Pilot 1, and therefore should be monitored and reported.

Moreover the deployment of the toolbox itself will be challenging due to its complex architecture, nevertheless some tools are not intended to be run on the SBC, but rather to monitor the incoming cyber threats, and orchestrate the updates and logging on the swarm of devices.

2.4.3 CYLCOMED tools evaluation: clinical aspects

For pilot 1, the valuable clinical feedback is provided through the continuous cooperation with FHUNJ. Not being deployed in a real life scenario, questionnaires would have a limited impact and are substituted by the discussion between the partners; the insights and major outcomes of this collaborative design process will be reported as additional results.

3. Pilot 2: Cybersecurity for Telemedicine Platforms

In healthcare, the continuous monitoring of patients via telemedicine platforms is necessary in certain scenarios and the role of the "CYLCOMED Pilot 2: Cybersecurity for Telemedicine Platforms" is indispensable in ensuring patient security and privacy.

The adoption of telemedicine platforms brings numerous benefits, including early detection of medical issues, improved adherence to care plans, enhanced quality of life for patients, increased access to healthcare, improved awareness of health conditions for the patient and time and cost reduction for hospitals and healthcare professionals.

Although these platforms offer numerous benefits, they are susceptible to cybersecurity threats due to their distributed nature and the transmission of sensitive patient data across public networks.

This pilot project tackles the crucial vulnerabilities linked to connected medical devices (CMDs) and their gateways. It aims to ensure the integrity of data collected from patients and transmitted to telemedicine platforms. As reliance on telemedicine grows and its exploitation in the healthcare system increases, safeguarding against data breaches, tampering, and misuse of medical devices becomes increasingly paramount.

Ensuring compliance with data protection regulations and cybersecurity guidelines, particularly under the Medical Device Regulation (MDR), adds an extra layer of importance to this pilot.

This pilot effectively utilises nearly the entire array of tools developed by CYLCOMED, highlighting the versatility and effectiveness of the toolbox. The comprehensive integration of these tools plays a crucial role in demonstrating their practical usefulness and resilience across various telemedicine scenarios.

The pilot’s emphasis on both real-world applications and integration is particularly noteworthy, as it offers a simulated testing ground for tools that are currently challenging to be assessed directly with real patients. This strategic approach ensures a comprehensive evaluation of the toolbox, especially for components that require simulated testing due to their sensitive nature. The pilot allows to bring to real-word application the developed tools, underscoring CYLCOMED's dedication to innovation and adaptability in the ever-evolving landscape of telemedicine cybersecurity.

Essentially, this pilot strengthens the cybersecurity infrastructure of telemedicine platforms. It goes beyond just improving patient safety; it forms the basis for the integration of innovative technologies in healthcare settings. Through evaluations in both real and simulated scenarios, the CYLCOMED solution's reliability and effectiveness are ensured, representing a precedent for secure and efficient telemedicine practices in the healthcare system.

3.1 Pilots design process: harmonising complexity

The pilot involves a wide range of stakeholders, thus its design is inherently complex. This requires a brief introduction to the design process, emphasising key milestones and critical considerations.

The design process evolved through the discussions held between the partners (who provide a representative sampling of the healthcare sector) through calls and workshops. At its core, the design process started with a clinician-centric perspective and grew from the tangible needs expressed by clinicians, laying a robust foundation for the pilot's conceptualization.

The design phase in the CYLCOMED project started with a series of presentations crafted for our clinically engaged partners. These sessions served to offer insights in the technology and to reveal its potential applications in the realm of telemedicine cybersecurity. A workshop with technical partners and one-to-one interviews held a pivotal role, representing a crucible where all partners collectively engaged in discussions, shaping the pilot by balancing definition of clinical demands, technical feasibility evaluations, and regulatory compliance.

The design process reflects the challenges faced when introducing new technologies into the hospital ecosystem, highlighting the complexities of seamlessly integrating novel tools in these contexts. The design included a deep focus on the subtleties of privacy, ethics, and clinical workflows.

3.2 Scenario details

In this scenario the cyclomed toolbox will be tested by improving the MD MHP (Mediaclinics Health Platform, see appendix B for technical overview of its capabilities) in the context of paediatric patients, in particular the clinicians will leverage the remote monitoring capabilities of the platform, recording and evaluating vital parameters recorded from the young patients.

The challenges tackled by CYLCOMED in this scenario are multiple, the toolbox will enable the telemedicine platform with the possibility of monitoring and analysing real time log and network data, in order to detect an incoming attack.

It will also provide a robust single sign-on solution and the possibility to offer end-to-end encryption over sensitive data.

	Pilot 2		
	Pilot 2	Sub pilot A	Sub pilot B
AI-based CMD Behavioural Analysis & Log Monitoring			
↳LOG Analysis	☑	☑	☑
↳Network Analysis	☑	☑	☑
Connected Medical Devices and Services Management Tools			
↳Service management tools	☐	☐	☐
↳Ansible playbook scanner	☐	☐	☐
Identity & Access Management and Data Protection for Connected Medical Devices			
↳IAM Single Sign-In solution Lus4MED	☑	☑	☑
↳Data protection solution FE4MED	☑	☑	☑
Connected Medical Device integrity			
↳Connected medical device integrity solution	☐	☐	☐
CYLCOMED Security Dashboard			
↳CYLCOMED Security Dashboard	☑	☑	☑

Table 6. Summary of CYLCOMED toolbox usage in pilot 2

As clarified in the above table, Pilot 2 and its sub pilots will integrate and validate most of the CYLCOMED toolbox, in particular it'll not include `Connected Medical Devices and Services Management Tools` due to deployment infrastructure, these are expected to be cloud based tools and, while MHP is cloud capable, the deployment sites has expressed the need to have all software locally deployed, making these tools unsuitable. Also the `Connected Medical Device integrity` tool has been specifically designed toward hardware based medical devices and therefore is not suitable for the MHP platform or the MDs it integrates.

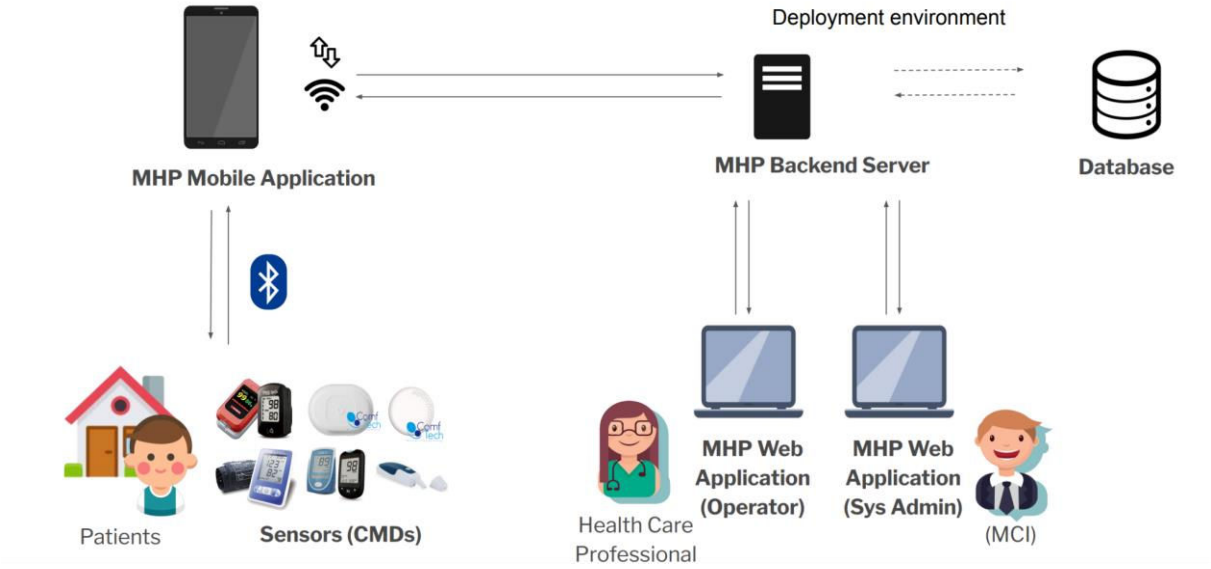


Figure 3: MHP Architecture

Due to the complexity and the broad range of needs, the logical conclusion has been to split Pilot 2 in two distinct deployments.

The first deployment, (deployment A from now on), is focused on leveraging real-world scenarios. It involves executing a live clinical observational study with actual hospitals and patients. In this deployment we operate within the parameters of the existing platform certification, utilising cybersecurity tools having minimal impact on the current infrastructure. Following established clinical protocols, deployment A ensures the integration of the tools into a real-world telemedicine environment.

The primary focus of deployment A is the exploitation of the MHP telemedicine platform to monitor health conditions of paediatric cardiac patients. It is important to note that, as the clinical protocol is currently in the finalisation phase, minor adjustments can be expected to further refine and enhance efficacy.

In another way, the second deployment (deployment B from now on) takes a broader approach, encompassing the entire telemedicine integration and testing process without direct involvement from real patients and hospitals. Deployment B uses MHP as a telemedicine platform too, but the application is deployed in a controlled environment. For this deployment the evaluation spans to the full suite of cybersecurity tools, including sub-pilots that specifically focus on ambulance transit scenarios and AI model analyses. This comprehensive testing methodology enables a complete assessment of the CYLCOMED solution's effectiveness and adaptability across diverse telemedicine scenarios. By excluding real patients and hospitals, it allows for a controlled yet expansive evaluation, ensuring the robustness, scalability and security of the solution in various telemedicine contexts.

Through the divided deployments, the pilot aims to collect insights from the real-world scenario while maximising the refinement of project outcomes.

The real-world deployment (deployment A) unfolds as an observational clinical study within existing hospital ecosystems, providing the integration of CYLCOMED tools. The detailed specifics of the clinical study are encapsulated within the clinical protocol, whereas deployment A is well defined in this document, in order to specify the information outside the scope of the clinical protocol. In this way, the pilot helps to bring the CYLCOMED tools within the hospital environments, even considering procedural and regulation requirements of collecting real-world data.

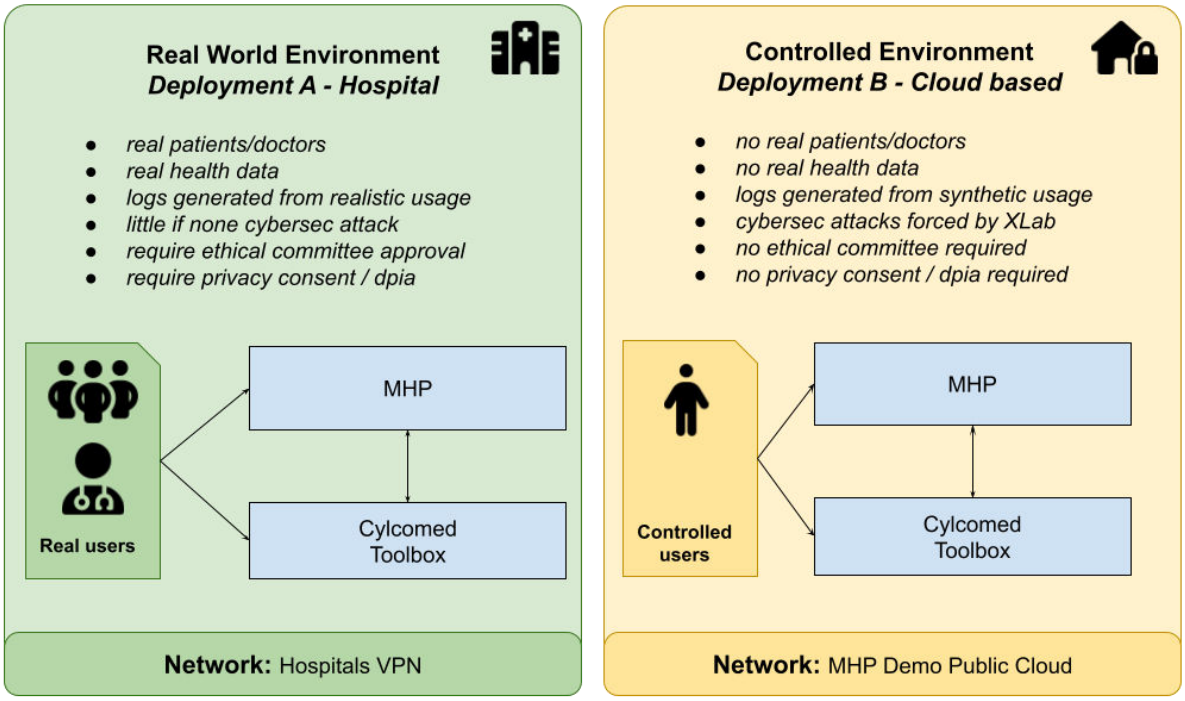


Figure 4: Schema describing the two different deployments of Pilot 2

3.2.1 Deployment A: real-world environment

The real-world environment will challenge the whole CYLCOMED ecosystem front facing fragile end-users such as paediatric children and their doctors. Therefore, the whole testing activity has to be approved by the ethical committee. To improve the quality of the overall experience the CYLCOMED consortium has been challenged with strict requirements, in particular to isolate the solution with a local deployment, and use already certified MDs as foundation.

- These limitations have been tackled during the common work of the partners, in particular:
- Pilot 2 will run over the MHP platform which has been previously certified by MCI in MDD (under the name Telecare Connect). The same software will be certified under MDR (now with the name MHP to reflect the new branding) before the pilot begins.
- MHP platform is using a set of off-the-shelf sensors all certified under MDD or MDR.
- Each hospital will be provided with a dedicated machine, provided by the consortium with the CYLCOMED equipment budget. This machine will be prepared with all the necessary applications and technical support will be provided over a dedicated VPN.
- All the data collected, from the three different hospitals, will be sent to CUB at the end of experimentation. Here partners will be able to access data and perform ML activities.

Within deployment A, clinicians actively engage with a certified version of the platform, aligning seamlessly with existing standards. The meticulous registration of technical data, including logs, serves a dual purpose. It generates an instrumental dataset for the refinement and optimization of tools, but it also unveils pivotal insights into clinicians' preferences and needs, offering a tangible understanding of the tool characteristics that are considered essential for effective integration into the clinical workflows. This deployment can also provide the basis for a better involvement of HIS technicians, providing the basis for discussion about protection and mitigation measures to be adopted by the hospitals.

3.2.2 Deployment B: controlled environment

Deployment B is used to assess the solution in a controlled environment. Deployment B consents to evaluate the impact of vulnerabilities or potential cybersecurity risks on patient safety, patient privacy and regulatory compliance. The assessment is considered most effective when it reflects the operational environment and intended clinical use cases of the product [28].

In the controlled environment of Deployment B, the pilot broadens into a comprehensive telemedicine integration and testing process. This phase requires no direct interaction with real patients and hospitals utilise the entirety of the CYLCOMED cybersecurity tool suite. The evaluation extends its arms to sub pilots dedicated to transit ambulance scenarios and AI model analyses, creating a controlled yet expansive evaluation ground.

The controlled environment will be then used to ensure the robustness, scalability, and security of the CYLCOMED solution across diverse telemedicine contexts. This strategic approach facilitates a thorough examination of the solution's effectiveness and adaptability, setting the stage for a seamless integration into the dynamic environment of telemedicine cybersecurity.

3.2.3 Sub pilots

The Sub pilots expand pilot 2 to cover an even broader area. In particular, Sub pilot A will explore the possibility of training machine learning models within the hospital network to enhance threat analysis, a key feature of the analysis and monitoring tools. Meanwhile, Sub pilot B will expose the solution to an even more sensitive environment, such as the transportation of a patient between two hospitals. In this scenario, the ability to detect anomalies on the network becomes crucial for the protection of patient data. Due to ethical and organisational requirements, it is possible that these sub-pilots will be deployed in a controlled environment.

3.2.4 Risks and threats

The fundamental threats in the scenario are outlined in the technical documentation of the platform, emphasising cybersecurity vulnerabilities. These identified threats will go through review at the conclusion of the process, if possible aligning with the methodologies suggested in Deliverable D4.1 to ensure robust mitigation strategies and enhanced security measures.

The technical documentation of the medical device (MHP telemedicine platform) is written using the guidelines of the European Medical Device Regulation 2017/745, which requires manufacturers to plan and implement a Risk Management and Analysis framework based upon the “ISO 14971 Medical devices — Application of risk management to medical devices” standard. The methodology that has been followed – which is suggested when the main features and software components have been identified and the software architecture has been depicted – foresees a “bottom-up” approach named FMEA - Failure Mode and Effect Analysis: this approach consists in analysing each component and the consequences of its possible failure for the patients’ safety. A brief breakdown of the FMEA model is outlined below:

1. Analysis of the main features of the Medical Device to identify all the aspects that can impact the patients’ safety (MCI uses ISO/TR 24971:2020 - Medical devices — Guidance on the application of ISO 14971 to focus on the correct characteristics)
2. Once these have been identified, all the hazards associated with them must be assessed, considering the intended use of the MD or any reasonably foreseeable misuse by the users; each hazard can belong to different categories, such as energy hazards (e.g. leaks, magnetic fields etc), performance hazards (related to data,

diagnostics, communication, cybersecurity etc), biological/chemical contamination, and so on

3. For each identified hazard, the foreseeable events sequences that can lead to specific harms for the patients must be considered: more than one hazard can lead to the same harm, and many harms can origin from the same hazard
4. For each identified sequence, the manufacturer must evaluate (quantitatively and qualitatively) the associated risk(s). Many standards require that each risk is evaluated and expressed in terms of powers of 10 to simplify the subsequent application and evaluation of counter-measures
5. Once every risk has been identified and evaluated, for each risk the manufacturer needs to apply and implement a counter-measure which should preferentially prevent the risk from arising; if the risk can't be prevented, the countermeasure should mitigate the risk considering the overall use of the MD; if the risk can't be mitigated or contained, the counter-measure should focus on protecting the users/patients. The counter-measures can be technological, procedural or documentary. Each counter-measure must be evaluated to guarantee its adequacy to the risk
6. The manufacturer carries out a new assessment on the residual risk after the application of the counter-measures. If the resulting risk is below the critical threshold defined by the manufacturer, the Risk management is complete and will be reviewed at least annually (after major changes, after new information about safety arises from the market, etc). If the residual risk is above the threshold, the design process must be reviewed to adjust the product features.

For peculiar risks (e.g. cybersecurity-related ones for software manufacturers, such as MediaClinics Italia) the manufacturer can avail itself of domain-experts, external subject. E.g. MCI has been supported by a Cybersecurity company to assess cybersecurity risks associated with the MHP platform. The manufacturer needs nevertheless to be able to prove the expertise of the subject carrying out the analysis/evaluation.

3.3 Scenario purposes

3.3.1 Deployment A: expected outcomes

In deployment A, the journey kicks off with the substantial challenge of navigating the complex terrain of ethical considerations to secure the approval of a local ethics committee of the clinical sites in the CYLCOMED consortium.

Securing the endorsement of ethical committees is not an easy task, particularly in the field of telemedicine applications. The challenge lies in aligning the protocol with stringent ethical standards, ensuring patient welfare, data privacy, and compliance with regulations.

The primary importance of conducting this observational prospective clinical study in a real telemedicine setting cannot be overstated. Gathering data in an authentic telemedicine environment provides a unique opportunity to unravel cybersecurity threats in hospitals.

Since the cybersecurity requirements change depending on the medical condition being monitored and devices being used, validating the cybersecurity measures in a real world scenario is necessary. This provides valuable insights that are nearly impossible to gain with theoretical considerations and simulations alone.

Definitely, it allows to create a crucial link between technical advancements and clinicians' perspectives on cyber threats. By immersing the cybersecurity tools in an actual telemedicine application, clinicians gain first hand insights into the challenges posed by evolving technologies. This experiential approach not only strengthens the technical robustness of cybersecurity measures but also bridges the perceptual gap between clinicians and cyber threats associated with emerging technologies.

Deployment A, therefore, serves as the perfect nexus between the clinical world and the technological realm. It not only validates the practicality and efficacy of the CYLCOMED solution but also fosters a mutual understanding among clinicians and technical experts. This relationship is instrumental in fortifying hospitals against cyber threats, ensuring that advancements in technology align seamlessly with the clinical perception of cybersecurity challenges in the dynamic environment of telemedicine exploitation.

3.3.2 Deployment B: expected outcomes

While still in a controlled environment, integrating the entire CYLCOMED toolbox into a fully operational telemedicine platform marks a significant leap forward for the future of cybersecurity in healthcare. This phase goes beyond the confines of real patients and hospitals, focusing on seamlessly incorporating the cybersecurity suite into platforms that clinicians regularly use. This integration offers a crucial opportunity for practical application and feedback, allowing clinicians to experience the tools tested in their daily practice during the real-world deployment.

By embedding the CYLCOMED toolbox into a platform known by the clinicians, Deployment B facilitates a comprehensive evaluation process. Integrating these tools into platforms already familiar to clinicians simplifies their ability to assess the impact on their routines and allows the clinicians to provide valuable feedback on the effectiveness and user-friendliness of the cybersecurity measures without requiring the involvement of real patients and thus without real data protection requirements. Such insights are essential to refine and optimise the toolbox suite for practical usage.

Moreover, this comprehensive integration lays the groundwork for future applications of the CYLCOMED solution in diverse healthcare settings. Clinicians, by experimenting with the

entire toolbox in a protected environment can actively contribute to the ongoing evolution of the cybersecurity framework.

This practical approach not only validates the technical strength of the tools but also ensures they seamlessly align with clinicians' expectations and workflows, fostering clinical usability of technology. In essence, Deployment B represents a crucial step towards the meaningful integration of cybersecurity measures into everyday healthcare practices.

3.4 Stakeholders

In Pilot 2 a broad range of stakeholders need to be considered in order to analyse the awareness level regarding cybersecurity in the healthcare system from different perspectives.

By implementing a portion of the pilot within hospital settings, actors that tech providers are used to interacting with (e.g. Hospital Service - IHS) and not so well known actors, such as ethical committees, are involved. This approach extends the scope of the analysis and ensures a more accurate understanding of the healthcare system.

In the following sections, a brief overview of the identified stakeholders is presented. The stakeholders will be involved in different aspects in the evaluation strategy, it is critical for a representative testing that the stakeholders are selected by their expected competences (see appendix c).

Stakeholder	Area of involvement	Pilot scope
Clinicians	Clinical	Usability/acceptability
Patients	Clinical	Usability/acceptability
Ethical committees	Clinical	Alignment with ethics and regulation but response is yes/no
Healthcare administrators	Clinical	Cybersecurity strategies
HIS technicians	Clinical / Technical	Intervention in case of threat
Researchers and Developers	Technical	Future development and innovation
Technology providers	Technical	Design and implementation
Medical Device Manufacturers	Technical	Design and implementation

Table 7. Pilot 2 identified stakeholders

3.4.1 Technology stakeholders

Technology stakeholders obtain from the development of this pilot a comprehensive understanding of clinical aspects as a significant output of the project. These insights enable them to effectively address the practical needs of hospitals and healthcare professionals. Importantly, this understanding is achieved while adhering to existing regulations and technological standards related to data protection and the development of medical devices.

Technology stakeholders can tailor their solutions to align with the operational requirements of healthcare environments. This heightened awareness of clinical functional requirements allows for the creation of technology solutions that are not only innovative but also practical and responsive to the dynamic challenges faced by healthcare institutions and professionals.

Moreover, the emphasis on compliance with cybersecurity and data protection regulations ensures that the developed technologies prioritise the security and privacy of patient information. This allows the development of technological solutions meeting the ethical and legal requirements associated with healthcare data management.

This dual commitment to clinical understanding and adherence to regulatory and technological standards positions technological stakeholders as valuable contributors to the pilot, facilitating the delivery of advanced and secure technology solutions that positively impact patient care and clinical professionals' workflow.

3.4.2 Clinical framework stakeholders

The involvement of clinical stakeholders is essential for a comprehensive evaluation of the impact and effectiveness of CYLCOMED solution. These stakeholders can assess how the project aligns with healthcare practices and its potential implications on patient care. Their assessment provides important insights into the practical aspects of implementing cybersecurity tools within clinical environments. This includes evaluating the feasibility of integrating new technologies, understanding potential workflow disruptions, and assessing the overall impact on patient outcomes. The involvement of clinical stakeholders ensures that the project outcomes are not only technically effective but are also aligned with the specific needs and challenges faced by healthcare professionals.

Furthermore, the enhancement of the awareness about cybersecurity issues among the healthcare professionals can be considered as another significant outcome of the project, since it fosters proactive measures to safeguard patient health data.

3.5 Pilot specific requirements

Additionally to the general aspects of tools requirements, and the pilot requirements, Pilot 2 design process has proved itself as a valuable opportunity to learn about additional non-functional requirements.

It is worth mentioning the most important functional requirements stem from the necessity to seamlessly integrate cybersecurity tools into existing clinical workflows. These tools must not disrupt patient care processes or compromise the efficiency of medical staff, demanding verification. Data security and privacy requirements involve being able to guarantee secure data transmission, storage, and access by the telemedicine platform. In addition to these technical safeguards, compliance with data protection regulations and ethical standards are required.

3.5.1 Clinical protocol

The major Ethical Committee related challenge is due to the implementation of cybersecurity tools in a healthcare setting, especially involving real patients. The primary concerns may include ensuring patient privacy, obtaining informed consent, and minimising any potential risks associated with the use of novel technologies. Ethical committees may analyse the protocol's clarity on these issues, demanding stringent measures to protect patient data and guaranteeing that participants are well-informed and voluntarily engaged.

Obtaining the Clinical Protocol Approval is an essential requirement for any clinical study and can be considered a substantial achievement.

It signifies that the research design adheres to the highest ethical standards, prioritising patient welfare and privacy. The approval ensures that the study adheres to the requirements for participant data protection, informed consent, study design and methodology, risk-benefit balance and compliance with regulations. The approval process involves a rigorous examination of the proposed study, fostering confidence in the research's integrity and its potential to contribute valuable insights in the fields of telemedicine and cybersecurity. The approval obtained by the ethical committee validates the project's commitment to ethical conduct, underscoring its credibility and fostering meaningful and responsible research.

The clinical protocol is a meticulously outlined plan that delineates the objectives, methodology, participant selection criteria, and ethical considerations for conducting a clinical study. In the context of the CYLCOMED project, the clinical protocol serves as a comprehensive guide for implementing cybersecurity tools in a real telemedicine environment. It specifies the study objectives and its design, ethical and regulatory considerations and the definition of how clinicians will integrate and utilise the CYLCOMED solution in their clinical practices, ensuring a systematic approach to evaluate the impacts on patient care and data security.

3.5.2 Deployment on premises

In deployment A of the project, a significant contribution comes from a partnering organisation providing specific equipment. This equipment serves as a practical bridge between the clinical and technological realms. By furnishing hospitals with this specialised hardware, Hospital Information Systems (HIS) gain invaluable hands-on experience, delving into the integration of new technologies. This direct interaction enhances their understanding of the equipment's requirements, fostering insights and knowledge crucial for adoption in the daily practices. The equipment, therefore, acts as a catalyst for collaboration, being a shared space for clinicians and HIS technicians to collaboratively exploit the implementation of cutting-edge cybersecurity tools, ultimately fortifying the hospital's digital infrastructure.

3.6 Evaluation strategy

Objective of evaluation is to assess the technical performance of CYLCOMED cybersecurity tools in a real telemedicine environment.

Evaluation strategy for Pilot 2 will be divided in two main sections, one tailored to the technical aspects that may be difficult for the end-user to perceive, and one tailored to every impact on end-user perspective. This will also enable the selection of more focused evaluation tools that better depict the KPI (key performance indicator) of each.
It is worth mentioning that the proper integration of the CYLCOMED toolbox with the telemedicine platform and its validation with software testing methodologies are considered a preliminary step that is taken for granted in this document.

3.6.1 CYLCOMED tools evaluation: technical aspects

By running in the real-world environment it'll be possible to evaluate the different performances with respect to running in a synthetic environment. This is interesting from a technical point of view, due to the natural differences that a real infrastructure can provide, but also to measure the human factor impact on the efficiency of some tools (ie. Logs analysis, the logs produced in the real environment will be more diversified compared to the controlled environment).

To improve the controlled environment as much as possible, some of the experience derived from the real-world environment will be exploited and subsequently distilled into scripted behaviours.

It must be noticed that all technical metrics individuated in the CYLCOMED toolbox evaluation are still applicable to Pilot 2 but, of course, due to the strict limitations imposed by the hospital infrastructure (network isolation ie), these metrics could be limited in efficiency and their result misleading in the real-world environment. This can be better known once the infrastructure definition is finalised. Therefore, the final version of this analysis will be perfected into the upcoming deliverables.

3.6.2 CYLCOMED tools evaluation: clinical aspects

We want to evaluate the CYLCOMED toolbox also from the user experience point of view, we will monitor both the usability of the tools that interact with the medical staff and the impact on their day to day clinical practice and the perceived security.

The main tools we plan to use are usability testing and questionnaires/interviews, since they serve as versatile tools for both Deployment A and B, providing a structured approach to gather valuable insights on usability, impact, security, education, and continuous improvement, ultimately enhancing the success and adaptability of the CYLCOMED cybersecurity solution.

3.6.2.1 Usability

Follows the list of KPIs from a usability perspective

1. User Experience Assessment: In the clinical study, patient questionnaires capture real-time insights into the usability and impact of cybersecurity tools on their telemedicine experience.
2. Privacy and Security Perception: Patients share perceptions on the privacy and security of their medical data, contributing to refining cybersecurity measures.

3. Feedback on Data Transmission: Assess patient perspectives on the efficiency and effectiveness of data transmission, crucial for real-time monitoring.

3.6.2.2 Clinical practice

Follows the list of KPIs from the clinical practice perspective:

1. Usability and Integration Assessment: Relevant clinical stakeholders evaluate the usability of cybersecurity tools within their workflow during the clinical study. Ongoing questionnaires facilitate feedback on tool integration and usability as clinicians incorporate cybersecurity measures into everyday practice.
2. Impact on Clinical Workflows: Clinicians provide insights into how the cybersecurity tools impact their daily clinical workflows, ensuring minimal disruption. Questionnaires help gauge sustained workflow integration, refining tools to align seamlessly with clinicians' routine practices.
3. Security Effectiveness Feedback: Relevant clinical stakeholders assess the effectiveness of cybersecurity tools in securing patient data and ensuring the integrity of medical information.
4. Educational Impact: Relevant clinical stakeholders share insights into the educational impact of the cybersecurity pilot on their understanding of cyber threats.
5. Continuous Improvement Insights: Relevant clinical stakeholders feedback during the clinical study contributes to iterative improvements in tool functionality.

Conclusions

The CYLCOMED project's ongoing design and evaluation process represents the effort of the partners to set the most meaningful pilots and provide the most valuable information and results from the process.

This report captures the current status, detailing the two pilots, their characteristics, expectations and contribution to the project. The Involvement of diverse stakeholders is represented in the variety of aspects needed to complete this document and ensures a holistic assessment.
A noteworthy result of the CYLCOMED project is that the designed pilots are able to embrace a really wide representation of the digital health sector, allowing for the CYLCOMED toolbox to be fully evaluated and from numerous different points of view.

It is important to note that this is a segment of a broader process that could provide insights for a comprehensive prevention strategy, with detailed reporting in D6.2 and D6.3, offering an encompassing overview of CYLCOMED's journey in telemedicine cybersecurity and its evaluation.

References

[1]	T. Walker, Interoperability a must for hospitals, but it comes with risks, Manag. Healthc. Exec. (2017) http://managedhealthcareexecutive.modernmedicine.com/managed-healthcare-executive/news/interoperability-must-hospitals-it-comes-risks (accessed February 28, 2018).
[2]	R. Kam, The human risk factor of a healthcare data breach - Community Blog, Heal. IT Exch. (2015). https://searchhealthit.techtarget.com/healthitexchange/CommunityBlog/the-human- risk-factor-of-a-healthcare-data-breach/ (accessed April 10, 2018).
[3]	Márquez, Gastón & Astudillo, Hernán & Taramasco, Carla. (2020). Security in Telehealth Systems From a Software Engineering Viewpoint: A Systematic Mapping Study. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2964988.
[4]	D. Kotz, C.A. Gunter, S. Kumar, J.P. Weiner, Privacy and Security in Mobile Health: A Research Agenda., Computer (Long. Beach. Calif). 49 (2016) 22–30. doi:10.1109/MC.2016.185.
[5]	R. Milliman, Nine in 10 NHS trusts still use Windows XP, IT Pro. (2016). http://www.itpro.co.uk/public-sector/27740/nine-in-10-nhs-trusts-still-use-windows-xp (accessed February 19, 2018).
[6]	K. Sengupta, Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images, Indep. (2017). http://www.independent.co.uk/news/uk/crime/isis-islamist-hackersnhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html (accessed February 19, 2018).
[7]	G. Bell, M. Ebert, Health Care and Cyber Security, 2015. G. Bell, M. Ebert, Health Care and Cyber Security, 2015. https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf.
[8]	https://www.ncsc.gov.uk/collection/10-steps
[9]	Hijmans, Hielke and Raab, Charles D., Ethical Dimensions of the GDPR (July 30, 2018). in: Mark Cole and Franziska Boehm (eds.), Commentary on the General Data Protection Regulation, Cheltenham: Edward Elgar (2018, Forthcoming) , Available at SSRN: https://ssrn.com/abstract=3222677
[10]	Johan Rochel, Ethics in the GDPR: A Blueprint for Applied Legal Theory, International Data Privacy Law, Volume 11, Issue 2, April 2021, Pages 209–223, https://doi.org/10.1093/idpl/ipab007
[11]	Available at https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm

[12]	Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.
[13]	Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006.
[14]	Article 19. Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.
[15]	Horizon 2020 Programme Guidance: How to complete your ethics self-assessment, European Commission, February 2019.
[16]	Ethics and data protection, European Commission, November 2018.
[17]	EC Guidance note on informed consent. Available at: https://ec.europa.eu/research/participants/data/ref/fp7/89807/informed-consent_en.pdf
[18]	Ethics in Social Science and Humanities, European Commission, October 2018.
[19]	The European Code of Conduct for Research Integrity, ALLEA - All European Academies.
[20]	https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[21]	https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[22]	https://www.enisa.europa.eu/publications/health-threat-landscape
[23]	IBM Security, Cost of a Data Breach Report 2023, https://www.ibm.com/reports/data-breach
[24]	Silver JK, Binder DS, Zubcevik N, Zafonte RD. Healthcare hackathons provide educational and innovation opportunities: a case study and best practice recommendations. J Med Syst. 2016. https://doi.org/10.1007/s10916-016-0532-3.
[25]	https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-psychotherapy-centre-vastaamo-data-protection_en
[26]	Biasin, Elisabetta and Kamenjasevic, Erik, Cybersecurity of Medical Devices: Regulatory Challenges in the EU (September 30, 2020). The Future of Medical Device Regulation: Innovation and Protection, Cambridge University Press, 2020, Available at SSRN: https://ssrn.com/abstract=3855491 or http://dx.doi.org/10.2139/ssrn.3855491
[27]	Chowdhury, N. (2014). Conceptualizing Multilevel Regulation. In: European Regulation of Medical Devices and Pharmaceuticals. Springer, Cham. https://doi.org/10.1007/978-3-319-04594-8_2
[28]	https://www.modbus.org/

[29]	https://github.com/logpai/loghub/blob/master/BGL/README.md
[30]	https://github.com/logpai/loghub/blob/master/HDFS/README.md
[31]	Playbook for threat modeling medical devices, MITRE, November 30, 2021.

Appendix A - Technical details for the testbench platform of VisionAir®

Description of the input and output data for the testbench platform

The following list of input and output data are derived of the output file generated by the execution of an experiment:

- drug
- weight
- targetCinpLow (*)
- targetCinpHi (*)
- targetPTCLow
- targetPTCHi
- CNTStrategy,
- repeStep,
- repeBolus
- fwRange
- ibolusMg
- wcoef
- bolus
- infusion
- infusionLimit
- unitVd
- absoluteVd
- EC50
- Cinp
- PTC
- TOF
- TOFCount
- TOFRatio
- ConsumedTotal
- RecoveryTime
- mtime
- cycle
- testCase
- expID
- ptcOutr
- ptcAboveHi
- ptcBelowLow
- Vd
- sysInfo

(*) These parameters are not displayed in the data output examples. If they are used, it is only when the strategy fwSim is used.

The following sections describe each data by groups. Some of these sections can include information about other data, but we are not sure if they are used or not.

Basic patient's attributes

- weight [integer - kg]. Relevant just for computing the initial bolus when CNTStrategy=basic or CNTStrategy=fwsim.
- age [integer - years]

- gender ["male", "female"].

Note: Age and gender have no effect in the model yet. Perhaps it can be found any significant literature describing PK/PD aspects of Rocuronium regarding the age and gender of patients. There are not any variable defined in the source code with these names.

Pharmacological patient's attributes

- drug; ["ROC", "CIS"]. Only ROC (Rocuronium) is implemented at the moment.
- unitVd [integer - mL/kg]. Unit Volume of Distribution in mL per kg of weight. Default: 38 mL/kg.
- absoluteVd [integer - mL]. Default: 0 mL.
- EC50 [double - µg/mL]. Coefficient for Cinp Effect transformation. EC50 is the concentration of drug in blood plasma (Cinp) resulting in 50% effect of the drug, i.e. TOF0=50 (TOF is in <0,100> [%]). Unit is micrograms per mL of Vd. Default value for Rocuronium: 0.823 µg/mL.
- wcoef [double - <0,1>]. Meaning the ratio of muscles in weight. Relevant for determination of initial bolus. Default: 1.0

Note: if unitVd is nonzero, then patient's Vd is determined using unitVd and weight. Otherwise, absoluteVd should be set (in mL).

An associated value is Vd of the central compartment, i.e. for computing the drug concentration in the blood plasma. Vd is computed in one of the following ways:

- Vd = unitVd [mL/kg] * Weight [kg], [mL] in total
- if unitVd = 0, then Vd := absoluteVd [mL] assuming absoluteVd is NOT ZERO.

Controller settings and target anaesthesia

- ibolusMg [double – mg/kg]. Dosage of initial bolus per kg of weight. Default: 0.6 mg (for a "standard person", otherwise set an appropriate wcoef).
- CNTStrategy; ["none", "basic", "basicInfusion", "fwsim", "fwsimPTC", "fwsimPTCInfusion", “Anal”, “PB”]. CNT will implement various experimental algorithms for controlled neuro-muscular blockade (NMB).
- targetPTCLow, targetPTCHi [integer]. High and Low ends for controlled value of PTC.
- targetCMHi, targetCMLow [integer]. High and low ends for controlled effect in the linear scale.
- targetCinpHi, targetCinpLow [double]. High and low ends for controlled concentration of the drug in plasma (Cinp).

Note: initial bolus is defined in milligrams of drug. Both bolus and continuous infusion are administered in diluted form (a solution) intravenously. By default, it is 10mg of Roc per 1mL of solution. Can be made also configurable if needed.

Note: targetCMHi/Low is not to be implemented in that early demo. Perhaps, the linear scale is still not very defined. Concentration Cinp is objective and should be preferred. targetCinpHi/Low us defined in the application but these variables are not used effectively. targetPTCHi/Low are not defined in the documents, but they are mentioned as controller settings for some control strategies

According to the information provided, the initial bolus is scheduled by the controller (CNT) if CNTStrategy is "basic" or "fwsim". The value of the absolute initial bolus is

bolusMG := IbolusMg * weight * wcoef [mg]

Then, bolusMG [mg] is converted to [mL] of liquid solution according to the concentration used.

Advanced CNT attributes depending on CNTStrategy

CNT Strategy can be different and the relevant attributes depend on the type of strategy. The following strategies are described in the documentation provided by BUT:

- “none". No infusion at all.
- "basic". Initial bolus. Then CNT administers periodic boluses set by “repeStep [s]” (time interval between boluses) and “repeBolus [mL]” (amount of bolus). This is a conventional approach and the NMT blockade goes well if RepeBolus is determined correctly. Actually it is nor performing an actual control because it only defines a scheduled set of boluses.
- "fwsim". Initial bolus. Then CNT simulates the patient and sets boluses if Cinp drops below targetCinpLow (it must be >=0, for example: 2). fwRange is relevant.
- "fwsimPTC". Initial bolus. CNT adds another bolus if patient's PTC exceeds targetPTCHi (it must be >=0) where PTC is an integer 0..15. fwRange is relevant.

The following strategies are defined in the source code, but the explanation about their operation is an assumption.

- "basicInfusion". Similar to basic strategy, but with some differences related with the valor of infusionLimit.
- "fwsimPTCInfusion". Similar to fwsimPTC strategy, but with some differences related with the valor of infusionLimit.
- “Anal”. The operation of this strategy is not clear. It could use some type of linear scale. It seems to administer a bolus when the simulated patient is above targetPTCLow. It uses the repeStep value.
- “PB”. Strategy of control suggested by Peter Biro base in the formula nBolus = (current − target) x 0.04 x iBolus. It uses the repeStep value.

The attributes associated to CNTStrategy are:

- repeBolus [integer - mL]. Repetitive bolus administered in repeStep [s] steps after the initial bolus at mtime=0.
- repeStep [integer – s]. Time interval between regular periodic boluses
- fwRange [integer - s]. Time range for forward simulation

CNT integrate PATMOD as its internal part so CNT can read its internal simulation state and the current reaction of patient to the infusion and also his/her future response.

With CNTStrategy=fwsim, CNT:

- schedules an initial bolus in the same way as with =basic strategy.
- in every cycle of simulation, after the initial bolus (mtime=0), CNT starts an internal simulation with PM "looking ahead/forward"

Forward Simulation: CNT simulates future cycles from the current mtime till mtime+fwRange [s]. The simulation runs PATMOD, i.e. the evolution of the PK/PD aspects, the concentration of Roc in blood plasma (Cinp) specifically. Future evolution of Cinp is checked with the given range of wanted <TargetCinpLow, TargetCinpHi>.

This algorithm is factually a minimization of bolus needed to keep the Cinp in the predefined range in the time horizon.

Typically, the first cycle is with addBolus=0, if Cinp is above TargetCinpLow after FwRange forward simulation, then no bolus is needed in the next FwRange seconds.

Having that state, CNT can continue simulating in time forward till mtime+fwRange and simulate future effect of previously administered relaxation drug. It can numerically predict the moment when some condition arises (like the drug effect drops under the preset bounds - targetCinpLow). fwSim algorithm determines bolus at mtime as the minimal bolus B to be administered at mtime so that drug effect at mtime+fwRange does not drop under lower target.

Relevant attributes for this control strategy are :

- CNTStrategy=fwsim
- initial bolus as above
- fwRange [s], the range of looking ahead.
- TargetCinpLow, TargetCinpHi [ug/mL]

Simulation system data

- mtime [integer - s]. Time between cycles
- cycle [integer]. Number of cycles.

Note: Model time (mtime) and cycle number MUST be strictly growing sequence of values. PATMOD and CNT have their internal simulation state which assumes that strictly.

Outputs from PATMOD

- TOF [integer - range <0,100%>]. Amplitude of the first twitch of Train of four (TOF) measurement.
- TOFCount [integer - range <0,4>]. Number of twitch pulses of the TOF measurement
- TOFRatio [integer - range <0,100%>]. Ratio between the fourth and the first twitch of the TOF measurement.
- PTC [integer - range <0,15>]. Measurement called Post Tetanic Count taking place when TOF[0] drops to zero.
- Cinp [double - µg/mL]. Concentration of the drug in plasma and also the source for pharmacodynamics (computing the effect of drug in the plasma) . Nonnegative number.
- LinearCM [integer – range <0,32>]. Effect of the drug projected to our virtual scale (covering TOF ratio, TOF count and PTC values).
- ConsumedTotal [double - mL]. Cumulative consumption of the drug in volume of infusion solution during the experiment. Summary of all boluses and a numerical integral of an infusion if implemented.
- RecoveryTime [s]. Expected time to 95% TOF, an almost full recovery and clearance of the drug.

Other attributes

The documents describe other attributes:

- testcase [text]. Identifier of a group of experiments.
- bolus [double]. It seems that it indicates the volume of the bolus to infuse according to the controller at each moment (probably in mg).
- infusion [double]. It seems that it indicates the infusion rate according to the controller at each moment (probably in mL/h)

There are some data described at the beginning of this section that are not described in the documents provided by BUT. These data are:

- infusionLimit. It seems that it indicates the maximum limit of the infusion rate that can be commanded by the controller (probably in mL/h)
- expID. Identifier or number assigned to a specific experiment
- ptcOutr. Indicates the number of times that PTC of the patient has been out of the target
- ptcAboveHi. Indicates the number of times that PTC of the patient has been above the target (> targetPTCHi)
- ptcBelowLow. Indicates the number of times that PTC of the patient has been below the target (< targetPTCLow)
- sysInfo. It doesn't seem to have a clear use. In the application it is assigned a fixed value "S1"

Note: The formula to calculate ptcOutr , ptcAboveHi and ptcBelowLow is not clear. Each cycle that the PTC is not in the target the value of the variable is incremented in 20.

REDIS data record

One of the documents describes the contents of the data record that must be created in REDIS database for controlling an experiment. We are not sure if it is correct or there can be missed data.
Data record for every vm.X.Y in the REDIS database has the following attributes:

- weight (number) - weight of the patient in [kg]
- age (number) - age of the patient (years)
- gender - { male, female }
- drug (string) - name of the drug { Rocuronium, Casatracurium, ... }
- bolus (number) [mL]
- infusion (number) [mL/hr]
- unitVd (number) - unit Volume of distribution in [mL/kg]
- absoluteVd (number) - absolute Volume of distribution [mL]
- targetTOF (number),
- targetPTC (number), TOF and PTC target values of regulation,
- EC50 (number) - concentration of the drug causing 50% effect [ug/mL]
- TOF (number) - output effect in TOF units,
- PTC (number) - similarly,
- mtime (number) - current model time [s]
- cycle (number)

Appendix B - Technical details of MHP

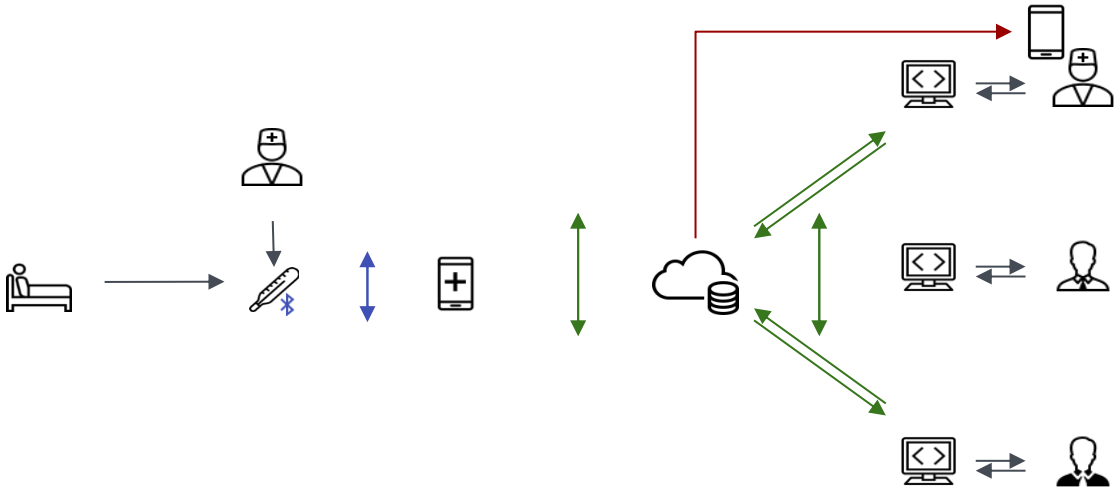
MCI designs and develops a proprietary platform called MHP - MediaClinics Health Platform, which makes available a versatile and modular telemedicine technological infrastructure that already has a large number of usage scenarios and specific references to its credit.

The main users identified are healthcare facilities, hospitals, doctors' offices, retirement homes, entities that provide social and health services, municipal, provincial and regional public health entities, and social and health cooperatives. Through the MHP platform, advanced telemedicine services are made available, which ensure comprehensive management and constant monitoring of patients.

Technology and functionality

The solution surface is very large, as we hold the whole technology stack starting from the medical sensor connected to the caregiver to its remote visualisation. To help us in the description we follow the data flow from its collection to its remote visualisation.

1. The patient, alone or aided by a caregiver, wears the medical sensors;
2. The sensors communicate to our data collection touchpoint via Bluetooth;
3. Our data collection applications, are developed on the Android mobile platform which makes the applications easily portable from one device to another, once they collect the data they communicate it with the cloud service;
4. The backoffice takes care of the centralised management of authentication and data storage, as well as all business logic. It was developed with a micro-service architecture and deployed in the cloud via docker containers;
5. At this point the health care staff, or the patient himself, can view the collected data via web-applications dedicated to individual use cases.



In the following paragraphs we will describe in detail the touchpoints and services offered by the platform.

Touch points

The system interacts with users in two scenarios, that of data collection and that of remote viewing and management. Various touch points have been developed for each of these scenarios, specifically:

- **MHP-Patient data collection application:** using this application the caregiver is autonomous and can manage sensor connection and communication with the physician (via integrated video call);
- **MHP-Hub data collection application:** this application is dedicated to non-autonomous caregivers, and is the one that requires minimal user interaction, in fact once it is turned on and configured it takes care of data acquisition in the background without any intervention;
- **MHP-Web application for patient remote management:** this web application is dedicated to patients or its caregiver, using it they can view and download his or her parameters to share with his or her physician;
- **MHP-Web application for remote management** This web application allows health care staff to view and manage caregivers remotely as well as contact them via video call.

Functionalities

- **Anagraphics and account management:** Allows you to manage all of a user's primary information (first name, last name, gender, social security number, etc.), address book, avatar, notes, and deactivation. It also allows a health care provider to be associated with a patient. All touchpoints also support two-factor authentication using time-based One Time Password (TOTP) technology.
- **Patient medical history:** Allows to record the medical history of a patient
- **Vital parameter collection:** Allows detection, visualisation and analysis of vital parameters, in particular
    - Body weight
    - EKG, heart rate
    - Respiratory signal/rate
    - Blood pressure
    - Oxygen saturation
    - Body temperature
    - Glycemia

Wearable

Respiratory

Glycemia

Blood

Oxygen

Body

Body weight

The sheer number of sensors supported is made possible by the modularization work done on the touchpoints that makes them de facto device-independent.

- **Vital parameter visualisation:** This service provides the ability for the physician to view, search, and analyse the collected parameters. In particular, the time trend of a parameter and analysis of Heart Rate Variability calculated from an electrocardiogram is shown. For signals over time, it is also possible to navigate the signal over 24 hours with a dedicated tool for visualising and tagging abnormalities.
- **Questionnaire service:** Allows web-configurable questionnaires to be administered to a patient and the results to be viewed by a clinician.

Appendix C - Stakeholders profile

Clinicians

Clinicians are professionals directly involved in patient care, diagnosis, and treatment. This group encompasses a diverse range of healthcare providers, including physicians, nurses, therapists, and other health professionals.

Competencies:

- clinical expertise,
- learning willingness,
- healthcare environment knowledge,
- collaboration with IT professionals,
- policy adherence.

Importance: Clinicians are crucial for evaluating and endorsing the project outcomes integrated in their daily practices. Their involvement ensures that the cybersecurity tools align and seamlessly integrate with the clinical workflow enhancing the quality of care while safeguarding against cyber threats.

Patients

Patients are the individuals receiving medical care and services within the healthcare system. They have interest in how the project impacts their health, treatment and healthcare experience.
Importance: Patient involvement is essential for validating the usability and security of CYLCOMED. Understanding patient experiences ensures that the cybersecurity tools are applicable and the added value perceived.

Ethical Committees

Ethical Committees are responsible for reviewing and ensuring the ethical conduct of the project. They safeguard the rights, well being and dignity of research participants by assessing the ethical implications of the research.

Competencies:

- ethical expertise,
- legal knowledge (confidentiality and privacy regulations),
- cybersecurity awareness,
- risk assessment.

Importance: Ethical committees provide oversight and approval for clinical studies and trials. Their involvement ensures that the implementation of CYLCOMED aligns with ethical standards, safeguarding patient welfare and privacy.

Healthcare Administrators

Healthcare administrators are professionals responsible for managing and overseeing healthcare providers, ensuring the delivery of high-quality and efficient healthcare services. Their role encompasses a wide range of responsibilities, such as strategic planning, regulatory compliance, care quality improvement and information technology efficient exploitation.

Competencies:

- leadership and management,
- decision making,
- communication and collaboration,
- quality improvement,
- cybersecurity awareness
- regulatory compliance.

Importance: Healthcare administrators guide the implementation of CYLCOMED within healthcare institutions. Their involvement ensures seamless integration and effective deployment of cybersecurity measures to enhance overall hospital security.

Hospital Information systems (HIS) technicians

Professionals advancing information technology within hospital settings. Their role encompasses ensuring health data security and management, system maintenance and integration between technologies.

Competencies:

- technical proficiency,
- health informatics knowledge,
- problem-solving,
- technology integrations,
- health information security and management.

Importance: Hospital Information systems (HIS) technicians ensure the technical robustness and security of CYLCOMED. Their involvement is indispensable for implementing cybersecurity measures that effectively protect patient data and healthcare systems from cyber threats.

Researchers and Developers:

Individuals who conduct systematic analysis to enhance knowledge in a specific field. In CYLCOMED, due to the technology-driven nature of the project, researchers and developers work together to explore new technologies and methodologies and apply findings as practical solutions or innovations.

Competencies:

- technical proficiency,
- health informatics knowledge,
- research design,
- data management,
- data analysis and interpretation,
- project management,
- communication and collaboration.

Importance: Researchers and developers drive the innovation behind CYLCOMED. Their involvement is crucial for continuous improvement, refining the cybersecurity solution based on emerging threats and technological advancements.

Technology Providers:

Provide solutions (products/services) related to information technology. They participate in the research project since their interest is to leverage technology efficiency and application in the healthcare field.

Competencies:

- technical expertise,
- innovation,
- technology integration,
- product development,
- cybersecurity awareness,
- regulatory compliance,
- adaptability, problem solving and strategic thinking,
- market research.

Importance: Technology providers play a pivotal role in implementing and refining CYLCOMED. Their expertise ensures the technical efficacy and seamless integration of cybersecurity tools into existing healthcare platforms.

Medical Device Manufacturers:

Design, produce and distribute medical devices among healthcare settings for diagnosis, treatment, monitoring and patient care. Their role also encompasses advancement in medical technology and its integration, since medical devices need to be able to communicate collected or generated data to other applications.

Competencies:

- technical expertise,
- innovation,
- technology integration,
- product development,
- regulatory compliance (EU Medical Device Regulation),
- clinical evaluation,
- risk management.

Importance: Manufacturers contribute essential insights into the compatibility and interoperability of CYLCOMED with existing medical devices. Their involvement ensures a harmonious integration, enhancing the overall efficacy of cybersecurity measures.