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

D7.4 Dissemination, Communication, Standardisation and Exploitation Final Report

Revision: v.0.6

Work package	WP7
Task	Task 7.1, 7.2, 7.3, 7.4, 7.5
Due date	30/11/2025
Submission date	30/11/2025
Deliverable lead	MARTEL
Version	0.1
Authors	Giada Martello (MARTEL), Ricardo Ruiz Fernandez (RGB), Andrés Castillo (FHUNJ)
Reviewers	Diana Ferro (OPBG), Dietmar Frey (Charité)

Abstract	Deliverable 7.4 presents a comprehensive report of communication, dissemination, standardisation and exploitation activities carried out from month 18 until month 36 of the project. Particular attention will be given to describing the project's communication and dissemination outputs, analysing the performance of the set KPIs, and synergies with sibling projects. Regarding standardisation and exploitation, the topics of standards relevant to the project, as well as performed trainings, the Booster service

	consultation outcomes, Key Exploitable Results (KERs) and Intellectual Property Rights (IPRs) will be thoroughly documented.
Keywords	Cybersecurity, risk management, connected medical devices (CMDs)

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	09/07/2025	ToC and first editing	Giada Martello (MARTEL), Ricardo Ruiz Fernandez (RGB)
V0.2	05/09/2025	Content for Communication and Dissemination section	Giada Martello (Martel), Galileo Disperati (Martel)
V0.3	15/09/2025	Content for Standardisation and Exploitation section	Ricardo Ruiz Fernandez (RGB)
V0.4	18/11/2025	Integration of partners' contribution and preparation for internal review	Giada Martello (Martel), Galileo Disperati (Martel), Ricardo Ruiz Fernandez (RGB)
V0.5	24/11/2025	Internal Review	Dietmar Frey (CUB)
V0.6	30/11/2025	Review and Finalisation	Giada Martello (Martel), Galileo Disperati (Martel)

Disclaimer

Funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Funded by the European Union (CYLCOMED, 101095542). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme

Nature of the deliverable:	R

Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

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

Executive summary

This report summarises the key communication, dissemination, standardisation, and exploitation outcomes of the CYLCOMED project during the final reporting period (M18 to M36). The project significantly advanced its mission to raise awareness and build capacity around the cybersecurity of Connected Medical Devices (CMDs), with a strong focus on stakeholder engagement and long-term sustainability.

Over this period:

- The consortium delivered an integrated communication and dissemination strategy, including active social media campaigns, participation in relevant industry events, development of high-quality multimedia materials, and engagement with similar EU-funded projects. This resulted in a broad set of website resources, as documented in the relevant sections below.
- Significant progress was made in standardisation efforts, including training sessions and collaboration with the Booster Service, which informed next steps for aligning the CYLCOMED Toolbox with relevant cybersecurity standards.
- The project consolidated its exploitation strategy, identifying Key Exploitable Results (KERs) and taking steps toward commercialisation and IPRs management, setting the foundation for post-project impact.
- The Advisory Board provided valuable feedback throughout this phase, contributing to offering strategic insights to the project.

This final phase reflects CYLCOMED's commitment to ensuring that its outcomes remain relevant, usable, and aligned with European digital health and cybersecurity priorities.

Table of contents

1 INTRODUCTION 10
1.1 Purpose of the document 10
1.2 Structure of the document 10
2 COMMUNICATION AND DISSEMINATION 12
2.1 Communication and Dissemination Tools and Channels 12
2.1.1 Website 12
2.1.1.1 CYLCOMED Website Analytics 13
2.1.2 Social Media 15
2.1.3 YouTube 18
2.2 Publications, Presentations, and Talks 19
2.2.1 Open Science Practices and Repository 22
2.3 Promotional Material 22
2.4 Newsletter 23
2.5 Media Relations 23
2.6 Events 24
2.7 Synergies With Other Projects And Initiatives 27
2.8 Impact Creation Monitoring 27
2.8.1 Communication and Dissemination KPIs 28
2.9 Lessons Learnt 29
3 STANDARDISATION ACTIVITIES AND OUTCOMES 30
3.1 CYLCOMED Standardisation Mission and Key Takeaways at Month 36 30
3.2 Cybersecurity Standards 31
3.2.1 Training Sessions About Relevant Standards 32
3.2.2 Surveys on Standard-related Issues 33
3.3 Booster Results 35
3.4 Lessons Learnt And Future Steps 36
4 EXPLOITATION ACTIVITIES AND OUTCOMES 38
4.1 Exploitation Objectives 38
4.2 Key exploitation Takeaways 41
4.2.1 Customers/stakeholders 41
4.3 Partners Exploitation Plans and Commitments 42
4.4 IoT Cybersecurity Market Considerations in the Healthcare Sector 43
4.4.1 The Global IoT Security Market indexes and Growth Drivers in the Healthcare Sector 43
4.4.2 Market potential of the pilot 1 on Infusion Controller and MD hospital equipment 43
4.4.3 Market potential of Pilot 2, the telemedicine Use Case 44
4.4.4 Key Challenges encountered 44
4.5 CYLCOMED Strategic Targets at M36 45
4.5.1 Approach to certification 45

4.5.2 SWOT analysis for CYLCOMED cybersecurity toolbox 47
4.5.3 PESTLE analysis for CYLCOMED cybersecurity toolbox 49
4.6 Roadmap for Commercialization and Future Uptake 51
4.7 IPR Considerations 51
4.7.1 IPR Agreement 52
5 CYLCOMED Advisory Board 54

List of figures

Figure 1: CYLCOMED Website Resources Tab Breakdown 13
Figure 2: Visit Overview, CYLCOMED Website 14
Figure 3: CYLCOMED Twitter Account, Post Impressions (below) 16
Figure 4: LinkedIn Job Function Insights List 17
Figure 5: LinkedIn Job Function Insights, “Others” 17
Figure 6: Members Reached, October 2024 – November 2025 18
Figure 7: CYLCOMED Booth, organised by HIMSS, with roll up and flyers; Paris, June 2025 22
Figure 8: CYLCOMED final newsletter snapshot, November 2025 23

List of tables

Table 1: Communication and Dissemination KPIs 29
Table 2: Toolbox components 39

Abbreviations

AMG	AcceleroMIography
AI	Artificial Intelligence
BP	Blood pressure
CMM	CompressoMiography
CTR	Click through rate
CVD	Cardiovascular Diseases
EMG	ElectroMiography
HF	Hearth failure
KERs	Key Exploitable Results
KPIs	Key Performance Indicators
ICU	Intensive Care Unit
IP	Internet Protocol
NIBP	Non Invasive Blood Pressure
NMT	NeuroMuscular Transmission
OR	Operating Room
TCP	Transmission Control Protocol
USP	Unique Selling Proposition
UVP	Unique Value Proposition

1 INTRODUCTION

This Final Report on Dissemination, Communication, Standardisation, and Exploitation (Deliverable 7.4) covers the period from Month 18 (M18) to Month 36 (M36) and provides a structured overview of CYLCOMED's outreach and impact-related activities during the second half of the project.

The document is structured into four main sections:

- Communication and Dissemination (Tasks 7.1, 7.4, 7.6)
- Standardisation Activities and Outcomes (Task 7.2)
- Exploitation Activities and Outcomes (Task 7.3)
- Advisory Board Activities (Task 7.5)

Each section presents the progress made, and strategic considerations undertaken in the final phase of the project. The report also reflects the project's efforts toward sustainability, stakeholder engagement, and the practical implementation of the CYLCOMED Toolbox.

1.1 Purpose of the document

This deliverable outlines the key communication, dissemination, exploitation, and standardisation activities conducted between Month 18 (M18) and Month 36 (M36) of the CYLCOMED project. The report aims to achieve the following objectives:

- Provide a clear and comprehensive overview of activities across the four areas mentioned above, including performance measurement against set KPIs. These efforts aim to raise awareness of the CYLCOMED project among stakeholders and reinforce its mission to strengthen the cybersecurity of Connected Medical Devices (CMDs).

- Analyse the relevant standards identified during the final reporting period and define conclusions and next steps, building on the outcomes of the Booster Service engagement undertaken by the consortium.

- Demonstrate collaboration and alignment among consortium partners and similar projects through joint initiatives such as publications, events, and shared outreach actions.

- Present the project's exploitation strategy, including key takeaways related to commercialisation, IPRs management, and planned future actions to ensure sustainability of key results.

1.2 Structure of the document

This deliverable is structured into the following sections:

- Section 2, **Communication and Dissemination**: this section presents the full range of multimedia and outreach activities carried out between M18 and M36. It includes an overview of the project website and its key components, such as newsletters, news articles, promotional materials, presentations, publications, videos, training activities, and events.

- Section 3, **Standardisation Activities and Outcomes**: this section analyses the standards relevant to CYLCOMED's scope, outlines the training sessions conducted during the reporting period, and presents findings from the Booster Service, as committed in the project plan.
- Section 4, **Exploitation Activities and Outcomes**: this section outlines the project's exploitation strategy, with a focus on long-term sustainability, future commercialisation potential, Key Exploitable Results (KERs), and Intellectual Property Rights (IPRs) management.
- Section 5, **Advisory Board**: this final section summarises the contributions of the Advisory Board, highlighting their involvement with CYLCOMED.

2 COMMUNICATION AND DISSEMINATION

Deliverable 7.1, Dissemination, Communication, Standardisation, and Exploitation Strategy and Plan outlined the project's mission and laid the groundwork for its communication and dissemination approach. It included the identification of key target audiences, the development of consistent messaging, the definition of communication challenges, and the establishment of relevant KPIs.

This deliverable uses the end of the first reporting period (M18) as a baseline to evaluate the effectiveness of the proposed strategy, with particular focus on the activities implemented. The following sections provide a detailed breakdown of the resources made available through the project website, as well as the communication and dissemination actions carried out from M18 onwards.

2.1 Communication and Dissemination Tools and Channels

This section seeks to provide a comprehensive breakdown of communication and dissemination activities conducted from M18 to M36 of the project. Particular attention will be given to performance indicators and stakeholder engagement related to website and social media.

2.1.1 Website

From M18 to the time of writing, 14 news articles have been published on the project's website, contributing to a total of 26 articles. These include:

- Articles promoting and summarising consortium meetings
- "Meet the partners" articles, spotlighting each partners' role in the project, their organisation's expertise, and team
- Technical articles on CYLCOMED's pilots and its toolbox
- Awareness-raising articles describing the legal environment
- Articles on events' participation, where relevant to the project
- A final article summarising the project's outcomes

Following the past deliverable dating May 2024, numerous tabs have been populated in the *Resources* section, as most activities happened in the second project period (M18-M36). These are:

- Toolbox: a tab including presentations on the toolbox components as well as a brief description of them
- Deliverables: a section updated with all public deliverables available for download
- Publications: a publications list, in reverse chronological order, including a link to published files (this section will be further documented in a dedicated paragraph)
- Presentations: includes a full overview of presentations at conferences (both physical and online), available in branded PPT in reverse chronological order, complete of acknowledgments of EU and SERI
- Press releases: a list, in reverse chronological order, of published press releases

- Promo materials: a section displaying multimedia materials (mainly flyers) showcased at events, both in printed and digital format
- Videos: a section dedicated to the project's videos, including interviews and trainings

In addition, the *Events* section displays a list of the project's past events, including a brief description and registration link (where possible). The website includes also all the project newsletters, amounting to six.

Figure 1: CYLCOMED Website Resources Tab Breakdown

2.1.1.1 CYLCOMED Website Analytics

At the time of writing, the CYLCOMED website has recorded 4,875 visits. A *visit* refers to the number of times users access the website. As shown in the image below, website traffic has doubled compared to the previous period, with a notable +100% increase in visits. This indicates successful outreach efforts, effective marketing campaigns, and growing interest in CYLCOMED's content. The website has also registered 10,956 pageviews and 8,744 unique pageviews, showing that users are exploring multiple pages, though not repeatedly visiting the same ones. An average visit duration of 2 minutes and 12 seconds suggests that users are engaging meaningfully with the site's content. On average, users perform 2.4 actions per visit, which may include page views, downloads, outlink clicks, or internal searches. Notably, a maximum of 57 actions within a single visit highlight that some users are highly engaged with the website.

The bounce rate of 61% indicates that a majority of users are leaving the website after viewing just one page. However, this is not necessarily a negative outcome. In many cases, especially for single-page content, users may quickly find the information they need and leave without further navigation, which still reflects a successful visit. In terms of downloads, the website recorded 6,079 downloads. These refer to:

- Press clippings: 191
- Presentations: 2.539
- Promo materials: 1.656
- Toolbox resources: 1,142
- Scientific publications: 318

- Other publications and reports: 48
- Privacy Statement: 59
- Others: 111

Additionally, the website logged 691 outlink clicks, suggesting it is effectively guiding users toward external resources. This is particularly valuable for event promotion, where timely access to external conference or congress websites is essential.

Figure 2: Visit Overview, CYLCOMED Website

When looking at the most visited pages on the CYLCOMED website, the top-performing sections include:

- News section, including blog posts – 1,350 views
- Events page – 1,028 views
- Consortium – 372 views
- Use Case 1 – 352 views
- Deliverables – 277 views
- Contact – 256 views
- Advisory Board – 230 views
- Publications – 223 views
- Newsletter – 220 views
- Vision and Strategy – 218 views
- Use Case 2 – 205 views
- Press Releases – 179 views
- Presentations – 165 views
- Toolbox – 74

In addition to core website sections, the article *"Cybersecurity for Medical Devices: a preliminary legal and ethical analysis"* attracted a notable 159 pageviews, reflecting strong audience interest in this aspect of the project. Other popular content includes the Promotional

Materials section (148 views) and the website article *"Meet the CYLCOMED Partner: EVIDEN, an Atos business"* (126 views). All remaining pages and specific articles not listed above received fewer than 100 pageviews each.

The data above indicates that visitors engage with a broad range of content, showing a clear preference for scientific outputs (such as pilot case descriptions), publications, presentations, and project updates (including the events and news sections).

In terms of user behavior and demographics, the majority of visitors access the CYLCOMED website via desktop devices (4,287 visits), followed by mobile devices (549 visits), and a smaller number from other devices such as tablets and phablets. This breakdown corresponds to the total number of visits shown in *Figure 2*.

When examining traffic sources:

- Over 3,681 visits originated from direct access, meaning users manually entered the website URL or accessed it through a bookmark
- More than 790 visits came from Google, the primary search engine
- Social networks generated over 230 visits
- Other websites contributed more than 140 visits through referral links

Among social platforms:

- LinkedIn is the main driver of traffic, accounting for over 80% of social visits
- X (formerly Twitter) follows with 17%
- YouTube contributes 1%
- GitHub accounts for less than 1%

A detailed analysis of social media performance will be provided in the next section.

In conclusion, the CYLCOMED website shows strong and growing engagement, with traffic doubling over the previous period. Users interact with a variety of content, especially scientific outputs and project updates. Most access comes via direct entry and desktop devices, while LinkedIn stands out as the top social referral source. These trends reflect effective outreach and increasing visibility of the project.

2.1.2 Social Media

As highlighted in D7.3, social media plays a crucial role in maximising the reach of the project's activities and results and serves therefore as a key component of its dissemination and communication strategy. At the time of writing, the project accounts for a total of 642 followers and 164 social media posts through X (formerly Twitter) and LinkedIn, against the set KPI of 1000 connections and 60 posts. Below, in the respective sections, a complete breakdown of posts analytics will be given, including data on impressions, members reached and engagement according to available insights, where possible.

X (Former Twitter)

X (formerly known as Twitter) is CYLCOMED's second social media platform. At the time of writing, the project's account includes 86 posts and 295 followers. While detailed analytics

such as audience insights and engagement rates are available only to premium users, visible metrics like impressions indicate that the most popular content focuses on consortium meetings and training webinars. This suggests that the audience is particularly interested in content related to cybersecurity in the healthcare sector.

It is also important to note that, following major geopolitical developments over the past year, X has experienced a significant decline in users and engagement, with a reported loss of approximately 10% of its European follower base[1]. This trend is confirmed by comparing X's October 2024 transparency report with that of April 2025, which shows a consistent drop in monthly active users.

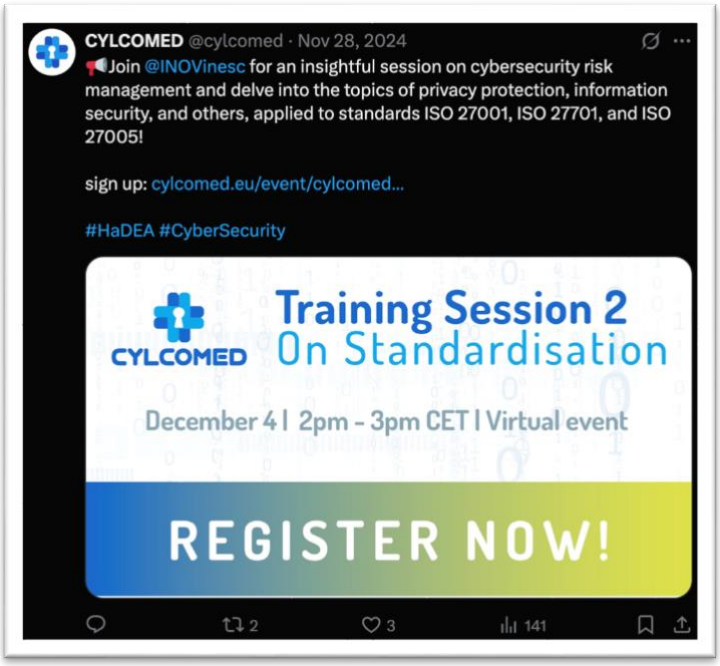

Figure 3: CYLCOMED Twitter Account, Post Impressions (below)

LinkedIn

From the outset of the project, LinkedIn has proven to be the most effective social media platform, offering strong visibility among professionals of various industries, sibling projects, and the wider public. Unlike X, LinkedIn offers a broader range of analytics insights to free profiles; still, user demographics can be limited. Based on the most recent followers' demographics of the project's LinkedIn account at the time of writing, the largest traceable segment is composed of professionals in the education sector, followed by those in business development and engineering. Smaller proportions represent fields such as information technology, sales, research, and other areas, as shown in Figure 3.

[1] *https://www.politico.eu/article/elon-musk-x-europe-social-media-twitter-takes-hit/*

It's important to note that LinkedIn's job function data doesn't cover the whole audience. The remaining – and biggest data (see "others" on Figure 4, accounting for 44%) may be unavailable for several reasons, including:

- Users not filling out the "job function" field in their LinkedIn profiles, or using non-standard titles that cannot be classified easily
- Privacy thresholds that prevent LinkedIn from displaying data where sample sizes are too small
- Incomplete or outdated profile information

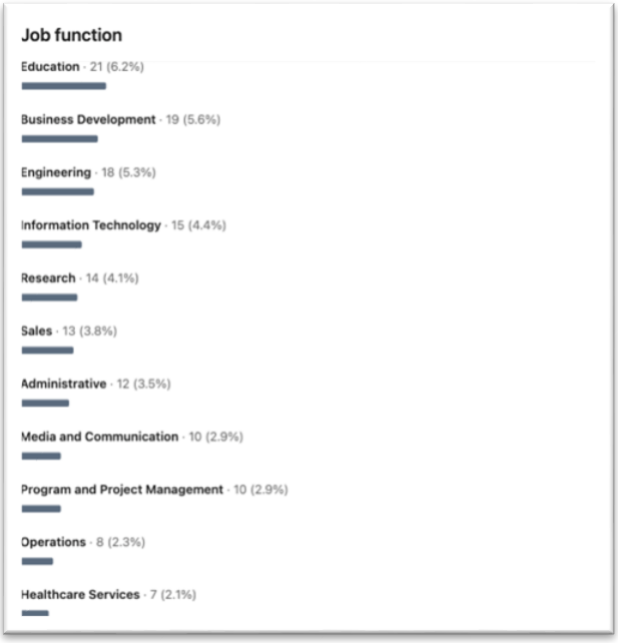

Figure 4: LinkedIn Job Function Insights List

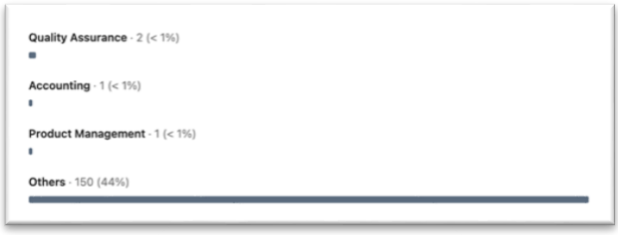

Figure 5: LinkedIn Job Function Insights, "Others"

In a nutshell, LinkedIn shows us a multitude of sectors that the project's followers belong to but can't offer more precise data, due to privacy and aggregational elements.

In terms of awareness raising, CYLCOMED's LinkedIn page recorded over 500 page views and 350 unique visitors (at the time of writing), from the page's launch in May 2023 to date. Considering the current number of followers (347) and the consistent posting activity (78

posts), these metrics align with what can be expected for a small page operating within a niche domain, namely, the cybersecurity of connected medical devices.

Given the specialised nature of the topic, it may be less accessible to a broader audience compared to more general healthcare subjects such as cancer. For this reason, CYLCOMED's communication strategy on LinkedIn has prioritised pairing written content with multimedia formats to enhance clarity and engagement. The focus has also been on awareness-raising content such as events, webinars, and publications, while more technical material has been shared primarily via the project's website.

It is important to note that not all followers engage with content, and not all visitors are followers. To boost visitors' engagement, more focus has been given to sharing multimedia resources (such as pictures and videos) and encouraging partners to reshare content. Overall impressions exceeded 9,300, which, given the niche audience and follower count, represents a modest but respectable reach.

In terms of reach, compared to 2024, CYLCOMED's LinkedIn page received a boost, totaling 4,400 platform members viewing its content.

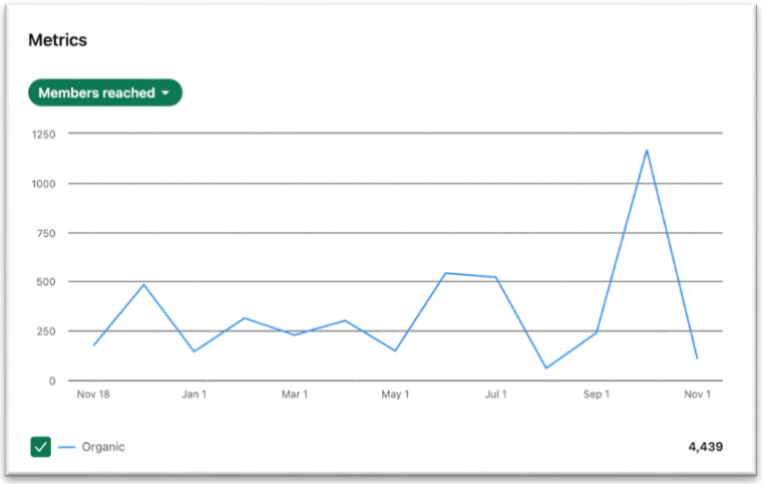

Figure 6: Members Reached, October 2024 – November 2025

Finally, regarding user engagement, CYLCOMED's LinkedIn page boosts an engagement rate of 10 %. This number refers to organic content (not sponsored) and can be considered a good achievement, especially when compared to LinkedIn's average engagement rate of 2.8%[2] for the healthcare sector, as analysed by the social media management platform Hootsuite for Q125.

2.1.3 YouTube

The project's YouTube channel, opened in September 2025, counts six videos, with a total of 196 views. The channel includes, in reverse chronological order:

[2] *https://blog.hootsuite.com/calculate-engagement-rate/#How_to_calculate_engagement_rate_automatically*

- CYLCOMED final workshop in Ljubljana, carried by partner OPBG, October 2025
- CYLCOMED at HIMSS 2025, featuring an interview with partner pediatric hospital Bambino Gesú, June 2025
- CYLCOMED Training Session 2, on Standardisation, carried by partner INOV, December 2024
- CYLCOMED Cluster Webinar, conducted with cluster projects NEMECYS, CYMEDSEC, and MEDSECURANCE, November 2024
- CYLCOMED Training Session 1, on Standardisation, carried by partners RGB and Niño Jesus Hospital, May 2024
- CYLCOMED Project introduction video, August 2024

During the project's lifecycle, the YouTube channel has been actively promoted via social media, and partners have been encouraged to repost videos on their social networks.

2.2 Publications, Presentations, and Talks

Publications

At the time of writing, the website's relevant section includes six peer-reviewed publications from consortium partners, three of which are conference proceedings, one of which is a journal article. In addition, CYLCOMED contributed to a white paper with projects that participated in HIMSS conference in Paris, in June 2025 and to another publication in 2024 with sibling projects.

Here is a list of publications available on the website's relevant section:

- L'alleanza della Cybersicurezza e dell'Intelligenza Artificiale nella Sanità Digitale: Sfide e Soluzione RWD del Progetto EU CYLCOMED, Recenti Progressi in Medicina, Ospedale Pediatrico Bambino Gesú, September 2025
- MDCG 2019-16 Guidelines: Case Study-Based Assessment and Path Forward; Androutsos, C. et al.; EICC 2025, June 2025, Communications in Computer and Information Science, vol 2500. Springer, Cham.
- LOMOS: An AI-Based Runtime Security Monitoring System Fit for the Cloud Continuum; Pita Costa, J. Ratkajec, H. Vladušič, D. Martinčič, T. Černivec, A. Činkelj, J. Davi, R. Favrin, S. Gorza, L. Di Marco, G. ; June 2025, Springer Nature, Euro-Par 2024: Parallel Processing Workshops.
- Navigating Cybersecurity Challenges in Healthcare: Challenges, Innovations, and EU Legal Framework for Connected Medical Devices ; Nisevic, M. Milojevic, D. ; June 2025, Springer Nature, Conference Paper (IoT Technologies and Wearables for HealthCare)
- The Cybersecurity Nexus of the AI Act and MDR 333 ; Nisevic, M. Milojevic, D. Rodrigues, J. Cadete, G. ; May 2025, Now Publishers.
- A Way Forward for the MDCG 2019-16 Medical Device Security Guidance – Feedback & recommendations for enhancement of MDCG 2019-16; Androutsos, C. et al.; June 2024, PETRA Conference (The 17th Conference on PErvasive Technologies Related to Assistive Environments).

In addition to the five publications available, Bambino Gesú Pediatric Hospital and KU Leuven submitted several publications that are currently being reviewed. Below, they are listed in reverse chronological order.

- Cybersecurity in Paediatric Healthcare Settings: A Narrative Review., Italian Journal of Paediatrics, April 2025, Ospedale Pediatrico Bambino Gesú
- Cybersecurity of Connected Medical Devices: Interdisciplinary Perspectives on Ethical, Regulatory an Practical Challenges in the EU, Journal of Cybersecurity, May 2025, KU Leuven
- HIMSS Joint White Paper following the Paris Conference with the EU-Projects Pavillion, June 2025, whole consortium

Throughout the CYLCOMED Project's lifecycle, partners made consistent and dedicated efforts to disseminate research results across a variety of channels. Over the past months, however, it became evident that the scientific publication process, particularly from submission to final acceptance and publication, has taken considerably more time than initially anticipated.

In line with the consortium's commitment to ensuring high-quality scientific output, partners opted to prioritise quality over quantity of outputs. This strategic choice led to a more selective approach in targeting reputable journals and conferences, which naturally extended the timelines.

It is important to note that the consortium is only now in a position to disclose the first results of the project, a key milestone for CYLCOMED that offers valuable, tangible insights. While the current project timeline limits the chance of working towards submissions, the availability of results demonstrates that the project is successfully meeting its objectives.

Nevertheless, the consortium exceeded expectations in other areas of dissemination. Notably, partners participated in more than eight scientific conferences, at the time of writing, 24 events in total, surpassing the original target, and carried out numerous local dissemination activities, including participation in national healthcare events, stakeholder forums, and workshops. These efforts significantly contributed to raising awareness about the project and its results across diverse audiences.

Presentations

The CYLCOMED website features ten presentations at the time of writing. Presentations have been uploaded in PowerPoint format to the relevant website tab, using the project's branding fonts and colors, as well as EU and SERI acknowledgements. The below list includes presentations in reverse chronological order in the field of medical AI.

- MDCG 2019-16 Guidelines: Case Study-based Assessment and Path Forward; EICC Conference 2025; Rennes, France, 18-19 June; Dusko Milojevic, KU Leuven
- Human Factor in Cybersecurity; ACCA Conference 2025; Ghent, Belgium, 22 May 2025; Dusko Milojevic, KU Leuven
- The Cybersecurity Nexus of the AI Act and MDR; Webinar on Adaptive AI for Pioneering Secure Healthcare Innovations, Online, 18 March 2025; Dusko Milojevic, KU Leuven

- Risk Management Applied to Cybersecurity and Privacy with ISO27001, ISO27701 and ISO 27005; CYLCOMED Training Session 2 on Standardisation, Online, 4 December 2024; Dr João Paulo Rodrigues, INOV
- Navigating Cybersecurity Challenges in Healthcare: CYLCOMED Project; The 5th International Conference EAI on Wearables in Healthcare, Online, 3 December 2024; Dusko Milojevic & Dr. Maja Nisevic, KU Leuven
- LOMOS: Runtime Security Monitoring Fit for the Cloud Continuum; 30th International European Conference on Parallel and Distributed Computing, IECCONT workshop, Madrid, Spain. 26 – 30 August 2024; Hrvoje Ratkajec, XLAB
- A Way Forward for the MDCG 2019-16 Medical Device Security Guidance; PETRA Conference 2024; Greece, 29 June 2024; Dusko Milojevic, KU Leuven
- Legal Challenges in the Internet of Medical Things (IoMT) in the EU – The Plea for Legal Clarity, May 2024; 11th Annual Governance of Emerging Technologies and Science Conference (GETS), Arizona, US, 16 May 2024; Dusko Milojevic, KU Leuven
- Training Session: Description of ISO/IEEE 11073 standard; CYLCOMED Training Session 1 on Standardisation | Online, 15 May 2024; Ricardo Ruiz Fernández, RGB Medical Devices; Santiago Bollain Pastor, FHUNJ
- Using AI Robots in Medicine: the interplay between technology, medicine and law as a gataway for discovering an appropriate liability regime, Geneva Digital Law Research Colloquium Online, 22 June 2023; Dr. Maja Nisevic, KU Leuven

Talks

During the project's lifetime, partners engaged in several talks, in the form of forums' participation or panels from other projects, which contributed to knowledge exchange and stronger synergies with sibling projects. The list below serves as a comprehensive overview of such occasions.

- EVIDEN partner invited at "XiA Internal Learning Lession" organized by XiA project on 11 December 2025
- SEPTON and SECURED project Open Day at Erasmus MC and panel "Cybersecurity and upcoming regulation to the Healthcare sector – How does it affect clinical practice?", participation of partner KU Leuven, October 2025
- SECURED project meeting, April 2025, presentation of toolbox tools LADS and FE4MED by partner FHUNJ
- ENFIELD project online webinar "Adaptive AI for Pioneering Secure Healthcare Innovation", March 2025; participation and presentation of partner KU Leuven
- Digital Health Ljubljana, February 2025; participation of partner XLAB at a dedicated panel about cybersecurity in the health domain
- NEMECYS project workshop, Ospedale San Raffaele, Milan, May 2024; participation of partners MCI and FHUNJ

A complete overview of events, both as organizers and participants, will be provided in the relative section below.

2.2.1 Open Science Practices and Repository

In accordance with open access principles championed by CYLCOMED, publications have been featured on the project's Zenodo community, created by partner Martel to further boost the dissemination of project's research, and available to the broad consortium. Publications on Zenodo include also other publications by sibling projects that are relevant to CYLCOMED.

At the time of writing, the publications on Zenodo account for 222 views and 406 downloads.

These high metrics translate into high interest of the scientific community in medical cybersecurity outputs.

2.3 Promotional Material

At the time of writing, the website boasts six flyers, in line with set KPIs. These include:

- A digital flyer created for the final workshop for developers (repurposed to be a workshop with sibling projects), in occasion of their workshop held in October 2025, during the last project plenary
- A flyer in Spanish and English created for partners EVIDEN and Niño Jesus Pediatric Hospital, showed at their joint e-workshop in September 2025
- An introductory flyer prepared for partner Bambino Gesú Pediatric Hospital, showed at the Italian Telecommunication Congress, April 2025
- A flyer on legal compliance, made for partner KU Leuven, showed at the EAI HealthWear 2024 conference, December 2024
- A flyer made for partner RBG, depicting their use case at Medica Fair, November 2024
- An introductory flyer, describing the project scope and main components

Figure 7: CYLCOMED Booth, organised by HIMSS, with roll up and flyers; Paris, June 2025

2.4 Newsletter

Under the dedicated website section, users can find six project newsletters, corresponding to the number of KPIs set in D7.1. The interval between each newsletter was on average of six months, with the exception of the second one, sent around one year after the opening newsletter.

Content included a spotlight on partners' expertise, consortium meetings, webinars organised and/or attended, and key industry events. The final newsletter provided an overview of key milestones as well as a summary of events and developments since the 5th newsletter dating back to March 2025. To date, the newsletter features 26 subscribers, with an average click through rate (CTR) of 24%, which, according to industry leaders such as Mailchimp is well above average and indicates strong engagement.

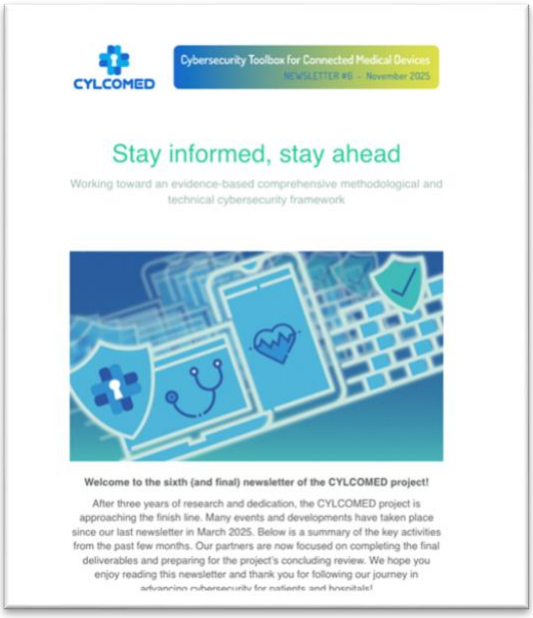

Figure 8: CYLCOMED final newsletter snapshot, November 2025

2.5 Media Relations

As far as press releases are concerned, the project's envisioned KPI of four press releases has been achieved. Below is a breakdown of each of them:

- Press release #1, introducing the project's scope and ambitions, as well as its consortium: here (January 2023)
- Press release #2, introducing the toolbox's components, available in English and Spanish (October 2024)
- Press release #3, disclosing further updates into the toolbox, available in English (March 2025)
- Press release #4, outlining the project's pilots, outcomes, and conclusion, available in English (November 2025)

2.6 Events

Since the inception of the project, CYLCOMED partners have participated to a series of events with the goal of raising awareness on the project's mission, the progress of its pilots and strengthening bonds with similar projects. Events have been organised online, in the form of webinars and training sessions, and in person, in the form of co-creation events, panel discussions, and conferences.

At the time of writing, partners participated in 25 events. Below is a comprehensive list of events in reverse chronological order, including details on partners' participation.

- Medica Fair, 17-20 November 2025, participation of partner RGB and project presentation
- EVIDEN's participation to MSWiM conference and presentation of LADS tool. "Misbehavior Detection and Mitigation on 5G Core Services in Kubernetes," the 27th International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), Barcelona, Spain, 27 -31 October 2025
- Data protection in clinic and in scientific research, in-person workshop on cybersecurity for medical staff, 17 October 2025, project presentation by partner Ospedale Pediatrico Bambino Gesú - 58 participants
- Cybersecurity Perspectives in EU Healthcare co-creation workshop with cybersecurity-cluster projects, 7 October 2025, led by Ospedale Pediatrico Bambino Gesú – 30 participants
- Anonymization of medical data: tools to preserve privacy, online workshop for medical staff, 23 September 2025, project and toolbox presentation by partners Hospital Niño Jesús of Madrid and Eviden, 58 participants
- European Interdisciplinary Cybersecurity Conference (EICC) 2025 - Medical Device Security and Privacy, 18-19 June 2025, project cluster paper presentation "MDCG 2019-16 Guidelines: Case Study-based Assessment and Path Forward" by partner KU Leuven
- Participation in cluster workshop "Innovative Solutions for Cyber Risk in Medical Devices: A Hands-on Approach", organised by project NEMECYS, 13 June 2025, Paris, participation of Ospedale Pediatrico Bambino Gesú
- Healthcare Information and Management Systems Society (HIMSS) Europe Conference 2025, 10-12 June 2025, project presentation and European project workshop with partners Martel and Ospedale Pediatrico Bambino Gesú
- Euroanesthesia 2025, 25-27 May 2025, project presentation and booth by partner RGB
- ACCA Conference 2025, Center for Foundations and Methods of Private Law, Ghent University, 22 May 2025, project presentation "Human Factor in Cybersecurity" by partner KU Leuven
- Healthcare Security - Hospitals and Pharmaceutics Security and Safety Conference, 21 May 2025, project presentation by partner INOV
- Telecommunications of the Future Congress, 9 April 2025, project presentation by partner Ospedale Pediatrico Bambino Gesú
- SECURED project meeting, 9 April 2025, presentation of toolbox components LADS and FE4MED by partner Hospital Niño Jesús of Madrid

- Adaptive AI for Pioneering Secure Healthcare Innovation, ENFIELD project webinar, 18 March 2025 , participation and presentation "The Cybersecurity Nexus of the AI Act and MDR" by partner KU Leuven
- Digital Health Ljubljana, 2-4 February 2025, panel participation and project presentation by partner XLAB
- The 5th International Conference EAI on Wearables in Healthcare, 2-3 December 2024, project presentation "Navigating Cybersecurity Challenges in Healthcare: CYLCOMED Project" and publication by partner KU Leuven
- Critical Infrastructure Protection & Resilience Europe, 12-14 November 2024, project presentation by partner Hospital Niño Jesús of Madrid
- Medica Fair, 11-14 November 2024, booth of partner RGB and project presentation
- 30th International European Conference on Parallel & Distributed Computing, 26-30 August 2024, project and toolbox component presentation "LOMOS: Runtime Security Monitoring Fit for the Cloud Continuum" by partner XLAB
- 17th PErvasive Technologies Related to Assistive Environments (PETRA) conference, 26-28 June 2024, project presentation "A Way Forward for the MDCG 2019-16 Medical Device Security Guidance" and publication by partner KU Leuven and cluster projects
- Euroanaestesia 2024, 25-27 May 2024, project presentation by partner RGB
- GETS Conference Annual Governance of Emerging Technologies and Science Conference, 16-17 May 2024, project presentation "Legal Challenges in the Internet of Medical Things (IoMT) in the EU – The Plea for Legal Clarity" by partner KU Leuven
- NEMECYS workshop at San Raffaele Hospital in Milan, Italy, 13-15 February 2024, participation of partner MCI
- Medica Fair, 13-16 November 2023, booth of partner RGB and project presentation
- Geneva Digital Law Research Colloquium, 22 June 2023, project presentation "Using AI Robots in Medicine: the interplay between technology, medicine, and law as a gateway for discovering an appropriate liability regime" by partner KU Leuven

Among the above events, the final hybrid workshop, held by Ospedale Pediatrico Bambino Gesú during the last plenary in Ljubljana, was particularly important as it gathered sibling projects and representatives from Health Ministries of Poland, Germany, Austria, and the Medical Chamber of Slovenia. Topics included patients' data protection, synergies among cluster projects, exploitation and standardisation, and projects' visibility in the wider EU-healthcare arena. This event represented another important occasion to reinforce collaboration and commitment towards cybersecurity in healthcare. A full summary of the event is available as a video and on the website.

Further, Niño Jesús Hospital and Bambino Gesú organised two workshops (in September and October) for their medical staff. While the Spanish hospital and partner EVIDEN presented the Toolbox, Bambino Gesú focused on the importance of training medical staff. Specifically for Ospedale Pediatrico Bambino Gesú, their workshop had a total of 58 attendees from different hospital departments including clinical wards, clinical engineering, clinical and laboratory research office, administration office, and IT personnel. The workshop hosted the following speakers:

- Alberto E. Tozzi - Head of the Predictive and Preventive Medicine Research Unit, Bambino Gesù Children's Hospital. Mr. Tozzi presented the CYLCOMED project and highlighted the importance of cybersecurity during remote monitoring of severe pediatric patients.
- Diana Ferro – PhD Reseach and Health Data Scientist in the Predictive and Preventive Medicine Research Unit concluded the workshop emphasizing the importance of integrating cybersecurity into a translational framework that aligns clinical care and research activities.
- Flavio Poletti - Head of cybersecurity office, Bambino Gesù Children's Hospital. Mr. Poletti discussed the most common behaviors that pose cybersecurity risks and outlined the most important precautions to take in the hospital.
- Gaetano Marrocco - Head of Pervasive Electromagnetic Lab, Tor Vergata University . Mr. Marrocco addressed the most important cybersecurity threats to medical devices, with a specific focus on implantable devices.
- Mirko De Maldè - CEO of Moveax. Mr. De Maldè presented cybersecurity challenges related to research projects and introduced methods for privacy preserving data sharing techniques.
- Giulio Barletta - DPO Office - Bambino Gesù Children's Hospital. Mr. Barletta reviewed key regulations regarding privacy and confidentiality that apply to clinical work and medical research.

Given the engagement in the workshop, the Education Management Department of Bambino Gesù Children's Hospital decided to plan and develop a structured educational program on cybersecurity for the hospital staff.

Finally, participation in HIMSS Europe 2025 (11-12 June) was also notable and contributed to generating further project's visibility. Considered as one of the biggest global conferences in the field of healthcare information technology and management, HIMSS attracts every year a plethora of stakeholders, from IT specialists and healthcare professionals to policymakers, ensuring broad visibility and networking.

HIMSS25 Europe amplified the project's visibility through:

- 290K+ social media impressions
- 77K+ subscribers via email campaigns
- 18M+ digital ad impressions
- 62% PR share of voice, affirming strong visibility within the digital health landscape

At HIMSS Europe 2025, CYLCOMED was represented by partners Ospedale Pediatrico Bambino Gesú, that participated in the European Projects co-creation workshop by highlighting its strides in their project pilot, and Martel, who covered project's participation from a media and editorial standpoint by publishing 7 social media posts (accounting for 998 impressions and 496 members reached on LinkedIn) and a website article (that genereated 46 page views).

In addition, Ospedale Pediatrico Bambino Gesú's representative, Dr. Diana Ferro, shared insights into her participation on HIMSS TV, and participated in the European Projects workshop organised by NEMECYS project on 13 June, reinforcing the cooperation with cluster projects.

2.7 Synergies With Other Projects And Initiatives

The CYLCOMED project has been part of a cluster of projects committed to boost the cybersecurity of connected medical devices since its onset. Once a month, representatives of projects CYLCOMED, SEPTON, ENTRUST, MedSecurance, NEMECYS and CYMEDSEC meet to discuss common initiatives that can support cluster's visibility and the maximisation of projects' results. The cluster was created in July 2023. Notable joint actions include:

- CYLCOMED final workshop on EU perspectives in Healthcare, October 2025
- Cluster paper "MDCG 2019-16 Guidelines: Case Study-Based Assessment and Path Forward, May 2025
- Participation in cluster workshop "Innovative Solutions for Cyber Risk in Medical Devices: A Hands-on Approach", organised by NEMECYS project, 13 June 2025, Paris, 15 participants
- Participation in the European Projects Co-creation workshop, that with 264 attendees ranked in the top 10 most attended sessions of HIMSS 2025, 11 June 2025, Paris
- Participation in the EU Projects Pavillion at HIMMS 2025, drawing an interested audience of over 200 participants, 10-12 June 2025, Paris
- Cluster webinar "Advancing Cybersecurity in Healthcare", organised by CYLCOMED, with the participation of projects CYMEDSEC, MedSecurance and NEMECYS, 34 participants and 46 views, November 2024
- Cluster paper A Way Forward for the MDCG 2019-16 Medical Device Security Guidance, May 2024

2.8 Impact Creation Monitoring

Throughout CYLCOMED's lifecycle, Communication and Dissemination KPIs were regularly monitored to help ensure the project's progress was effectively maximised. Overall, partners actively engaged in a wide range of activities, including presentations, participation in sibling project meetings, and industry conferences, to enhance visibility and support dissemination efforts.

While meeting all KPIs proved occasionally challenging, particularly when external factors beyond the project's control came into play (e.g. publication timelines), by the final stages of the project, nearly all KPIs have been successfully achieved.

The table below provides a comprehensive breakdown of all communication and dissemination KPIs.

2.8.1 Communication and Dissemination KPIs

KPIs	Target	Status at M36
Journal publications	≥ 12 articles, including scientific publications (peer-reviewed and open access preferred) with an impact factor greater than 1,5	6 published publications; 2 currently submitted (under review)
Flyers Posters/roll-ups	No of flyers: 6 No of posters/roll-ups: 4	6 flyers; 0 posters/roll-ups
International conferences (3 in Y2, 5 in Y3, 4 in Y4)	≥12 participations/publications	18
Workshops (Y2, Y3, Y4) - (in person or online)	≥ 8 fairs and conferences where beneficiaries will take part and present CYLCOMED concept, results and demos.	6
Training Workshops (in person or online)	≥ 2 training workshops with 40 stakeholders attending each workshop.	1 training workshop (OPBG); 1 training workshop (FHUNJ); 1 training workshop (RGB), 1 training workshop (INOV)
Workshops for Developers	Workshop for developers organised in Y3 with >= 30 participants	In person workshop with cluster projects
Project website	≥ 1500 unique visitors (average per year)	1300 average per year
Video clips	≥ 6 online videos	7
Social media	Project accounts on Twitter and LinkedIn: ≥ 1,000 connections/followers in total; ≥ 60 posts on social networks	642 followers 164 posts
Press releases/ newsletters	≥ 4 press releases to be translated and published by the consortium members ≥ 6 newsletters (one every 6 months)	4 press releases; 6 newsletters

Multimedia training materials	12	12

Table 1: Communication and Dissemination KPIs

2.9 Lessons Learnt

The CYLCOMED project brings together partners from a range of industries, including healthcare, technology, legal, consulting, and cybersecurity, making a multidisciplinary framework a core strength from the outset.

To ensure progress was aligned and results could be acted upon promptly, partners developed a habit of regularly updating one another, reinforcing the importance of timely and effective communication across disciplines.

3 STANDARDISATION ACTIVITIES AND OUTCOMES

3.1 CYLCOMED Standardisation Mission and Key Takeaways at Month 36

CYLCOMED Task 7.3 equipped partners with essential skills and knowledge through a series of training sessions, enabling effective engagement with standardisation practices while promoting innovation and knowledge valorisation across industries and among tool developers. CYLCOMED was selected for a dedicated consultation under the EU Booster program, an initiative offered by the European Commission. As a result, partners have been cooperating with EU Booster experts in the field, with whom the consortium had very productive interactions. The booster consultancy facilitated the contact with the CEN TC251 coordinator for the IEEE 11073 standard. Within the Booster service, CYCLOMED opted for the identification and adaptation of standards that are valuable for the specific methods and tools developed and used by partners. The focus in year 3 has been on learning more about the current development status of the most applicable standards and discussing improvements. All this has been summarised in a presentation ("HSBooster on Medical Cybersecurity Standardization") made by RGB to the consortium and the EU Booster assigned expert.

Below is a list of key takeaways from the Booster consultation:

- The CYLCOMED consortium has been working with an EU expert under the standardization umbrella and has reached a high level of awareness regarding applicable standards in their particular domain.
- The ISO/IEEE 11073 (SDC protocol) has been identified as the primary standard to consider achieving interoperability among connected medical devices (CMDs). As it inherently addresses interoperability challenges, cybersecurity is already integrated within its framework. Additionally, there is potential for CYLCOMED tools to contribute valuable insights to the standard, offering possible enhancements that could be shared with the relevant Standards Development Organisation (SDO).
- The CEN TC251 standardisation group has been identified and contacted regarding ISO/IEEE11073. Members were invited to a videoconference on providing explanations on the CYLCOMED KERs development. The CYLCOMED consortium is supporting the promotion of the standard. Partner RGB sent a newsletter to over 4000 stakeholders, including hospital management and procurement responsible, doctors and medical devices manufacturers and distributors.
- The CYLCOMED consortium has been working on the adaptation of the tools to MDCG 2019-16 standard.

Future cybersecurity tools will likely focus on orchestration, automation, and advanced threat detection. As SDC implementations mature and become more widespread, we can expect to see:

- Centralised security management platforms: tools for managing certificates, access policies, and security configurations across a large fleet of SDC-enabled devices.
- Automated vulnerability scanning and penetration testing tools specifically for SDC environments.

- AI/ML-driven anomaly detection and threat intelligence for SDC networks: systems able to identify unusual behavior indicative of a cyberattack.
- Integration with broader hospital cybersecurity frameworks: tools bridging the gap between medical device cybersecurity and the hospital's overall IT security posture.

3.2 Cybersecurity Standards

The CYLCOMED consortium reviewed applicable standards, as highlighted in a dedicated document, which contained the work performed under the supervision of the booster service. A summary is presented below:

The EU's Medical Device Cybersecurity Mandate:

MDR&NIS2: The "Why"

Cybersecurity is now a **mandatory patient safety requirement** in Europe.

- The Medical Device Regulation (MDR) is the primary, legally binding law that governs all medical devices in the EU.
- The MDR makes cybersecurity a mandatory safety requirement under its General Safety and Performance Requirements (GSPRs).
- Manufacturers must design devices according to the "state of the art" to protect against unauthorized access and prevent patient harm.
- Wider Context: NIS2 Directive: The EU's broader NIS2 Directive sets out a general, horizontal cybersecurity baseline across critical sectors, including Health. NIS2 introduces strict requirements for Risk Management and Incident Reporting, with fines up to €10 million or 2% of turnover.

The Bridge — MDCG Guidance (The "What to Do")

MDCG Guidance: Bridging the Law and the Technology

The MDCG interprets the law, mandating a Security-by-Design approach.

- The Medical Device Coordination Group (MDCG) issues non-binding guidance (e.g., MDCG 2019-16 Rev.1) to officially interpret the MDR's broad GSPRs.
- MDCG's Role: It acts as the necessary bridge, translating abstract legal safety requirements into concrete, lifecycle-based cybersecurity activities.
- **Key Requirements (Security-by-Design):** The guidance mandates integrating security from development through post-market phases. This includes:
  - **Risk Management:** Assessing the impact of threats on **patient safety**.
  - **Secure Design:** Requiring security throughout the product lifecycle.
  - **Post-Market Activities:** Establishing processes for **vulnerability management** and timely patching/updates.
- For the Health sector, the MDCG Guidance serves as a **sector-specific interpretation** for meeting the high-level security goals of the NIS2 Directive and the MDR.

The Solution — IEEE 11073 SDC Protocol (The "How to Do It")

Technical Conformity: Using IEEE 11073 SDC

The SDC protocol provides a standardized, secure pathway for interoperability.

- The **IEEE 11073 SDC (Service-oriented Device Connectivity)** protocol is an international standard that enables **safe and manufacturer-independent interoperability** for medical devices at the point of care (e.g., OR, ICU).
- **The Power of SDC:** SDC is a powerful **enabling technology** that manufacturers use to **prove conformity** with the "state of the art" and MDR requirements.
- **Built-in Security Features:** SDC directly implements the technical controls required by the MDCG Guidance:

  - **Mutual Authentication:** Mandates **TLS encryption** and X.509 certificates to ensure only authorized devices communicate. This directly addresses the MDR's **unauthorized access** requirements.
  - **Data Integrity:** Ensures clinical information is secured via **end-to-end encryption**.
  - **Risk-Based Authorization:** Uses **Participant Key Purpose (PKP)** standards to grant fine-grained, risk-based access to specific device functions.

Most important of all, CYLCOMED partners have identified that this particular IEEE11073 standard, which started its conception in the 80s, is finally started to be deployed. This fact was detected in the last Euroanaesthesia Congress (ESA 2025) in Lisbon, where it was disclosed that this standard is being adopted by large players like Dräger, GE, Mindray and Philips among others under the protocol acronym SDC.

This is highly significant and has served as a key message for the developers of CYLCOMED's cybersecurity tools, as it provides a clear indication of where the project's results could be further exploited and brought to impact. Considering this fact, the CYLCOMED toolbox becomes even more relevant, as the project proposes implementing software-based cybersecurity tools on an external board connected to the legacy device. This offers a practical short-term solution that can help avoid the need for full re-certification of existing medical devices.

As a result, one of CYLCOMED's key outcomes is the conclusion that, following a thorough review of applicable standards, the consortium is well-positioned to exploit the project's results, even beyond CYLCOMED's official timeframe.

3.2.1 Training Sessions About Relevant Standards

During 2025, several presentations were provided by the CYLCOMED consortium with the goal of deepening the consortium's knowledge of relevant industry standards. Below list provides a comprehensive overview of them.

- RGB Presentation by the EU booster expert and CYLCOMED Consortium on current applicable standards, November 2024, Ricardo Ruiz (RGB).
- Presentation of EU standardization booster expert to CYLCOMED partners about current applicable standards, January 2025.

- Internal dissemination to CYLCOMED partners about current status of IEEE 11073 standard, Ricardo Ruiz (RGB).
- Presentation “Risk Management Applied to Cybersecurity and Privacy with ISO27001, ISO27701 and ISO 27005. A birds-eye view of what Cybersecurity Risk Management is”, December 2024, João Rodrigues (INOV).
- Deep consideration in the project of MDCG guidelines as presented in CYLCOMED_D3.4 - Guidance improvement.

3.2.2 Surveys on Standard-related Issues

Besides the standards already mentioned in section 3 of D7.3, particularly the MDCG guidelines, the most relevant achievement in year 3 has been the study of standard ISO/IEEE 11073 and its commercial *plug&trust interoperability SDC protocol*. The ISO/IEEE 11073 Service-oriented Device Connectivity (SDC) family of standards is a crucial development for medical device interoperability, especially in acute care settings. Below is further information on its cybersecurity implementation.

1. Cybersecurity is a Core Design Principle:

- **Integrated Security Features**: SDC standards are designed with security in mind. They incorporate stringent security protocols, including TLS-based security mechanisms with mutual authentication to ensure that only approved devices and systems can interact, and data transmitted are encrypted. This protects hospital assets and patient information from misuse or theft.
- **Data Integrity and Confidentiality**: the use of TLS protocols ensures the integrity and confidentiality of information. Secure data transport is achieved through end-to-end encryption based on X.509 public key infrastructure for digital certificate creation.
- **Authorization and Access Control**: connectivity to identified devices on the network is managed based on whitelists for authorization. Manufacturers and healthcare organisations also need to implement and manage trust stores, permit/deny lists, and action authorisation matrices.
- **Zero-Trust Cybersecurity**: some implementations and kits for SDC are already incorporating a zero-trust cybersecurity approach, further enhancing security.

2. Key Standards and Their Role in Security: The SDC family comprises the "*Participant Key Purpose (PKP)”* and "*Device Specialization (DevSpec)”* standards.

- Core Standards (e.g., ISO/IEEE 11073-20702 Medical DPWS, ISO/IEEE 11073-10207 Domain Information and Service Model, ISO/IEEE 11073-20701 Architecture and Binding): these lay the foundational interoperability and include mechanisms for safe and secure data exchange in a distributed system, and dynamic network participant discovery. Medical DPWS (MDPWS) is derived from OASIS DPWS and defines extensions and restrictions for medical device safety requirements.
- Participant Key Purpose (PKP) Standards (e.g., ISO/IEEE 11073-10700 Base PKP, P11073-10701 for metric data, P11073-10702 for alerts, P11073-10703 for external control): these define requirements for participating providers and consumers, allowing manufacturers to have expectations about how other manufacturers' devices will behave. This common understanding is crucial for performing risk management, verification,

validation, and usability engineering for safe and secure system functions. The latest versions of PKP standards, like ISO/IEEE 11073-10700-2024, explicitly address requirements for the allocation of responsibilities for SDC base participants, contributing to overall system safety and security.

3. Ongoing Challenges and Mitigation:

- **Expanded Attack Surface**: increased connectivity, while beneficial, expands the attack surface for cyber threats like data breaches, ransomware, and Denial-of-Service (DoS) attacks.
- **IoMT Vulnerabilities**: IoMT (Internet of Medical Things) devices can have vulnerabilities (e.g., unpatched firmware, default credentials).
- **Balancing Security and Usability/Patient Safety**: a significant challenge is to implement robust security measures without negatively impacting clinical treatment and patient safety by preventing or delaying authorised access.
- **Legacy Device Integration**: integrating older devices that may not fully support SDC's security features presents a challenge.
- **Compliance and Regulatory Adherence**: adhering to regulations like HIPAA and GDPR for patient data protection is paramount.

Mitigation Strategies:

- **Robust Encryption and Authentication**: strong encryption (e.g., AES-256 for data at rest, TLS/SSL for data in transit) and robust authentication (e.g., MFA, X.509 certificates) are critical.
- **Access Controls and Network Segmentation**: role-based access controls (RBAC) and network segmentation help isolate medical devices and limit the impact of a breach.
- **Regular Audits and Patch Management**: regular security audits, vulnerability assessments, and timely patching of firmware and software are essential.
- **Secure API Design and Incident Response**: secure API design and a comprehensive, tested incident response plan are also vital.
- **Collaboration**: continued collaboration between healthcare providers, policymakers, and technology developers is necessary to address implementation challenges and ensure compliance.

4. Continuos Evolution:

- The IEEE 11073 series is continually evolving to meet the changing needs of the healthcare industry and keep pace with technological advancements and emerging cybersecurity threats. This includes exploring the integration of AI and machine learning for proactive threat detection.
- New standards and amendments are regularly published to enhance existing protocols and address new challenges. For example, amendments to nomenclature standards are being developed to include terms relevant to SDC systems.

In summary, ISO/IEEE 11073-SDC is actively addressing cybersecurity through its inherent design principles of mutual authentication, encryption, and robust data integrity measures. However, the dynamic nature of cyber threats in healthcare means continuous vigilance, updates to standards, and strong implementation practices in order to maintain a secure interoperable medical device ecosystem.

3.3 Booster Results

HSbooster.eu is a 30-month initiative funded by the European Commission, offering the European Standardisation Booster. This service delivers expert support to European projects, helping them accelerate their path to market through strategic engagement with standardisation.

The CYLCOMED consortium has interactively participated in the EU standardization Booster. During the booster training, the consortium shared with the reviewer our current state of awareness about the applicable standards for the CYLCOMED project. In return, the expert shared his view in a dedicated document, titled “HSbooster.eu Final Analysys.pdf”, after the consortium’s identification of the SDC protocol as a relevant one, the Booster service put CYLCOMED in contact with the SDO in charge of coordinating efforts for the ISO/IEEE 11073 works.

The advances made by the SDO suggest a roadmap towards full deployment of e SDO. Thanks to the EU standardization booster consultancy, CYLCOMED got in touch with the CEN TC 251 coordinator and learnt about the great impact that the deployment of ISO 11073 standard will generate.

The OR.net is an association coordinating all efforts around SDC, including networking and joint ventures. The association provides a member list on their website for promising candidates (e.g. Narcotrend).

Paths for ISO/IEEE implementation

For legacy devices seeking interoperability with SDC, manufacturers have several options, depending on factors such as the device’s existing hardware capabilities, applicable regulatory requirements, and how hospitals are currently using these devices. Below is an overview of the available pathways.

A. The most robust, but also the most resource-intensive, approach is to perform a full firmware update on the device, integrating an SDC library that enables native communication over a network interface. This option requires sufficiently powerful hardware, reliable network access, and a mechanism for deploying firmware updates. Since this involves modifying the software of a medical device, it falls under the scope of the Medical Device Regulation (MDR) and must comply with ISO 13485 for development and lifecycle management, in accordance with the device’s applicable safety classification.

B. The second most robust approach is similar in nature, with many of the same challenges, though it may offer shorter development time. In this case, a separate software component would handle the translation between SDC and the device’s proprietary communication protocol. Depending on how the system is integrated and the nature of the data exchanged, this solution could fall under a different safety classification, which may have regulatory implications.

C.

1. The approach that some other manufacturers like Dräger have already gone in the past is to have a separate piece of small connector hardware (a small micro-pc the size of a raspberry-pi), usually directly attached to the legacy device. The connector then talks to the legacy device using its regular interface, which usually is a serial port, and on the other end outputs SDC messages over an ethernet/wifi port. The main advantage here is that this is a minimum effort retrofit for most hospitals, as no updates or external connection of the device is required, and no native ethernet interface on the legacy device is required. However, in my opinion the main advantage is that, according to the MDR, a component that merely translates signals from one format to another is

not categorized as “Medical Device” and there for its development does not fall under ISO 13485.

2. (A variation of the C1 approach): instead of deploying a dedicated connector device for each legacy device, it is also possible to use a centralised, “server-scale” connector that handles protocol translation for multiple devices simultaneously. This approach is particularly effective for smaller devices or scenarios where several devices operate together in a shared setup, such as infusion pump racks, allowing for streamlined integration and reduced hardware overhead.

These approaches (excluding C2) are also detailed by specialised companies such as Surgitaix, which provides a commercial SDC software library called sdcX. More information can be found on their product page. To access the evaluation environment, an NDA must first be signed. Once in place, Surgitaix provides access to a virtual machine image for evaluation purposes. The image can be downloaded here. This is an .ova file that can be run using VirtualBox. It contains an Ubuntu 24.04 LTS system preconfigured with examples demonstrating how to use and integrate the sdcX library binaries. The sample project, HelloSDC, is located in the sdcX directory within the default user’s home folder. To set up the environment, the user should run the update.sh script found in the same folder. Once the setup is complete, a Visual Studio Code project will be available with buildable examples of the sdcX library, which you can explore and modify as needed.

3.4 Lessons Learnt And Future Steps

The CYLCOMED toolbox concept adapts well in the hospital equipment, and its implementation as an external board is a first step towards minimizing certification issues of legacy devices. However, there are grounds for improvement for enhancing medical functionalities (such as CYLCOMED’s use case’s infusion controller). The CYLCOMED implemented approach is OK for Vision Air solution, because the integration level achieved has been performed as the manufacturer has made the required user-interface modifications, as well as a route-map for alarms indications.

However, the lack of a general communication protocol between medical devices forces the OEM solution to being limited. In effect, e.g. changing the legacy infusion pump in the infusion controller would require new implementation of work for the integration of a different protocol. For other manufacturers willing to use the OEM solution, it would become cumbersome if they are requested to devote so much engineering work, e.g. adapting the proprietary protocol to the medical application.

However, ISO IEEE 11073 deployment by big players comes at the right moment. In the ESA2025 fair (June 2025), big players have presented their legacy devices incorporating the Service Device Communication (SDC) protocol (commercial name). This is an interoperability solution that operates as a universal language among medical devices in different clinical settings, ranging from critical to non-critical wards or even telemedicine. The procedure they have followed to minimize certification efforts is the use of an external board, which performs only the translation functionality between the legacy device proprietary protocol and the SDC protocol.

The acceptance of SDC, and its future agreed to wide deployment, represents a huge breakthrough for future works. The project is now well-positioned to exploit its results beyond the official CYLCOMED timeframe by aligning with this major, industry-backed standard. As a result of this, the OEM solution will “talk” SDC, thus avoiding the adaptation effort from manufacturers. Additional changes can be made, such as incorporating in the External board

all user-interface issues related to cybersecurity functionalities and alarms using an ad-hoc display. As a result, we can anticipate that this concept will make it possible for the OEM to be used without requiring legacy devices' re-certification. However, if the solution brings additional medical functionalities to those already existing in the certified legacy device, the OEM board must undergo certification. This effort, however, will be much lesser because the device is not in direct contact with the patient.

4 EXPLOITATION ACTIVITIES AND OUTCOMES

CYLCOMED has been supported in this task by an expert from the EU exploitation booster facility. The activities of the joint actions included:

Completion of “Module A” according to the applicable EU documentation, which relates to:

- Exploitation pillars training on the G2M process and related concepts - where Market Definition Canvas and Value Proposition Canvas were described
- Assessment/review/identification of KERs

Subsequently, we targeted “Module B”, on the assessment of the unique value proposition (UVP) of KERs.

The Exploitation Strategy was refined to effectively present to the European Commission. In the various meetings, the expert emphasised the importance of demonstrating how we plan to bring our results to market and the necessity of securing funding for our innovations.

- **Business Case Development:** The EU expert shared insights on how to create a compelling business case, highlighting the need to clearly define the problem we are solving, demonstrate the market potential, and outline the competitive landscape. He stressed that the first page of any proposal should convincingly present the problem and our solution to capture the interest of reviewers and investors.
- **Willingness to Pay:** We discussed the importance of establishing the willingness of the client to pay for our solutions. This involves quantifying the costs associated with the problems we aim to solve and demonstrating the value our solutions provide to potential customers.
- **IP Ownership and Collaboration:** A significant portion of the discussion focused on the ownership of intellectual property (IP) and how to fairly distribute ownership among partners, especially considering the contributions made by hospitals and other stakeholders. It was suggested that it is needed to define our roles and commitments clearly to ensure a collaborative approach moving forward.

4.1 Exploitation Objectives

The first step included the definition of the main KERs of the project.

In this regard, two main KERs were defined, as outlined below

- **KER 1, CYLCOMED TOOLBOX:** involves various tools that mostly but not entirely interact with each other, and perform specific functions in each of the project's pilots. On the other hand, not all tools participate in all scenarios. Therefore, to better describe the structure of CYLCOMED's Toolbox, its modularity, flexibility, adaptability, and efficiency, we have grouped the tools into four layers that make up the final toolbox architecture:

  1.- Data Collection and Analysis Layer
  2.- Device Integrity, Security and Service Management Layer
  3.- Identity, Access Management and Data Protection Layer
  4.- Security Dashboard and Visualization Layer

Tool name in GA (picture of toolbox)	Tool Name in D7.3 (table 5)	Tool name in D6.2	Proposed acronym	Owner
AI-Behavioural Analysis	AI-Behavioural Analysis	Live anomaly detection system	LADS	ATOS
AI powered log monitoring	CMD Log Monitoring	Log moniotring system	LOMOS	XLAB
IAM & data protection	uSelf for Medical Data	Self sovereign identity solution	LuS4MED	Atos
IAM & data protection	Functional Encryption for Medical Data	Data protection solution	FE4MED	Atos
IAM & data protection	Open Policy Agent	Authorization solution	C-OPA	MARTEL
External Linux Board	Device Integrity Check	CMD integrity		RGB
Security dashboard	Cybersecurity Dashboard	Security dashboard		Atos

Table 2: Toolbox components

From a clinical perspective first, Vision AIR's User Manual indicates the Tool box installation procedures to carry out.

STRATEGY

In developing the exploitation strategy, the consortium placed a particular focus on the use cases defined for Pilot 1 and Pilot 2 within the CYLCOMED project. While the CYLCOMED

software tools are designed to support both scenarios, the market potential for Pilot 2 (telemonitoring) is considered more readily scalable than that of Pilot 1 (hospital equipment).

Pilot 1 is centered around a NeuroMuscular Transmission (NMT) intelligent infusion controller. Our analysis also considered the commercial potential of the Linux External Board, which integrates CYLCOMED's full suite of cybersecurity components alongside other clinical functionalities. However, due to system constraints, each Linux Board can only execute one of the additional tools provided in the CYLCOMED Toolkit.

In contrast, other cybersecurity tools within the Toolkit have broader business potential, as they can be adapted and deployed in various contexts beyond the Linux Board, such as automotive, avionics, railway, industrial, etc.

In the same medical Hospital Equipment field, the Linux Board could also serve as an interoperability hub, enabling legacy medical devices, such as infusion pumps or multiparameter monitors of various brands, to connect seamlessly with Hospital Information Systems (HIS). This represents a valuable opportunity for retrofitting older equipment with modern connectivity and security features. Besides the Linux Board, the remaining CYLCOMED cybersecurity software components can be applied in other domains of the medical sector, each offering distinct market expansion opportunities. Only in the medical sector, these domains may include telehealth, personal health devices, homecare systems, or industrial medical IoT platforms, among others.

- **KER 2,RISK MANAGEMENT:** The Risk Management Tool enables organisations to help implement various risk management frameworks and benefit-risk schemes. Due to the generality of the Risk Management Tool, it can be used by any use case where risk management is a shared responsibility. Target end users include: hospitals, Connected Medical Devices manufacturers, supply chain participants. The Risk Management Framework was tailored to be generally applicable to a wide range of risk management frameworks, and does not prescribe any framework. The Risk Management Tool has been used for managing risks, either for internal use or when responsibilities are shared among entities, to be tested by users, and for education purposes.

Strategy

Risk management tools usually fix a framework, and organizations must adhere to particular tools, hindering collaborative environments, where there are shared responsibilities among different organizations, with different frameworks.

As risk management of connected medical devices depends on several stakeholders, patients, doctors, service providers and suppliers, the need for generalization was key in enabling all parties to use the same tool, and being able to use it without their internal frameworks, standards and best practices. In contrast, based on the analysis of a wide range of standards (e.g., ISO 27001, ISO 27002, ISO 27005, NIST CSF, ISO 14971) and best practices, the Risk Management Tool was designed considering the general patterns of risk management, enabling the inclusion of any standards, or even combinations.

4.2 Key exploitation Takeaways

Main lessons learnt from M18 to M36 of the project.

The Foundation for Cybersecurity Needs is based on the fact that digital transformation in healthcare, driven by the widespread adoption of Connected Medical Devices (CMD), has created unprecedented cybersecurity challenges. CYLCOMED is aligned with the primary goal, to facilitate the adoption of security tools to reduce risks in CMDs.

Device Market Growth is huge, and its size is a key indicator of the need for security solutions. This market is expected to grow at a Compound Annual Growth Rate (CAGR) of approximately 10.10% between 2022 and 2028.

The CYLCOMED Key Exploitable Results have been identified. These are the competitive Edge of CYLCOMED cybersecurity tools:

- LADS: Faster detection of zero-day attacks.
- LOMOS: An AI-driven, flexible anomaly detection tool already validated in a demanding hospital scenario.
- FE4MED: It is an Attribute-Based Encryption (ABE) solution that ensures fine-grained access control while protecting data both in transit and at rest.
- LuS4MED: It is a decentralized authentication framework built on Self-Sovereign Identity (SSI), empowering users with complete control over their personal data and credentials."
- Cybersecurity Dashboard: Offers high usability with centralized visual insights for informed decision-making.
- C-OPA: A general-purpose and highly flexible policy engine for securing any service or component.
- External Linux-based board: as OEM solution to minimise medical system certification with cybersecurity tools
- Risk Management Tool: offers a general solution for risk management, without fixing any specific standard.

4.2.1 Customers/stakeholders

It is relevant to mention that market approach to market is not the same depending on the CYLCOMED partner. This represent an added difficulty when trying to reach IP agreements:

RGB: Healthcare institutions; Industrial Manufacturers/ Anesthesiologists.Others: Anesthesiologists, Hospital purchase dept, Hospital Technical Service, Medical Devices manufacturers; Specialties distributors; CMD Platform Integrators

ATOS: For the Toolbox, healthcare institutions; for individual tools, system integrators.

XLAB: Early adopters are expected to be pilot hospitals within the CYLCOMED consortium. These hospitals will use LOMOS to monitor their connected medical devices and provide feedback to refine the tool for broader CMD market adoption. Others: Hospitals & Care Centres, CMD Manufacturers / Authorised Representatives & Suppliers,Telemedicine/ CMD Platform Integrators, SMEs active in Healthcare domain.

MARTEL: Given the general-purpose nature of the C-OPA component, it could theoretically fit any scenario where a service needs to be secured with arbitrary security policies. Within the CYLCOMED scenarios, the focus was on protecting access to an encryption/decryption

service, to ultimately help secure the data being recorded by medical devices. Pilot hospitals are likely to be the first to make use of our solution. But theoretically, any service provider or software developer needing a solution for securing their services and/or components will likely be the ones to benefit the most from what C-OPA provides.

INOV: Due to the generality of the Risk Management Tool, it can be used by any use case where risk management is a shared responsibility. Target end users include hospitals, Connected Medical Devices manufacturers, supply chain participants, etc.

4.3 Partners Exploitation Plans and Commitments

An overview of joint exploitation options has been defined, clarifying the potential path to market. These options include the potential setup of a spin-off company and/or separate exploitation by individual partners, with legal structures also considered.

Clarifying the KERs' offer, the VP has been described, detailing the concept, stakeholders, and their contributions. The Unique Selling Proposition (USP) has also been defined in D7.3 (section 4.5.2). The product to be sold has been described in more detail via a "Catalogue of the CYLCOMED assets and requirements" in D7.3 (section 4.5.1). The client base has been better explained in D7.3 including separate subsections detailing the specific client types and key challenges for both the hospital equipment and telemedicine use cases. An Exploitation & Business Plan has been created presented in D7.3 and its annexes, using detailed information gathered from partner surveys. Also, a Business Plan, including business cases for the pilots, has been described in section 4.5 of D7.3.

A draft IPR Agreement was included in Annex 7.1 of D7.3. It has now been adapted to represent the current consensus among partners on the strategy for managing intellectual property. The last version of the IPR Agreement is being agreed upon with the following contents:

- The Key Exploitable Results (KERs) are described.
- A joint IPR Agreement by partners defines ownership of the Key Exploitable Results.
- This document will serve as a Memorandum of Understanding for future commercial exploitation agreements.
- Clear Ownership:
  - ATOS: Owns LADS, LUS4MED, FE4MED, and the Security Dashboard. Plans to include the tools in its cybersecurity for healthcare portfolios and pursue separate exploitation.
  - RGB: Owns the External "Linux Board". Will lead the commercialisation of the Linux Board and NMT controller, presenting KERs to investors and early adopters.
  - XLAB: LOMOS is background IP of XLAB. Will focus on market positioning, promotion at industry fairs, and extended collaboration with hospital partners to promote the LOMOS success story.
  - MARTEL: Will present the C-OPA tool to relevant groups once the asset is confirmed.

The document reflects the awareness of the collaboration potential and the benefits of working together on future projects. However, while there is a clear interest, it is difficult at this TRL

level to reach specific compromises. However, the collaboration proposal will be made possible when specific business opportunities can be reached.

4.4 IoT Cybersecurity Market Considerations in the Healthcare Sector

When taking into consideration the market potential of cybersecurity tools, it must be understood that these are “horizontal” type of solutions applicable to many domains (such as telemedicine, hospital equipment, etc) of different sectors (medical, automotive, railway, avionics, industry, etc).

4.4.1 The Global IoT Security Market indexes and Growth Drivers in the Healthcare Sector

Considering devices which are directly relevant to the healthcare industry's increasing adoption of connected medical devices (CMDs). The sources indicate a significant and rapidly growing market for IoT security solutions in general. The global IoT security market is projected to grow from USD 14.9 billion in 2021 to USD 40.3 billion by 2026 [1,2].

This represents a Compound Annual Growth Rate (CAGR) of 22.1% during this forecast period. The market is described as very diverse and competitive, with various key players from different sectors.

The IoT cybersecurity market in the healthcare sector is poised for continued growth. This trend is propelled by several key factors:

- Digital Transformation: the healthcare industry is undergoing a digital transformation with the widespread adoption of IoT devices, telehealth solutions, and CMDs.
- Data Protection: as healthcare organisations embrace these technologies, they face significant cybersecurity challenges, creating a need for robust measures to protect sensitive patient data and ensure medical system integrity.
- Regulatory Mandates: regulations from security authorities in North America and Europe, such as Europe’s General Data Protection Regulation (GDPR), have compelled companies to improve IoT security measures like device authentication, secure connectivity, and data loss prevention.

In view of the above, we will restrict the market analysis to the domains of pilots 1 and 2.

4.4.2 Market potential of the pilot 1 on Infusion Controller and MD hospital equipment

RGB is currently competing with two unique devices with exclusive functionalities (Vision DUO and Vision Air) in the High-Acuity Patient Monitors & Consumables market; it was valued at over 2.500M€ in 2024 and is set to increase to 3.200M€ by 2029. Hemodynamic Monitoring and Depth of Sedation Monitoring remain in the two largest markets. Regional Oximetry and NMT Monitoring will be the fastest-growing segments, driven by clinical recommendations and an increasing emphasis on multi-high-acuity parameter monitoring [3,4]

Vision AIR launched in 2023 as the first multiparameter monitor for real-time monitoring of main vital signs including NMTCuff®, capnography and respiratory rate to alarm for respiratory failure typically after surgery, in intensive care and on the general care floor. The patented

product is based on extensive research; it is CE-cleared and has been validated on more than 3 million patients. The multiparameter monitor includes several modules such as ECG, respiration, oxygen saturation, blood pressure (invasive and noninvasive), 2 temperatures, capnography, and anesthetic gases, as well as cardiac output. The device features wireless and cable communication for connection to the central station and information systems. The target market is made of sophisticated hospital wards such as Operating Room (OR), similar to Vision DUO, recovery room and Intensive Care Unit (ICU).

Vision AIR is a complementary product line to accelerate the market penetration of VISION DUO, with leverage from the respective sales forces, distribution channels, and network. It captures a larger share of the patient's journey (beyond the operating room), increasing the addressable market value by more than 4x. There are operational synergies in not just sales and marketing, but also in manufacturing, R&D, regulatory affairs, and administration.

4.4.3 Market potential of Pilot 2, the telemedicine Use Case

The global telemedicine market is substantial and projected to grow significantly, expected to reach USD 330 thousand million by 2029.

The primary target market for this technology is the management and prevention of chronic diseases, with a particular focus on cardiovascular diseases (CVDs) and hypertension. This focus is driven by the significant healthcare burden these conditions represent.CVDs are the leading cause of death globally, accounting for an estimated 17.9 million deaths each year, which is 32% of all global deaths.

In Europe, CVDs cause over 3.9 million deaths annually, and heart failure (HF) alone affects more than 15 million Europeans.

Hypertension is also highly prevalent. A 2022 global study found that 36% of participants were hypertensive, with Europe having the highest prevalence at 48.9% [5,6].

The business model for technology providers involves supplying devices for companies that manage telemedicine services, through either direct purchase or a rental model. These solutions can be embedded within broader telemedicine ecosystems to support healthcare providers, general practitioners, and individual users in monitoring chronic conditions.

4.4.4 Key Challenges encountered

The most relevant key challenges to achieving the wide deployment of pilot's technology can be grouped into technological, regulatory, and systemic hurdles.

Technological Readiness and Development

- Incomplete Development of Key Features: in the case of pilot 2, a significant challenge is that medical grade solutions can be far from being ergonomic, and viceversa. Precision and User friendliness is a must. Therefore, a major hurdle for medical technology is to complete its development and prove its reliability and effectiveness in real-world settings.

Regulatory and Clinical Validation

- Pending Certification: for pilot 1, although components are technologically mature, certification is still missing. This is a crucial step required to open the door to the market. Certification of Pilot 1 can be described as " difficult" due to the fact that it is class III

("life-dependant"). It remains a pending task before the product can be commercially launched.

- Need for Extensive Validation: the pilot 1 solution requires "extensive validation in real-world settings" to ensure it is ready for wide-scale impact to ensure the solutions are clinically relevant and designed for real-world implementation.

Systemic and Patient-Related Hurdles

- Integration into Healthcare Models: In pilot 2, a significant challenge is the need to move towards an integrated care model. Current care models often focus on managing single diseases, whereas many patients suffer from multimorbidity (multiple concurrent diseases). There are still significant knowledge gaps around comorbidity, and successful wide deployment requires the technology to facilitate coordination and fit within a more holistic approach to patient care.
- Overcoming Patient-Side Barriers: the success of pilot 2 telemedicine is tied to patient behaviour. Factors that contribute to hospital admissions include patients' lack of adherence to medication and diet, lack of knowledge of symptoms, and lack of access to healthcare professionals. While the technology aims to address these issues, its wide deployment depends on its ability to effectively engage patients and secure their adherence, which the ergonomic design and user-friendly app are intended to facilitate.
- Market Timing: there must be a strategic challenge related to market readiness and timing. The overall adoption by healthcare providers and users is anticipated within a 3-5 year timeframe after certification approvals.

4.5 CYLCOMED Strategic Targets at M36

The study that follows is based on the fact that products/services certification has been achieved. The CYLCOMED consortium will continue efforts after the project time frame (although each partner searching for its own route). CYLCOMED has offered partners a great opportunity to know each other, and therefore it is expected and there is an intention to find market opportunities. However, there is a missing route towards certification before free sales can start to happen. The subsection below describes the required approach to certification in the case of Hospital CMDs type of equipment.

4.5.1 Approach to certification

Certification of medical devices is a complicated, expensive and time-consuming process.

- For this purpose, the strategy has been to incorporate the security features that result from CYLCOMED in a standard external Linux-based board, with enough CPU power so that performance of essential functionalities is not compromised. Specifically, in order to minimize certification work, we have connected via a serial channel to the medical monitoring device (legacy device) with monitoring functionalities preserved from cybersecurity hazards. The external module is intended to interoperate with the user interface SW component of the medical monitoring device, e.g. to report about the status of the SW integrity.

- There are pending key works so that implementing cybersecurity tools imply a modification in the legacy devices (and certification), depending on the solution adopted such as

Protocol adaptation between the legacy device (Vision Air multiparameter monitor) and the external CYLCOMED board. Besides, some added functionalities may require a modification in the protocol, e.g. in the case that vital sign or control data is processed in the legacy device (e.g. in the case of the control algorithm being implemented in the medical device). This is the case of alarms generated by external devices (such as infusion pump), which may alter the workflow of the medical device (e.g. a "syringe empty" condition must pause the control process until solved. Also, a modification of the external peripherals (such as infusion pump's brand) will be required and the legacy device's user-interface may need to be modified accordingly if it uses control/medical data (such as alarms) to fulfil the particular application (NMT control).

Our goal is to avoid the need of re-certification of legacy devices (infusion pump's tree or multiparameter monitor) that act as components of the new medical system. The CYLCOMED external board must operate autonomously to cover the required functionalities of the more complex system.

These are:

Functional Requirements:

- **Communication hub**: It translates the various proprietary protocols from legacy devices into the ISO/IEEE11073 standard. In the future, all legacy devices will be compliant to the standard and this SW component Will not be necessary. Certification of a protocol translator is not necessary.
- **Medical added features**: In our case, the board has full information about the patient's status and can provide an AI layer for data processing. In our case, the control algorithm that determines the new dose infusion based on the patient´s status. These medical features require specific certification of the external board.
- **Display of Medical System's performance:** It is part of the new added functionality and must be certified.

Non Functional Requirements:

- **Firewall for cyber-attacks:** Cybersecurity tools will be incorporated in a transparent way inside the CYLCOMED external board. The benefit is that it implements a necessary feature without altering the legacy device.
- **Alarms:** However, for this to occur, the alarms generated will be reported to the dashboard application, which could be in a separate screen (or the one for medical application). This feature must be certified.

- As a result of a good approach to the final architecture, the benefits are several, depending on the solution adopted. Protocol adaptation between the legacy device (Vision Air multiparameter monitor) and the external CYLCOMED board means we do not need to make SW changes in the legacy devices. Thus, no legacy device re-certification for this. Besides, the installation of the close-loop controller permits to avoid SW changes in the legacy device. Thus, no legacy device re-certification for this. Also, a modification of the external peripherals (such as infusion pump's brand) will not require additional work when SDC is in place. No legacy device re-certification for this. FInally, the legacy device's user-interface using a touch screen outside the legacy device avoids making SW changes in the legacy device, related to cybersecurity or medical performance configuration or alarms to fulfil the application (NMT control). Thus, no legacy device recertification.

- However, the external board certification becomes much simpler, if we incorporate a (touch screen) display to it. This is so because the translator functionality from proprietary to SDC protocol does not require certification. As a result, theEMC validation or safety certification is much simpler, because it is not required to alter the legacy device. This way, the external board becomes a medical system when it performs medical functionalities, as it is the case with the infusion controller. Therefore, it must comply with MDR directive. At the same time, safety requirements are easier to comply with, however, than a medical device. It is a simpler device than a medical device -such as a multiparameter monitor, or an infusion pump-, with sensors and actuators in direct contact with the patient.

A concluding interpretation of the SWOT and PESTLE findings describes where the project stands in terms of market readiness, competitiveness, and external influences.

4.5.2 SWOT analysis for CYLCOMED cybersecurity toolbox

The integrated SWOT analysis incorporates information from the core enabling technology, the External OEM Board/Cybersecurity Toolbox developed in the Pilot 1 (NMT Infusion Controller) and the Pilot 2 (Telemedicine Solution).

For example, the External OEM Board in Pilot 1 is a common component that allows both the NMT Infusion Controller (for new medical functionality) and includes the Cybersecurity Toolbox (for security and interoperability) to be deployed. The combined SWOT analysis reflects these synergies and shared challenges.

Integrated SWOT Analysis: Pilot 1 & Pilot 2

This analysis covers a **Linux-based External OEM Board/Cybersecurity Toolbox** to deliver both the NMT Infusion Controller and Telemedicine solutions.

Strengths (Internal Factors)

- **Proprietary and Best-in-Class Sensor Technology:** CYLCOMED leverages the patented **NMTCuff® (CMG-based) technology** for NMT monitoring, which is considered superior to competitors (AMG/EMG) and immune to OR electrical noise. It also measures NIBP.
- **High TRL and Market Readiness for Core Products:** The flagship product, the legacy multiparameter monitor **Vision AIR** is at **TRL 9**, fully certified and ready for market. This provides a stable base for new developments.
- **Proprietary Closed-Loop Control Algorithm:** NMT Infusion controller has an advanced, patented control algorithm (derived from Fuzzy Logic) after a long history (since 1988) of developing infusion controllers. It is a unique capability for the **NMT Infusion Controller**.
- **Unique Cybersecurity/Interoperability Solution:** The **Linux-based External OEM Board** offers an exclusive, easy-to-install, and cost-effective solution for other manufacturers to meet evolving cybersecurity standards and enable interoperability with legacy medical devices.
- **Strong and Protected IP:** This asset holds a large portfolio of patents and trademarks, including **sole ownership of NMTCuff®**, exclusive commercialization rights to NMT-related joint patents, and patents for the infusion controller and telemedicine solutions.

- **Recurring Revenue Potential:** The OEM model and the Vision AIR product lines generate significant **recurrent income** from the sale of single-use and reusable cuffs and accessories.

Weaknesses (Internal Factors)

- **Weak Synergies and Cross-Selling:** NMT Infusion controller and Telemedicine product areas target different end-users (**anesthesiologists, OR/ICU staff and Home Care**) and do not share the same distribution network, not allowing for efficient cross-selling and leverage of the existing installed base.
- **Low TRL for Advanced Products:** The **Cybersecurity Toolbox** is at a low **TRL 4**. The **NMT Infusion Controller** is TRL 7, but the holistic version is TRL 5. The **Telemedicine software** is TRL 7. This wide disparity in maturity levels presents development and resource risks.
- **Long Certification Time for New Solutions:** The certification process for the novel technologies (**Infusion Controller** and **Cybersecurity Toolbox**) is lengthy and can take *at least three years*, delaying market entry and commercialization.
- **Limited Scope/Holistic Gap:** The infusion controller solutions are currently limited by the lack of reliable commercial sensors for critical parameters like pain (nociception) and consciousness (hypnosis), forcing them to rely on less reliable PK/PD models or not yet integrated systems.
- **Market Position as Technology Provider:** For the telemedicine solution, Mediaclinics is explicitly positioning itself only as a *technology provider* (selling/renting devices).

Opportunities (External Factors)

- **Massive and Growing Markets:** The target markets are undergoing exponential growth:
    - **NMT Monitoring:** Fastest-growing segment in the high-acuity market, with a potential size of $**1,5 b**illion.
    - **IoT Security:** Global IoT security market is expected to grow at a CAGR of **22.1%** to $**40.3 billion** by 2026.
    - **Telemedicine:** Global market to reach $**330 billion** by 2029.
- **Regulatory/Clinical Drivers:** Clinical recommendations (like ASA's) are driving mandatory adoption of NMT monitors. Additionally, new regulations like GDPR and security standards mandate the use of solutions like the Cybersecurity Toolbox.
- **Partnership and OEM Integration:** The External OEM Board allows for significant market penetration by partnering with major medical device manufacturers (MD manufacturers) who are eager to simplify certification and quickly adopt best-in-class NMT technology.

Threats (External Factors)

- **Certification Complexity and Delay:** The primary technical and time-to-market risk across the entire ecosystem is the complexity and length of the certification process for new medical devices, which can significantly delay all new product launches.
- **Competition from Established Manufacturers:** While CYlcomed partners have a NMT's technology superior, competing solutions (AMG/EMG for NMT) are sold by large companies that dominate the global critical care market.

- **High Reliance on Partner Adoption:** The success of the OEM board and the Cybersecurity Toolbox hinges on the willingness of MD manufacturers to integrate a third-party component into their products.
- **Technical Obsolescence/Cybersecurity Evolution:** The TRL 4 status of the Cybersecurity Toolbox means it may struggle to keep pace with the rapidly evolving and competitive IoT security market.
- **Patient/Doctor Behavioral Inertia:** The adoption of autonomous drug control and new telemedicine routines requires a significant behavioral shift from doctors and high adherence from patients.

4.5.3 PESTLE analysis for CYLCOMED cybersecurity toolbox

The **Cybersecurity Toolbox** is provided on an **External OEM Board (Linux-based)**. PESTLE analysis is carried out on the basis of this integrated solution, focusing on its function as a tool to improve cybersecurity and interoperability for Connected Medical Devices (CMDs).

PESTLE Analysis of CYLCOMED 's Cybersecurity Toolbox (External OEM Board)

P - Political Factors

- **Stringent Regulatory Mandates:** Regulations imposed by security authorities in North America and Europe are driving companies to improve IoT security measures. This includes compliance with protected data standards, commercial value data, and personal data rules, such as Europe's **General Data Protection Regulation (GDPR)**.
- **Compliance Imperative:** The healthcare sector is driven by the imperative to protect patient data and ensure the integrity of medical systems. The toolbox is a solution to help manufacturers achieve sales certificates in an ever-evolving security scenario.
- **Standard Adaptation:** Any new implementation must take into account and adapt to currently available standards in the highly regulated field of cybersecurity.

E - Economic Factors

- **Massive Market Growth:** The target market, the global IoT security market, is expected to grow from **$14.9 billion in 2021 to $40.3 billion by 2026**, representing a Compound Annual Growth Rate (CAGR) of 22.1%.
- **Cost-Effective Compliance:** The product offers a considerable **cost/effective solution** for manufacturers to obtain a certificate of sales by providing an easy-to-install, unique solution without needing deep, in-house cybersecurity experience.
- **Flexible Revenue Models:** The exploitation strategy includes manufacturing and selling the Linux board, and also finding ways to license the cybersecurity tools. This can be expanded to various service models (framework as a service, single plane as a service) or as individual components/products.

S - Sociocultural Factors

- **Digital Transformation in Healthcare:** The healthcare industry is undergoing a digital transformation with the widespread adoption of IoT devices, which promises to revolutionize patient care and enhance medical outcomes.
- **Increased Risk Awareness:** As healthcare organizations embrace connected medical devices (CMDs), they face unprecedented cybersecurity challenges, making robust security measures a necessity for protecting sensitive patient data.
- **Targeting End-Users:** Marketing efforts will target both hospital technical services and the medical device manufacturers (MD manufacturers) who provide the integration of the module into their technology.

T - Technological Factors

- **Interoperability Hub:** The board functions as an **interoperability hub**, allowing different legacy medical devices (like infusion pumps or multiparameter monitors of any brand) to connect to the Hospital Information System.
- **Legacy Device Integration:** The solution is designed to interoperate legacy medical devices and incorporate applicable cybersecurity tools, simplifying product certification because the rest of the components are already certified legacy devices.
- **Elegant and Unique Solution:** The external module is described as an "elegant solution" and unique, offering exclusive protection against cybersecurity hazards while providing a development toolkit.
- **Technology Readiness Level (TRL):** The project is currently at a relatively low TRL 4, indicating that substantial development work remains, and certification is not guaranteed within the project's timeframe.

L - Legal Factors

- **Certification Simplification Strategy:** The use of an external Linux-based board is a deliberate architectural choice to reduce costs and **accelerate certification** by embedding new functional and cybersecurity capabilities without requiring the complete re-certification of the primary medical device monitor.
- **Compliance Assurance:** The primary objective of the asset is to facilitate the adoption of security methods and tools to reduce cybersecurity risks in CMDs with respect to required security requirements.

E - Environmental Factors

- **Digital Infrastructure Impact:** The product's focus is on integrating Connected Medical Devices (CMDs) and IoT security, contributing to the digital infrastructure and connectivity footprint of healthcare, which is part of the larger technological ecosystem.
- **Sustainable Security Model:** The external module allows for continuous updates and security integration into legacy devices, extending the lifespan and functionality of existing medical equipment, which can be seen as a more sustainable approach than requiring the replacement of entire systems to meet new standards.

4.6 Roadmap for Commercialization and Future Uptake

KER 1 will be related to manufacturing a new product (Linux board) and finding ways such as licensing cybersecurity tools. It will be used in two ways:

1) As a component of the Infusion Controller of RGB
2) As an external OEM component to be linked to other legacy devices

RGB's most urgent task is to certify the medical device and make the required clinical trials so that they can obtain the necessary commercial certificate of free sale.

RGB is also in the initial stages of developing robot technologies with the potential to extend the product line over time. The team has a proven capacity to maintain its innovative leadership and brings an ability to deliver results in highly profitable markets.

There is a rapidly expanding market opportunity.

RGB estimates that the close-loop drug delivery system's demand will grow with a steep trajectory over the next years as more affordable and safe solutions are achieved.

- Addressable market exceeding 100M patients/year
- Target market of 15.000 Hospitals and 160.000 ORs in the first 10 years. The market is 400.000 ORs worldwide
- Short term is to reach 20M€ and be cash flow positive in the 2nd year after product certification, with 50% market penetration, with an estimated return of 15%
- Medium term (5 years) is to reach revenues exceeding 100M€ /year with a market share of 20% and an estimated return of 10%
- RGB sees 1,500M€ as the size of the potential market for NMTs when most of the 400.000 ORs in the world will have an essential high-end NMT monitor available.

RGB plans to incorporate CYLCOMED tools that potentially fit it this specific case and others related to CMDs in general as proof of concept. Besides, this solution could be exploited as OEM module incorporating CMD´s interoperability tools.

The Risk management tool is ready to be tested by users, and for educational purposes. With some improvement, it could be commercialized

4.7 IPR Considerations

There is an agreed strategy so that the joint IPR document is currently in progress. The role of the partners that are generating a KER has been the following in CYLCOMED:

RGB: Carry out the Exploitation Booster's activity; In case of a valid Unique Value Proposition, has planned activities to present the KERs to relevant groups (early adopters, investors, etc.), once assets are confirmed (outside of Project timeframe)

ATOS: Inclusion in cybersecurity for healthcare portfolios, separate exploitation of tools from the Toolbox, presentation to clients, etc.

XLAB: Establish liaisons and cultivate synergies with related projects, promotion in cybersecurity and health industry fairs, Identify further funding opportunities, market positioning activities including. pitches to targeted customers. The channels will mainly consist in an extended collaboration with the hospital project partners after the project, collaborating with them at their events, shows, social media channels, and websites to promote LOMOS success story.

MARTEL: In case of a valid Unique Value Proposition, has planned activities to present the KERs to relevant groups (early adopters, investors, etc), once assets are confirmed (outside of Project timeframe)

4.7.1 IPR Agreement

At the time of writing this document, the CYLCOMED partners are in the process of signing an IPR Agreement. The purpose of this IPR Agreement is to specify with respect to the Project the IPR ownership of Results that have been developed within the Project and have been selected and prioritized due to its high potential to be "exploited" – meaning to make use and derive benefits, downstream the value chain of a product, process or solution, or act as an important input to policy, further research or education (hereinafter referred to as "KERs").

IPR Ownership

Considering that Results Ownership is governed by the relevant provisions in Section 8 and specifically subsections 8.1 and 8.2 of the Consortium Agreement, as well as article 16 of the Grant Agreement, this document further establishes:

- that "Generation of Results" means that an owner has developed through substantial effort, research, time, and expense, specific Components or Other Materials
- the following table lists the percentage of ownership for Components and Other Materials that make part of KER generated in the Project

KERS	Component	Owner	IPR %
Live anomaly detection system LADS	K-C1	ATOS	100%
Self-sovereign identity solution LUS4MED	K-C2	ATOS	100%
Data Protection solution FE4MED	K-C3	ATOS	100%
Security Dashboard	K-C4	ATOS	100%
Board external to legacy device	K-C5	RGB	100%
Log Monitoring System (LOMOS)	K-C6	XLAB	100%
Open Policy Management	K-C7	MARTEL	100%
Risk Management Tool	K-C8	INOV	100%
Ethical Committee Packet	K-C9	OPBG	100%
Quality Improvement Assessment Packet	K-C9	OPBG	100%

The document is in principle a Memorandum of Understanding that could be used at a later stage when reaching commercial exploitation agreements. Partners have had the opportunity to collaborate in joint efforts during the project but have tried to make a clear line of which developments belong to whom.

At the time of writing this document the IPR document is still being debated . Some clarifications have been done: As per consortium agreement of the Cylcomed project signed by the parties, the results of Cylcomed project are owned by the party that generates them.

Partners OPBG, RGB,XLAB, MARTEL, ATOS and INOV (in the table) expressed their willingness to further valorize the possibility of joining efforts to exploit the above-mentioned KERs (outside the project time frame), in which case it would be evaluated and secured the needed resources; rest of partners agree to give to partners in the table the full right to exploit their owned tools declaring to have nothing to claim.

The parties acknowledge that the project's results do not allow an immediate market perspective and that further cooperation is needed to fully exploit the potential of the cybersecurity tool. The Parties agree to start an open discussion on the intellectual property rights of each contributor once the tool is exploitation ready (TRL7-8).

The OPBG tools in the table are described in more detail; The other tools have been adequately described in the project deliverables:

Ethical Committee Packet – K-C9 OPBG

Pursuant to national and European regulatory frameworks governing biomedical research, including the General Data Protection Regulation (EU) 2016/679 and the Charter of Fundamental Rights of the European Union, the Ethical Committee Packet submitted by Ospedale Pediatrico Bambino Gesù (OPBG) certifies that all research activities involving human subjects, personal health data, and connected medical device deployment under the CYLCOMED project have received full ethical clearance. The documentation includes approvals relating to the study protocol, informed consent, and assent procedures for pediatric participants, data handling safeguards, and oversight mechanisms for artificial intelligence–enabled components. This ethical authorization, granted by the Italian Regional Institutional Review Board (IRB), confirms compliance with the highest standards of research integrity, patient protection, and lawful data processing, and is a prerequisite for commencing project activities at the clinical site.

Quality Improvement Assessment Packet – K-C9 OPBG

The Quality Improvement Assessment Packet includes the qualitative and quantitative validation framework to assess toolbox implementation requirements and standards. Tested and approved in accordance with the internal governance and clinical risk management protocols of Ospedale Pediatrico Bambino Gesù (OPBG), affirms that the CYLCOMED project's proposed implementations have undergone a formal review by the hospital's stakeholders. This evaluation ensures conformity with institutional care standards, clinical pathway integration requirements, and regulatory obligations applicable to the deployment of connected medical devices and cybersecurity interventions in healthcare environments. The completion of this packet provides documented evidence that the CYLCOMED activities meet institutional thresholds for safety, efficacy, and operational readiness, thereby authorizing the initiation of pilot and demonstration activities within hospital facilities in full accordance with applicable national health legislation and international best practices.

5 CYLCOMED Advisory Board

As of this writing, the **CYLCOMED Advisory Board** is composed of four distinguished experts from across Europe, bringing deep knowledge and practical insight into cybersecurity, AI, healthcare, and regulatory landscapes:

- **Juan Carlos Muria-Tarazon**
  University Professor in Applied Research and Knowledge Transfer, AI and Cybersecurity, Polytechnic University of Valencia, Spain
- **Magdalena Mycek**
  Chief Specialist, Department of e-Health, Ministry of Health, Poland
- **Evangelos Markatos**
  Professor of Computer Science, University of Crete, and Head of the Distributed Computing Systems (DCS) Lab at ICS-FORTH, Greece
- **Bernardo Muñoz**
  CEO, Medical Online Technology

Short biographies and exclusive interviews with these board members, highlighting their perspectives on CYLCOMED's key focus areas, are available in the **Advisory Board** section of our website

In the initial phase of the project, the Advisory Board was formed from a group of experts involved during the proposal stage. While their feedback was useful in reviewing early requirements (particularly in **WP3**), the demands of their schedules made ongoing engagement difficult.

Recognising the need for more **responsive and available expertise**, **WP7** decided to restructure the board. Rather than relying on a fixed group, the consortium opted for a **more flexible model** — consulting a range of specialists on specific topics such as:

- Hospital and clinical cybersecurity
- Clinical trials and research ethics
- Regulatory compliance
- Results exploitation
- Healthcare innovation

This shift allowed for targeted input from professionals best suited to each project challenge as it arose.

CONCLUSIONS

From a communications and dissemination standpoint, the CYLCOMED project, which started in December 2022, has since then established a clear brand identity, reflected in both online and offline dissemination and awareness activities. The whole consortium has mobilised to maximise the reach of the project through talks, events, trainings, and workshops, highlighting the multidisciplinary of CYLCOMED. Key communication verged on partners' expertise areas, the legal dimension of CMDs cybersecurity, and insights into the two project's pilots, as well as the toolbox and its components. The project has also continuously strengthened ties with similar European projects, in particular those belonging to the MDCG 2019-16 Cluster. At the time of writing, the website comprises a rich portfolio of presentations, publications, blog articles, and videos. In addition, social media presence has been regular and rich of different content.

The variety of communication and dissemination outputs has contributed to increasing the awareness of CYLCOMED's mission and the communication of its key outputs. It is worth noting that some C&D KPIs have not been met, specifically the number of publications and the number of posters. For the former, a detailed explanation is provided on page 20. As for the scientific posters, these were linked to abstracts and publications. In this case, the consortium members did not consider it necessary to prepare posters and instead opted for presentations and talks, which still ensured effective dissemination.

Regarding standardization tasks, CYLCOMED has equipped partners with essential skills and knowledge through a series of training sessions, enabling effective engagement with standardisation practices while promoting innovation and knowledge valorisation across industries and among tool developers. CYLCOMED was selected for a dedicated consultation under the EU Booster program, an initiative offered by the European Commission. As a result, partners have been cooperating with EU Booster experts in the field, with whom the consortium had very productive interactions. The results are available upon demand. The booster consultancy facilitated contact with the CEN TC251 coordinator for the IEEE 11073 standard. Within the Booster service, CYCLOMED opted for the identification and adaptation of standards that are valuable for the specific methods and tools developed and used by partners. The focus in year 3 has been on learning more about the current development status of the most applicable standards and discussing improvements.

Regarding Exploitation, CYLCOMED has been supported in this task by an expert from the EU exploitation booster service. Joint actions activities included, among others, the identification and assessment of KERs; the description of the Market Definition and Value Proposition Canvas for each asset. An IP agreement has been prepared for signature among partners. There is still a considerable amount of work to be done in the next exploitation stages. This is evident as CYLCOMED targeted a low TRL value. However, in the Annex of this document it can be seen that the steps forwards have been identified, with concrete actions to be carried out in order to reach a joint exploitation of CYLCOMED results in the following years.

REFERENCES

[1] https://intentmarketresearch.com/latest-reports/critical-care-devices-market-8940#:~:text=ICUs%20account%20for%20the%20largest,and%20advanced%20life%2Dsupport%20equipment.

[2] https://intentmarketresearch.com/latest-reports/critical-care-devices-market-8940#:~:text=These%20devices%20are%20crucial%20in,solutions%20in%20critical%20care%20settings.

[3] https://www.grandviewresearch.com/horizon/statistics/telemedicine-market/application/telecardiology/global

[4] https://www.grandviewresearch.com/industry-analysis/digital-health-cardiovascular-market-report

[5] « HSbooster.eu Final Analysys » Final report by EU expert for standardization booster (internal Document) May 2025)

[6] Final report by EU expert for exploitation booster (internal) November 2025

ANNEX

Exploitation Booster

Executive Summary of the Service

This report summarises the process followed and the main outcomes of the Go to Market (G2M) service for the beneficiaries R G B MEDICAL DEVICES SA and the other partners involved in the CYLCOMED project.

It presents the different Modules and sessions carried out during the service delivery along with the agenda of each meeting and the related participants. It then introduces the terminology used, and the one main tool presented and exercised:

- Exploitation Intentions table

It also includes a template for a Memorandum of Understanding, useful for project partners to progress in agreeing on exploitation rights, building on what was signed as the Consortium Agreement (Annex 1); an overview of the overall methodology and approach used during the delivery (Annex 2); as well as general suggestions on financial and non-financial tools to be used along the go-to-market pathway (Annexes 3 and 4).

The Expert was appointed on January 16th, 2025, and the following Modules were included in the G2M service:

- Module A: Kick-off (G2M-A)
- Module B: Unique Value Proposition & Key Exploitable Result(s) (G2M-B)
- Module C: Exploitation Strategy (G2M-C)
- Module D: Business Plan (G2M-D)
- Module E: Access to other funding & entrepreneurship support
- Module F: Reporting (G2M-F)

The Beneficiary was contacted on February 17, 2025.

On Wednesday 19 of March, 2025, an introductory call with the Beneficiary was organised to discuss expectations, get a first insight on the state of the art, present the service and introduce preparatory activities, and agree on a first service delivery plan, based on the Modules activated within the G2M. On the same day, the Expert sent to the Beneficiary all the information and the “Exploitation Intentions” table to be shared with Participants and filled before the delivery of the “Exploitation Pillars Training”.

Then, on April 3, 2025, an additional meeting was held with the aim to prioritise the KERs.

Drafts of the “Exploitation Intentions” tables filled in by Beneficiaries have been returned on April 12, 2025.

The “Exploitation Pillars Training” took place on June 6, 2025, where the basic concepts of exploitation were introduced by the expert, with particular attention to the concepts of KERs, use/adoption of KERs and impact generation. During the session the main discussion was held on the “Exploitation Intentions” table.

During the training, participants and experts aligned on the definitive list of KERs to be supported during the service, which is:

- *Cylcomed Toolbox as KER1*
- *Risk Management Tool as KER2*

Finally, the expert introduced the main tools to be used during the next session: the Market Definition Canvas and Value Proposition Canvas. At the end of the training, the Expert agreed with participants to hold the UVP workshops on July 18. and asked them to fill in the tools presented during the training in order to provide initial comments/suggestions before the UVP workshops.

[2] G2M trainings and workshops
[2] G2M - Module A

Exploitation Pillars training held on June 6, 2025

- **Post workshop support**

Support in fine-tuning available information and provision of final comments, pre and after the workshops

The exploitation intentions tables discussed during the workshop demonstrated significant progress in defining and consolidating the final set of Key Exploitable Results (KERs) related to the CYLCOMED Toolbox and the Risk Management Tool. The following improvements were particularly evident and should continue to be reinforced in the final documentation:

- Each KER now more clearly articulates the key challenges faced by its target users and the specific value of the proposed solution. The CYLCOMED Toolbox effectively addresses the growing need for secure interoperability and simplified certification in connected medical devices, while the Risk Management Tool targets the fragmentation of risk governance processes across healthcare organizations. Further elaboration on the urgency and scale of these challenges, supported by market data and regulatory drivers such as MDR, NIS2, and ISO 81001-5-1, would strengthen the business rationale for exploitation.
- Both KERs are progressively positioning themselves within an increasingly competitive landscape. The CYLCOMED Toolbox highlights its modular architecture and the complementarity of partners' tools as distinctive assets, whereas the Risk Management Tool differentiates itself through framework-agnostic flexibility. A deeper benchmarking exercise comparing features, pricing models, and adoption barriers would better define each KER's unique value proposition and competitive edge.
- Market readiness and time-to-deployment are becoming more explicit. The CYLCOMED Toolbox combines hardware and software components with different TRL levels, offering short-term commercialization opportunities through the Linux Board and longer-term exploitation through advanced cybersecurity modules. The Risk Management Tool, currently at TRL 6–7, is ready for pilot testing and educational use, but requires a clearer roadmap toward full commercialization.
- Both KERs would benefit from defining measurable indicators that demonstrate concrete value for adopters, such as reduced certification effort, accelerated risk detection, improved compliance, or enhanced operational resilience. Establishing such KPIs will be crucial for assessing impact and post-project sustainability.
- The need to distinguish between research-oriented and market-ready elements within each KER is evident. This differentiation will clarify exploitation timelines and facilitate resource prioritization in the upcoming Business Plan phase (Module D).
- Finally, while IP ownership structures are becoming clearer—particularly within the CYLCOMED Toolbox—both KERs should finalize their protection and licensing strategies to ensure coherent and coordinated exploitation across partners.

Overall, the CYLCOMED and INOV exploitation plans are maturing toward a well-structured and market-oriented framework. Continued effort should focus on strengthening market validation, quantifying user benefits, and finalizing IPR and commercialization strategies to support successful deployment and sustainability beyond the project's lifetime.

G2M – Module B

UVP workshop for KER1 held on 29th July 2025

- **Post workshop support**

The tools prepared and discussed during the workshops showed clear progress by the CYLCOMED team:

- **Clarified Value Proposition for KER1 (CYLCOMED Toolbox)**: The Linux Board is now positioned as both an OEM and external module, addressing the need for secure interoperability of connected medical devices and simplifying CE/FDA certification. Each component (LADS, LOMOS, C-OPA, LuS4MED, FE4MED) is linked to measurable outcomes such as reduced certification effort, shorter mean time to detection, and improved audit traceability.
- **Quantification of impact and ROI**: Next step is to develop a one-page ROI calculator for OEMs, quantifying avoided engineering costs, reduced certification iterations, and integration time saved.
- **Strengthened exploitation planning**: A draft exploitation roadmap with defined milestones (specification freeze, CE plan, pilot agreements, OEM LOIs) is in place. Engineering gates (and KPIs (e.g., ≥90% log coverage, MTTD < 5 min) are being established.
- **Market focus emerging_** Target customers and early adopters include 3–5 OEMs (infusion, ventilation) and 3 pilot hospitals (OR/ICU). RGB's existing distributor network (> 20 countries) provides immediate channel leverage.
- **KER2 (Risk Management Tool)**: The tool's positioning as framework-agnostic and multi-party ready was validated. Next steps include UX refinement through pilots with hospital risk teams and CMD manufacturers, and development of "Exec View" analytics for leadership decision-making.

Elements requiring further work (next modules/actions)

- For both KERs, break down the target market by segment (hospital type, OEM category, data readiness) and define a bottom-up TAM/SAM. Confirm ICPs and top-10 target accounts.
- Translate technical benefits into KPIs and ROI statements (time-to-market saved, audit effort reduced, energy and compliance cost avoided). Back these with pilot data and testimonials.
- Compile a one-page competitive grid contrasting CYLCOMED Toolbox and Risk Management Tool with comparable med-tech cybersecurity offerings (SIEM/IAM/NAC suites, OEM gateways, ERM platforms). Use axes such as integration effort, certification readiness, collaboration features, and total cost of ownership.
- Finalise the joint IPR agreement. Clarify ownership of Linux Board vs. software components, pursue the LADS patent, and assess defensive publications for the Risk Management Tool. Prepare a freedom-to-operate (FTO) review for the board and anomaly-detection modules.
- Define three SKUs for the Toolbox (OEM Core, OEM Plus, Hospital Add-On) and SaaS/on-prem tiers for the Risk Management Tool. Publish a price card, SLA templates, and pilot-to-conversion plan.
- Prepare harmonised entries for both KERs, covering problem, solution, TRL/CRL/IRL, quantified benefits, IP status, visuals (architecture + dashboard), and contacts. Reference relevant standards (IEC 62304, IEC 81001-5-1, ISO 14971, IEC 80001-1) and link to the EU Health Data Space context.

G2M – Module C

UVP workshop for KER1 held on 29th July 2025

- **Post workshop support**

The tools prepared and discussed during the workshops showed clear progress by the CYLCOMED team:

- Two complementary exploitation paths have been defined **OEM integration** (Linux Board embedded in new medical devices) and **external add-on** (for legacy CMDs). Both follow a structured deployment flow: **prototype** → **pilot** → **certified OEM integration**, with validation

gates for cybersecurity, safety, and regulatory compliance. ROI reporting and compliance traceability are now embedded in the roadmap.

- The CYLCOMED Toolbox directly addresses MDR/NIS2-driven demand for certified cybersecurity in connected medical devices, offering measurable value in reduced certification effort, accelerated CE/FDA readiness, and improved anomaly detection (MTTD ↓, audit hours ↓). The Risk Management Tool complements this by enabling cross-organisation risk coordination and traceability, supporting ISO 14971 and IEC 81001-5-1 compliance.

Elements requiring further work (next modules/actions)

- Refine segmentation by **device type** (infusion, ventilation, monitoring), **hospital size**, and **data/cyber maturity**. Build a bottoms-up TAM for OEMs and hospitals, and a rolling **Top-10 OEM/hospital accounts list per quarter**.
- Expand benchmarking beyond general "healthcare cybersecurity" to include OEM gateway vendors, hospital IT security suites (SIEM/IAM/NAC), and risk management platforms. Contrast on five axes: **certification readiness, integration effort, policy flexibility, compliance automation,** and **total cost of ownership.**
- Confirm the **open-core strategy** (adapters and connectors open; control plane, AI modules, and board firmware proprietary).
- Formalise cross-partner coordination (RGB, XLAB, ATOS/EVIDEN, MARTEL, INOV) with a **RACI matrix** covering engineering, regulatory, IP, and commercialization roles.

G2M – Module D

Business Plan workshop held on 29th July 2025

- **Post workshop support**

The tools prepared and discussed during the workshops showed clear progress by the CYLCOMED team:

- Priority customer segments have been defined, focusing on **connected medical device manufacturers** (infusion, ventilation, monitoring equipment) **and high-acuity hospital departments** (seeking to strengthen cybersecurity and compliance. Initial Ideal Customer Profiles (ICPs) include OEMs with in-house regulatory teams and 1–2 certified devices, and hospitals with existing cybersecurity or interoperability initiatives. Buyer personas (Regulatory Lead, Clinical Engineer, CISO, QA/Compliance Manager) have been mapped and will guide the next validation interviews.
- YLCOMED provides a **clinically validated, modular cybersecurity toolbox and OEM Linux board** that accelerates CE/FDA compliance and safeguards legacy and new CMDs through explainable AI, policy-based access control, and secure data sharing, **reducing certification effort, audit time, and operational risk** for both hospitals and manufacturers.

Elements to refine in next modules / actions envisaged

- Define how value is captured, including license, subscription, and service revenues across OEM and hospital channels.
- Establish indicative pricing: pilot offer €10–15k (credited on conversion); OEM/hospital subscription €25–40k per site per year; professional services capped at ≤25% of annual contract value.
- If adapters and connectors remain open-core, formalise the **commercial path** for premium offerings (managed edition, paid support, marketplace listing).
- Build a short **go-to-market plan** including buyer persona campaigns, conference targets (health-tech, cybersecurity, med-device), lead conversion metrics, and initial traction milestones (pilots → paid deployments).

G2M – Module E

Future steps workshop held on 30th July 2025

- **Post workshop support**

To make CYLCOMED investable, several key conditions were defined:

Evidence commercial validation: To demonstrate both technical soundness and commercial viability, CYLCOMED must assemble an evidence pack showcasing measurable ROI for adopters.

Security and compliance assurance: Funders and early adopters will expect verifiable security and compliance artefacts. CYLCOMED must provide documentation on edge performance, model drift monitoring, penetration testing, SBOM, and a DPIA template, demonstrating alignment with IEC 81001-5-1, ISO 14971, and MDR cybersecurity requirements.

Repeatable commercial motion: The go-to-market process must be seen as scalable and repeatable. CYLCOMED should prepare a pilot playbook, a partner enablement kit (installation runbook, demo dataset, ROI calculator), and **a rolling list of top-priority OEM and hospital accounts** segmented by sub-domain. This ensures funders can see a structured growth engine rather than isolated pilot efforts.

Financial model and investor readiness: A baseline financial plan should demonstrate break-even at 8–10 active paying sites, gross margins above 70–75%, and cash burn tied to clear milestones (certification, first OEM design-ins, paid pilots).

For private investment (seed/CVC), investors are expected to look for:

- **Traction:** 2–3 paying sites or signed MSAs, pilot-to-production conversion rate ≥40%, and visibility to ~€500k ARR within 6–9 months.
- **Verifiable ROI:** quantified certification and operational savings (e.g. cost/time reduction per device).
- **Economics:** standard price card, capped professional services.
- **Team completeness**.

Defensibility and governance: Investors will require clean IP ownership chains from consortium partners, clear delineation between open-core and proprietary assets, and a structural data advantage (e.g., insights from deployments that enhance threat-detection models).

Funding strategy and capital structure: The reference funding frame is a €1–3M seed round, or an equivalent blended path through the EIC Accelerator or national innovation programs, to reach 8–10 paying customers and operational break-even. Public instruments such as EIC Transition, and EIT Health should be positioned not as substitutes for equity but as de-risking components within the overall financing strategy.

Module D – Business Plan for KER 1 (GTM-D)

1. Executive Summary

CYLCOMED aims to commercialize a device-adjacent cybersecurity toolbox for connected medical devices. The core offering is a Linux-based hardware module and software stack that sits alongside new or legacy devices, enforcing fine-grained access policies, performing AI-driven anomaly detection, providing user-controlled identity and encryption services, and generating audit-ready artefacts (e.g. SBOMs, DPIAs, threat models). The market for connected medical devices is large and growing – forecast to reach USD 152.71 billion by 2030, up from USD 75.99 billion in 2025. Within this, the dedicated medical device security market is expected to grow from USD 8.32 billion in 2025 to USD 15.02 billion by 2032. Rising cyber-attacks (over 300 healthcare data breaches were reported in the first half of 2025, new regulatory mandates, and the explosive growth of networked devices create a timely opportunity for CYLCOMED's solution.

Our mission is to enable safe interoperability for medical devices without forcing manufacturers to rewrite certified firmware**.** We target two primary customer groups: (1) original equipment manufacturers of high-acuity medical devices who need to comply with new FDA and EU cybersecurity requirements, and (2) hospital clinical engineering and cybersecurity teams who must manage fleets of legacy devices. In the first three years, we aim to secure design-in commitments from at least three OEMs, launch paid pilots with three hospital networks, and generate cumulative revenues exceeding €7 million. By year five, we expect recurring revenue from licensing and monitoring services to surpass hardware sales, achieving positive EBITDA and building a global customer base.

With a clear value proposition and early validation in clinical environments, CYLCOMED is positioned to deliver significant value to device manufacturers and healthcare providers. We have assembled an experienced team, established key partnerships, and defined a realistic go-to-market and product development plan to execute on this vision.

2. The Organisation

Company Mission & Vision: Our mission is to *"make every connected medical device safe by design and compliant by default."* The vision is to become Europe's reference provider for device-adjacent security and compliance services in healthcare.

Short-term objectives (2025–2026) include finalizing the industrial design of the CYLCOMED security board, securing CE marking and FDA clearance, and signing "lighthouse" pilot customers. Long-term objectives (2027–2030) include expanding into remote monitoring and home-care applications and building a connector marketplace for additional device protocols and integrations.

3. The Product/Service

The CYLCOMED toolbox is a combination of a device-adjacent hardware module and a suite of software services that together provide comprehensive cybersecurity and compliance for connected medical devices. Importantly, our solution works without altering the device's certified firmware, instead operating as an external security layer. Key components include:

- **Hardware Security Module:** A hardened, low-power Linux-based board that can be embedded into new medical devices or attached externally to legacy devices. It provides secure connectivity (Wi-Fi, BLE, Ethernet), a trusted execution environment, and tamper-resistant storage for cryptographic keys and certificates. This module essentially acts as a security co-processor for the medical device, handling communications and enforcement in a controlled environment.
- **Policy Engine and API Gateway:** A policy enforcement engine (based on Contextual OPA) that externalizes authorization rules for device functions, cryptographic operations, and data access. It enables fine-grained access control and command filtering without requiring changes to the device's own software. Manufacturers or hospitals can define rules (e.g. which user or subsystem can invoke a certain function) in a high-level policy, and the engine ensures the device only operates within those parameters.
- **Anomaly Detection:** AI/ML models that analyze system logs, network traffic, and device telemetry to identify suspicious or abnormal behavior in real time. This includes detecting potential zero-day exploits or misuse (via LADS – Live Anomaly Detection System) and monitoring logs for patterns that indicate faults or intrusions (via LOMOS – Log Monitoring System). These analytics help identify cyber threats or malfunctions early (reducing mean-time-to-detect) and provide alerts to security personnel.
- **Identity and Encryption Services:** A self-sovereign identity module for authenticating clinicians, devices, and even software components, coupled with functional encryption services that allow selective encryption of sensitive health data. For example, certain data fields can be encrypted such that only authorized parties (with the correct keys or attributes) can decrypt them. These services ensure data confidentiality and integrity both at rest and in transit, addressing privacy requirements.

- **Unified Security Dashboard:** A centralized software interface for fleet management, policy authoring, incident response, and audit reporting. Through the dashboard, hospital security teams or OEM support teams can monitor the status of all CYLCOMED-enabled devices, adjust security policies on the fly, review anomaly alerts, and generate compliance reports (such as SBOMs or risk assessment summaries) on demand.

The CYLCOMED toolbox has been prototyped and validated in realistic clinical environments (operating room and intensive care unit scenarios) with pilot partners. These prototypes demonstrated that the hardware board can be integrated with devices like infusion pumps and patient monitors, and that our policy engine and anomaly detection work in live hospital network conditions. The core technology components are at a high Technology Readiness Level but will undergo final industrial design and verification for regulatory approval.

We plan to complete product development and initial certification in the next 6–9 months. Specifically, by Q1 2026 we aim to finalize the hardware design for manufacturability, complete software module testing, and achieve required regulatory compliance (CE marking under EU rules, and FDA clearance in the U.S.). Commercial launch is targeted for Q2 2026 after obtaining these approvals and completing pilot trials. Post-launch, the roadmap includes developing plug-in connectors for additional protocols (e.g. CAN bus in older ventilators, LIN, or proprietary vendor APIs), integration with hospital EHR (Electronic Health Record) systems for seamless data exchange, and a cloud-based analytics service for cross-site security benchmarking. This roadmap ensures that after the MVP launch, we can address a wider range of devices and provide more value (such as aggregated benchmarking of security events across hospitals).

The CYLCOMED solution offers several unique benefits to our customers: it creates a security and compliance layer external to the device, minimizing any changes to legacy systems. This means OEMs can add strong cybersecurity and privacy features to their devices without redesigning or re-certifying existing firmware, significantly reducing the cost and time of compliance. The toolbox is pre-integrated – it combines multiple security functions (identity, encryption, logging, anomaly detection, access control) that would otherwise require separate tools, thus cutting integration effort and ensuring all components work seamlessly together. For hospitals, our module provides centralized visibility and control over a fleet of heterogeneous devices, reducing incident response time (unified logging and anomaly alerts can cut Mean-Time-To-Detect and Mean-Time-To-Respond) and simplifying workflows (e.g. one system to manage policies and updates across many devices). Finally, CYLCOMED automatically produces audit-ready documentation (like SBOMs, threat models, vulnerability assessments), which can shorten security review processes by regulators or hospital procurement – a clear advantage as regulatory scrutiny increases.

4. The Market

Market Size and Growth

Healthcare is undergoing a transformation towards connected care, and the connected medical devices market is growing rapidly. Global market size stood at ~$76 billion in 2025 and is projected to double to ~$152.7 billion by 2030 (14.98% CAGR). This includes devices such as remote patient monitors, smart wearables, implantable sensors, and IoT-enabled diagnostic equipment, all of which require network connectivity and data exchange. Within this broader space, the medical device cybersecurity market is a fast-emerging segment: estimated at $8.3 billion in 2025, it is expected to reach $15 billion+ by 2032 (around 8.8% CAGR). Growth is driven by the proliferation of IoT-enabled medical devices and escalating cyber threats. Notably, North America currently leads in medical device security spending with roughly 37% global market share, but the Asia-Pacific region is the fastest-growing, reflecting a surge of connected device adoption in those markets. This indicates a worldwide demand for solutions like CYLCOMED, with strong initial opportunities in the U.S. and Europe and increasing potential in APAC.

New regulations and guidelines are raising the bar for cybersecurity in healthcare technology, effectively creating a regulatory push for solutions. In the United States, the FDA has significantly updated its requirements for medical device cybersecurity. In June 2025, the FDA issued final guidance that expanded expectations for "cyber devices," including requirements that manufacturers provide a Software Bill of Materials and address known vulnerabilities in premarket submissions. The guidance also promotes the use of Vulnerability Exploitability eXchange (VEX) documents to help regulators and hospitals understand which software vulnerabilities actually affect a device. In practice, this means any new device submission after mid-2025 must demonstrate robust cybersecurity controls and transparency, or risk refusal by the FDA.

In Europe, the Radio Equipment Directivehas introduced mandatory cybersecurity requirements (via Delegated Regulation (EU) 2022/30) for wireless-enabled equipment. These requirements become mandatory from 1 August 2025 for devices with radio connectivity. However, medical devices that fall under the EU Medical Device Regulation or In Vitro Diagnostics Regulation are *exempt* from the RED delegated act, since they are expected to meet cybersecurity requirements through sector-specific standards. In other words, an MRI machine or connected infusion pump is governed by MDR (which includes general safety requirements covering cybersecurity), but if a device is non-medical IoT it must comply with RED's new rules. This regulatory nuance means that medical device manufacturers can either leverage compliance solutions like CYLCOMED to meet MDR's implicit cyber requirements, or if they are outside MDR, they will need to comply with RED directly. Additionally, the EU is moving forward with the Cyber Resilience Act, which in coming years will impose horizontal cybersecurity obligations on connected products (including some medical devices). Countries like Germany are likely to be leaders in enforcing these regulations and demanding compliance. Overall, the evolving regulatory landscape strongly favors solutions that can provide out-of-the-box compliance (e.g. producing SBOMs, enabling secure updates, enforcing access control), which is a core part of CYLCOMED's value.

Our target customers face pressing needs at the intersection of healthcare, technology, and security. OEMs (device manufacturers) need to accelerate time-to-market for new devices while meeting stringent cybersecurity requirements from regulators and customers. They often lack deep cybersecurity expertise in-house, and retrofitting security late in development or after launch is costly. Thus, OEMs are looking for ways to embed security "by design" without starting from scratch, exactly what CYLCOMED's module offers as a plug-in security platform. They also need to provide evidence of security (to regulators, hospital buyers, notified bodies), creating demand for solutions that automatically generate compliance artefacts and documentation. On the other hand, hospital clinical engineering and IT security teams are grappling with managing *heterogeneous fleets* of devices (infusion pumps, ventilators, monitors, etc.) from various vendors, many of which were not built with modern cybersecurity in mind. Their key needs include: visibility into device inventory and network behavior, the ability to isolate or control device functions to prevent misuse, and mechanisms to ensure patient safety isn't compromised by a cyber incident. All of this must be achieved with minimal disruption to clinical workflows. Customers (whether an OEM or a hospital) also increasingly expect that security solutions integrate with their existing systems – for example, a hospital CISO might want alerts from the CYLCOMED system to feed into their central SOC (Security Operations Center) dashboards. In summary, customers want comprehensive security with low integration overhead. Early adopters of a solution like ours include manufacturers of high-acuity devices such as infusion pumps, ventilators, dialysis machines, surgical robots, and the hospitals that deploy these in critical care areas. These stakeholders are actively seeking ways to secure devices that, if compromised, could directly impact patient safety.

Competitive Landscape

The medical device cybersecurity space is nascent but increasingly crowded with both traditional security vendors and specialized startups. Incumbent security companies like Palo Alto Networks, Cisco, and Check Point have started offering healthcare IoT security solutions

(e.g. Palo Alto's acquisition of Zingbox led to its Medical IoT Security product). Companies like Claroty (which acquired Medigate) and Armis focus on agentless network monitoring and asset management for hospitals, giving visibility into all devices on the network. These solutions excel at inventorying devices and detecting known vulnerabilities or anomalous traffic patterns on the network. However, they generally operate at the network layer and often cannot actively control device behavior (they don't sit on the device, so they can't enforce policies on device functions), they also typically require integration with hospital networks or installation of sensors, which can be a heavy lift.

On the OEM side, there are specialist firms like MedCrypt (offering encryption and embedded security libraries for device makers), or Cybeats (focused on SBOM management and supply chain risk) which provide point solutions for manufacturers. These often involve incorporating software into the device firmware or development process. Other competitors in adjacent areas include IoMT security platforms like Ordr and Forescout, which again concentrate on network-level anomaly detection and inventory. Overall, current solutions either protect at the network layer (monitoring traffic, detecting devices) or at the application layer (scanning software for vulnerabilities). *None provide an off-the-shelf, device-adjacent hardware module that wraps around a device to enforce security and compliance.* This is CYLCOMED's differentiator: we implement a "security boundary" adjacent to the device, at the interface between the device and the outside world – with fine-grained policy enforcement at the service call and cryptography level. This approach means we can block unauthorized commands or data flows in real time and insert missing security functions (like encryption or authentication) *without modifying the device's own software*. Our nearest comparables might be certain network micro-segmentation or firewall appliances, but those do not understand device-specific functions or generate device-specific compliance data. To our knowledge, no direct competitor currently offers the same blend of hardware module + integrated compliance tooling targeted at medical OEMs and hospitals.

Barriers to Entry

Entering the connected medical device security market presents significant barriers, which in turn protect well-prepared players like CYLCOMED. Regulatory and domain expertise is a high barrier, any solution touching medical devices must comply with healthcare regulations and cybersecurity standards (IEC 81001-5-1, ISO 14971 risk management, etc.). New entrants face a steep learning curve to build a product that meets these requirements and to navigate certifications. Clinical validation and trust is another barrier: hospitals and OEMs are rightly cautious with new technology that interacts with life-critical devices. Establishing credibility (through clinical pilots, regulatory approvals, and partnerships) is essential and time-consuming. There are also technical integration challenges, medical devices often use proprietary protocols and have real-time constraints, so a deep understanding of biomedical engineering is required to integrate a security solution without impacting device performance. Additionally, scaling a hardware-based solution involves overcoming manufacturing and supply chain hurdles; production of medical-grade hardware requires ISO 13485 processes and quality controls that are non-trivial to set up. Finally, the sales cycle in healthcare is notoriously long and relationship-driven, which favors companies that already have industry connections or footprints. In summary, any new competitor would need significant capital and time to achieve what CYLCOMED (with its consortium roots and head start) has done. These barriers to entry mean that once we establish our product with key reference customers and certifications, it will be difficult for copycats to quickly displace us.

Unique Value Proposition

Amidst these market conditions, CYLCOMED's value proposition stands out clearly: we enable legacy and new medical devices to become secure and compliant by adding an external module, with minimal changes to existing systems. For OEMs, this translates to *faster regulatory approval and faster time-to-market*, instead of spending 1–2 extra years redesigning device software for cybersecurity, a manufacturer can integrate our board and meet FDA/EU

expectations in a fraction of the time. We essentially serve as a “drop-in” cybersecurity solution that provides all necessary controls (authentication, encryption, monitoring) as well as the evidence (SBOMs, vulnerability assessments) for regulatory submissions. Our estimates suggest this could reduce an OEM’s development cycle by many months and avoid potentially millions in costs of delaying product launch (we plan to demonstrate this with cost-of-delay ROI calculators in our sales process). For hospitals, our proposition is unique in that it secures devices from the outside, many hospitals cannot update or patch the devices they own (due to regulatory constraints on firmware), but with CYLCOMED they can overlay security policies and monitoring on top of devices as they are. This means improved safety and compliance for legacy devices that would otherwise remain vulnerable. In short, CYLCOMED accelerates certification and secures legacy devices without firmware changes. We back this up with measurable outcomes (e.g. reduced incident response times, ready-made audit reports, demonstrable compliance with new laws). This unique approach, combined with our team’s regulatory know-how and early mover advantage, forms a compelling value proposition that we will emphasize in all our marketing and sales messaging.

5. The Business Model and Marketing Strategy

CYLCOMED will generate revenue through multiple streams, combining product sales with recurring subscriptions and services to build a robust business model:

- **Hardware Module Sales:** We will sell the CYLCOMED Linux security board to device manufacturers (OEM customers) as a component to be integrated into their new products or to be retrofitted on existing devices. We plan to charge a one-time fee per board. Additionally, for OEM engagements, we will charge a non-recurring engineering or integration fee for the first design-in project to cover customization and support during development. This NRE fee helps offset our engineering costs and deepens the partnership. After initial integration, we will offer volume-based pricing on the hardware for production orders (tiered discounts as the OEM orders thousands of units). For hospital buyers who use the module as an external add-on to legacy devices, the hardware will be sold per unit as a small appliance.
- **Software and Monitoring Subscription:** The core monetization is expected from software licensing. Each deployed module (whether in an OEM device or attached to a hospital’s device) will require an annual subscription to activate the software stack and cloud/dashboard services. This subscription (per device per year) covers use of the policy engine, anomaly detection and AI analytics, identity management, regular security updates, and access to the cloud dashboard and support. For OEMs, this could be structured as an annual license per device sold (revenue-sharing model) or a bundle into their service contracts. For hospitals that directly purchase modules for their old devices, we’ll charge them a subscription for the connected services. Over time, this recurring SaaS-like revenue should grow and provide a high-margin stream that can surpass hardware sales.
- **Professional Services:** We will offer value-added services such as integration support, custom policy authoring, security policy audits, staff training, assistance with compliance documentation (e.g. helping an OEM prepare their FDA cybersecurity filing or a hospital prepare for an IT audit), and incident response support. These services will be monetized through consulting fees or support contracts. We also plan to offer premium support SLAs (Service Level Agreements) for both OEMs and hospitals, ensuring rapid response times and dedicated solutions engineering for those who opt for an enterprise support package.
- **Connector Marketplace:** In the future, we envision an online marketplace for protocol connectors and analytics plugins. As we (or third parties) develop new connectors for additional device protocols or specialized analytics modules, these can be sold or licensed to existing customers to extend the toolbox’s capabilities. For example, if a new plug-in is created to support a particular vendor’s proprietary protocol, other customers can purchase that plug-in. This marketplace could also include advanced

analytics packages (e.g. a module for predictive maintenance analytics on device logs). This creates an ecosystem effect and an additional revenue stream.

Our go-to-market approach will be two-pronged. The primary focus is direct engagement with OEMs, since integrating our solution at the manufacturing stage embeds us into the product value chain. We will employ a direct sales force (leveraging the industry contacts of our CEO and team) to reach mid-to-large medical device manufacturers. We'll emphasize how we can *accelerate their regulatory approval and prevent costly cybersecurity redesigns*, using tools like ROI calculators that show the cost of delayed market entry without our solution. The secondary channel targets hospitals and healthcare delivery organizations for the retrofit use-case. For this, we may partner with medical device distributors or system integrators that already service hospitals. For example, RGB, a partner from our consortium, has a distribution network in Europe that we plan to utilize for reaching hospital clients. We will also explore partnerships with system integrators who manage hospital IT and IoT deployments, enabling them to include CYLCOMED as part of their offering.

To seed the market, we will run an Early Adopter "Lighthouse" Program: select OEMs and hospital sites will receive discounted hardware and premium support in exchange for being reference sites and providing feedback and KPI data. For instance, a hospital in the program might get modules at cost for their ICU devices, in exchange for sharing data on how it reduced their security incident response times, which we can then use in case studies. These lighthouse customers will also be featured in co-marketing (joint press releases, conference talks) to build credibility.

Given our target audiences (medical device executives, clinical engineers, healthcare CISOs), we will employ content-driven and relationship-driven marketing:

- We will participate in major industry conferences such as HIMSS (Healthcare Information and Management Systems Society conference), RSA Healthcare, and MEDICA (the global med-tech trade fair in Germany), where we can demonstrate our solution and network with both providers and manufacturers.
- We plan to publish white papers and thought leadership articles on topics like compliance with the new EU Radio Equipment Directive or FDA cybersecurity guidelines, positioning CYLCOMED as an expert in medical device cybersecurity and a solution to upcoming regulatory challenges. These will be distributed online and via industry forums.
- Webinars and workshops will be organized for hospital clinical engineering teams on how to secure legacy devices, ideally in partnership with healthcare cybersecurity associations or using our pilot hospital experiences.
- We will seek media coverage and case studies by collaborating with our pilot customers: e.g. a joint press release with a hospital that implemented CYLCOMED highlighting improved security metrics, or a success story with an OEM who rapidly got FDA approval for a device using our toolbox.

Market Segmentation and Positioning: Initially, we are focusing on high-acuity medical devices, those used in critical care (OR, ICU) where both the risks and regulatory pressures are highest (e.g. a hacked infusion pump in an ICU could be life-threatening, and thus hospitals and regulators are very sensitive about their security). Devices like infusion pumps, patient monitors, ventilators, dialysis machines, etc., are an ideal starting point. These are also devices that often need to interoperate (e.g. pump sending data to monitoring systems), a key use-case for our toolbox. Geographically, our initial focus is Europe (especially Germany, Italy, France), where our team has experience and where the MDR provides a strong impetus for cybersecurity (and where domestic manufacturers are abundant). Germany in particular, with its large med-tech sector and stringent BSI (Federal Office for Information Security) guidelines for healthcare, is a prime early market. Italy and France also have sizable hospital networks and local manufacturers that we can approach (and Italy is our home base). After establishing in Europe, we plan to expand to North America (US & Canada), aligning with the timeline when the FDA's new guidance and potentially new legislation (PATCH Act enforcement, etc.) make

cybersecurity a must-have for all devices entering the US market. Our positioning is centered on being the *fastest and most comprehensive path to compliance and security* for connected medical devices. In all messaging, we will emphasize how CYLCOMED *"wraps around" devices to instantly upgrade their security*, effectively future-proofing devices against evolving threats and rules. This positioning is unique compared to competitors who either monitor passively or secure only new devices; we will be *"the solution for the 15-year-old device in your hospital basement as well as your next-gen smart device in development."* By highlighting our ability to accelerate certification and secure legacy devices without firmware changes, we tap into two urgent pain points and differentiate ourselves.

6. The Team and Management Structure

Key Team Members and Roles: CYLCOMED's leadership team brings together expertise in med-tech, cybersecurity, and regulatory compliance, reflecting the interdisciplinary challenges of our business:

- **Chief Executive Officer (CEO):** An experienced med-tech business development professional who oversees company strategy, fundraising, and partnerships. The CEO's background includes leadership roles in healthcare technology firms and a track record of bringing medical innovations to market. They will drive investor relations and strategic partnerships (e.g. OEM alliances) and ensure the company stays aligned with market needs.
- **Chief Technology Officer (CTO):** Responsible for the overall product architecture, including hardware design and software stack integration. The CTO has deep experience in embedded systems engineering and cybersecurity, likely having led development of secure devices or IoT products in the past. Under the CTO's guidance, the engineering team will ensure the CYLCOMED board and software meet performance, safety, and security requirements.
- **Regulatory & Quality Lead:** This person manages our compliance with medical device regulations (CE marking process, FDA submission preparations) and heads the Quality Management System (ISO 13485 processes, documentation). With extensive experience in standards like IEC 62304 (medical software lifecycle), IEC 81001-5-1 (health software cybersecurity), and ISO 14971 (risk management), they ensure our product and processes satisfy all regulatory expectations. They coordinate closely with external test labs and notified bodies, and maintain our technical files and clinical evaluation reports.
- **Product Manager:** Acts as a bridge between the technical team and the customers. The product manager engages with OEM partners and hospital users to define requirements, prioritize the roadmap, and identify new use cases. They also coordinate pilot deployments (making sure the engineering team supports the pilots and that feedback is collected systematically). This role is crucial for ensuring we build a product that truly fits into clinical workflows and OEM development cycles.
- **Chief Information Security Officer (CISO):** Overseeing internal and product security, the CISO drives threat modeling, penetration testing, and vulnerability response for the CYLCOMED solution. They establish our security assurance program (so that our product is secure-by-design) and will interface with hospital CISOs and OEM security teams during evaluations. The CISO also ensures we practice what we preach in terms of cybersecurity (secure cloud, development practices, etc.), reinforcing trust with customers.
- **Sales and Marketing Lead:** Leading the go-to-market execution, this role handles marketing campaigns, product positioning, and manages the pipeline of prospects. They run the Lighthouse early adopter program, nurturing those key accounts, and also develop channel partnerships (for example, managing the relationship with RGB or any distributor). As we scale, this person would build a sales team (including perhaps regional sales reps or clinical solution specialists) and a marketing team to expand outreach.

CYLCOMED will maintain a lean and agile management structure. Weekly executive team meetings will review progress against goals, and each executive has clear domains but we encourage cross-functional decision making (for instance, the CTO, Product Manager, and Regulatory Lead will jointly review whether a new feature is ready for release from both a tech and compliance perspective). We employ a RACI (Responsible, Accountable, Consulted, Informed) matrix for major projects to ensure clarity in execution responsibilities. Strategic decisions (major investments, pivots, key hires) are made in consultation with the Board of Directors, which meets formally each quarter. The Board comprises the founders and representatives from major investors or stakeholders. We are conscious of balancing speed (as a startup we need to move fast) with the rigour required in healthcare (where quality and safety are paramount), so our governance model emphasizes accountability and quality controls even as we iterate quickly on development.

The team's origin in an EU consortium provides a built-in network of partners that we will continue to leverage. For example, RGB, our consortium partner specialized in medical device production and distribution, is a strategic ally, they act as a lead commercial partner in Europe, helping with manufacturing scale-up and providing sales channels in certain markets. We also maintain relationships with the research institutions and universities from the project, which can be engaged for joint R&D or accessing talent (internships, etc.). On the deployment side, our partnerships with pilot hospitals and OEMs are not just customer relationships but collaborative partnerships – their input shapes our product, and in turn we help them solve pressing problems. These early alliances will likely convert into long-term commercial contracts, and possibly even co-development of new features. As part of our growth strategy, we may also seek partnerships with large healthcare IT firms or cybersecurity providers to integrate CYLCOMED's capabilities into broader solutions (for instance, partnering with an EHR vendor to integrate our identity management into their single sign-on). Overall, the team and partnership structure is designed to maximize reach and credibility despite our startup size, by tapping into established networks.

7. The Operative Plan

Our operational plan lays out how we will execute on development, regulatory approval, manufacturing, and deployment over the next few years. Key milestones and activities include:

- **2025 – Q1 2026: Product Finalization.** In this phase, we complete the industrial design and engineering of the CYLCOMED hardware board (moving from the prototype PCB to a production-ready design, including enclosures if needed for external modules). Simultaneously, we finalize all software components – ensuring the policy engine, anomaly detection (LADS/LOMOS), identity management, etc., are integration-tested and verified. We will conduct internal conformity assessments against relevant standards: for example, verifying software development processes and outputs comply with IEC 62304 (medical software lifecycle), verifying cybersecurity risk management per IEC 81001-5-1 and ISO 14971, and creating the required documentation (risk management file, test reports). We will also prepare the first complete set of SBOMs and VEX reports for our solution, since the FDA now expects those in submissions. By Q1 2026, we plan to submit our regulatory filings, a CE technical dossier to our Notified Body in Europe and a 510(k) or De Novo submission to the FDA in the US (depending on classification), incorporating the latest FDA guidance on cybersecurity. Achieving these submissions will be a critical milestone signaling that our product meets safety and cybersecurity requirements.
- **Q2 – Q3 2026: Pilot Deployment.** Upon (or while awaiting) regulatory clearance, we will initiate pilot deployments with our early adopters. The plan is to deliver first batches of boards to three OEM partners (for integration into their development devices or limited market release products) and to install external CYLCOMED modules on devices in three "lighthouse" hospital sites. During this pilot period, we will closely monitor performance and gather key performance indicators: for instance, *Mean Time To Detect (MTTD)* and *Mean Time To Respond (MTTR)* to security incidents in those

hospitals (comparing before vs. after CYLCOMED), number of security policy enforcement actions (e.g. blocked unauthorized access attempts) on devices, and reduction in audit preparation time for hospital IT (since our system provides reports). We will iterate on both hardware and software based on pilot feedback, for example, if an OEM finds they need a different form-factor board or a hospital needs a new dashboard feature, we can adjust before full commercial launch. This phase will prove out our manufacturing logistics on a small scale and help refine user documentation and training materials.

- **Q4 2026: Commercial Launch.** With pilots validating the solution and (expected) regulatory approvals in hand, we will transition to full commercial launch. This involves ramping up manufacturing via contract electronics manufacturers (we plan to partner with an ISO 13485-certified electronics manufacturing service to produce the boards at scale). We will also formalize a distribution agreement with RGB (our partner) or similar distributors in target regions, ensuring we have channels to deliver and support the product in multiple countries. By Q4 2026, we aim to release version 1.0 of the CYLCOMED Dashboard and Connector Marketplace to the general market, this means our cloud services are robust, billing/subscription systems in place, and initial additional connectors available for customers. Internally, this quarter will also see the build-out of customer support and field engineering functions to handle new customer onboarding beyond the pilots.
- **2027 – 2028: Scale-Up.** In the subsequent two years, the focus is on scaling sales and broadening the product capabilities. We plan to onboard additional OEMs beyond the initial three, leveraging the success stories from pilots to sign new design-in agreements. The product will expand into remote patient monitoring and home-care devices (which is a growing segment as healthcare extends out of hospitals). We will develop connectors for major vendor protocols (for example, if a large device maker has a custom protocol, we create a module for it, or connectors to standard health IoT protocols). Integration with hospital enterprise systems, such as Electronic Health Records or Security Information and Event Management systems, will be developed to ensure our product meshes well in the hospital IT ecosystem. Another goal for this period is to launch a cloud-based analytics platform that aggregates anonymized security data from all our deployed sites (with customer consent) to offer cross-site benchmarking, for instance, allowing a hospital to know how its security incident rate compares to peers, or an OEM to see trends across all their devices. Operationally, by 2027 we will also evaluate entering the North American market fully, which may involve setting up a U.S. subsidiary or partnerships for distribution/support.

Internal vs. External Activities: We strategically decide what to keep in-house versus outsource. Our core intellectual property, security policy engine, anomaly detection models, etc., is developed in-house by our R&D team. We will also keep the critical system architecture and integration know-how internal. However, certain activities are more efficient to outsource: manufacturing (as mentioned) to experienced partners; some testing can be done by specialized labs (for example, independent penetration testing or electromagnetic compatibility testing for CE certification). We also utilize external legal consultants for regulatory filings in various jurisdictions to ensure compliance. Our approach to R&D remains collaborative: we will continue research collaborations with universities and possibly EU research grants to stay at the cutting edge (e.g. exploring AI in cybersecurity or new encryption techniques). This allows us to tap external innovation while focusing our internal team on product development and delivery.

The operative plan requires specific investments at different stages. In 2025–2026, spending on product development and certification is heaviest, this includes hiring engineers, paying for certification lab fees and clinical evaluations, setting up the cloud infrastructure, and manufacturing the pilot batch. As we shift to deployment, investment goes into manufacturing setup (tooling, initial component inventory) and customer support capabilities. We also allocate budget for the lighthouse pilot program (essentially marketing expense in the form of

discounted hardware and on-site support). Throughout, we maintain focus on efficient resource management: given our funding (detailed in Section 9), we operate with lean principles, but we ensure critical path tasks (like certification submissions) are well-resourced to avoid delays.

Progress against this operative plan will be monitored via milestones and KPIs at each stage.

8. Financials

We have developed three-year financial projections (2026–2028) based on a conservative market uptake scenario. All figures are in Euros (€) and reflect the expected ramp-up from pilot stage to early commercial growth. Key assumptions include moderate OEM adoption (a few major deals by Year 3) and steady growth in hospital retrofits.

- **Year 1 (2026):** We project revenue of approximately €2 million. This is composed of about 1,000 CYLCOMED boards sold (either to OEMs or for pilot deployments) at an average selling price (ASP) of ~€1,000 each, totaling ~€1.0M in hardware revenue, plus about €1.0M in services and software subscriptions (early subscription fees, and any paid integration services with pilot customers). Operating expenses in Year 1 are estimated at €4 million, reflecting heavy R&D costs, certification expenses, pilot program support, as well as initial marketing and business development spend. We anticipate an EBITDA of around –€2 million (a loss) in the first year, which is expected for an R&D-heavy startup. Cash flow will be negative in Year 1; however, this is financed by existing grants and seed capital (from the Horizon Europe project and initial investors), meaning we have the funds allocated to cover this planned burn.
- **Year 2 (2027):** Projected revenue is around €5 million. This assumes scaling to ~3,000 boards sold, with an ASP slightly lower (~€900) as volume increases and we possibly offer OEM volume discounts, yielding ~€2.7M from hardware. Additionally, recurring subscription and service revenue grows to about €2.3M (as the devices sold in Year 1 contribute a full year of subscriptions in Year 2, plus new ones coming online). Operating expenses are expected to be about €6 million, as we scale up operations: higher manufacturing costs, growing the team (sales, support, U.S. expansion groundwork), and continued R&D for new features. EBITDA in Year 2 is approximately –€1 million, still a net operating loss. The loss narrows compared to Year 1, but we do not expect to be break-even yet due to deliberate reinvestment in scaling the business (building inventory, entering new markets). The cash flow gap in Year 2 will be covered by the funding raised (as described in the Resources section) – essentially, we invest ahead of revenue to capture market and will burn some of the investment capital.
- **Year 3 (2028):** Projected revenue jumps to about €10 million. This is driven by more significant OEM deals and hospital uptake: we estimate roughly 6,000 boards shipped this year (the ASP may further drop to ~€800 with higher volumes, contributing ~€4.8M hardware revenue), and a substantial increase in subscription/services to ~€5.0M. By Year 3, the cumulative number of devices in the field paying subscriptions yields a solid base of recurring revenue. Operating expenses are projected at €8 million, as the organization reaches a steady state of operations – we'll have larger support and sales teams by this point, and potentially offices in multiple regions, but also efficiencies of scale in production. EBITDA is forecast at around €2 million (positive). This implies we achieve break-even during Year 3, likely mid-year, and become profitable on an EBITDA basis by the end of 2028. At this point, the cash flow turns positive, which gives us the ability to reinvest from our own revenues into further growth (such as developing the connectors marketplace and pursuing expansion into the US and Asia without solely relying on external funding).

These projections are based on conservative uptake, for instance, we assume only a handful of OEMs on board by Year 3 and a limited rollout in hospitals (perhaps 10–30 hospital networks adopting in some capacity by then). We deliberately did not assume any blockbuster deal or exponential growth yet, given the long sales cycles. If we perform better (e.g. secure a big OEM partnership earlier), these numbers could be higher. We also assume a gradual decrease

in hardware ASP, as typically happens with volume and as hardware costs potentially drop; however, we also expect to improve gross margin on hardware through manufacturing efficiency. On the expense side, a large portion is staff costs (growing from ~15 FTEs in Year 1 to ~30+ FTEs by Year 3) and ongoing R&D (we continue roughly 15–20% of spend in R&D even in Year 3 to stay ahead on product). Marketing and sales expense grows to about 25% of revenue by Year 3 as we expand go-to-market efforts. We assume no major debt servicing costs in these projections since the plan is to use equity/grant funding.

By Year 3 the business becomes self-sustaining. Gross margins are expected to be healthy, on hardware, initially modest (maybe 30-40% for low volumes) but improving to 50%+ with scale; on software subscriptions, margins are very high (80%+) as those are largely software/cloud costs. Overall, we target a gross margin above 50% by Year 3. We will monitor Customer Acquisition Cost relative to Customer Lifetime Value (LTV); our goal is a CAC of <15% of LTV, ensuring our sales and marketing spend is efficient. We expect Annual Recurring Revenue growth to exceed 50% year-on-year in the early years, reflecting the compounding effect of subscriptions. The balance sheet at the end of Year 3 is anticipated to show a healthy cash position (assuming we raise the planned funds, there should be a buffer left by Year 3 given we start generating cash) and limited liabilities (perhaps some working capital financing for inventory if needed). We do not anticipate long-term debt in the first 3 years aside from possible venture debt for inventory which would be small relative to equity.

The financial plan will be continuously refined as we gather real data from pilots and early sales – we will maintain a lean approach, ensuring that we can adjust expenditures if revenues fall short, and conversely ready to accelerate growth investments if product-market fit proves very strong.

9. The Resources

To achieve our objectives, we have mapped out an investment plan that details the funding needed, the timing of its use, and potential sources. Over the next three years, we seek approximately €5 million in additional funding (on top of existing grants/seed money) to execute this business plan.

The €5M will be allocated strategically to cover key areas:

- **~40% (about €2.0M) for Product Development and Certification:** This includes completing R&D, paying for certification processes (regulatory consulting, lab testing, clinical validation studies), and expanding the development team as needed for product readiness. It also covers building the secure cloud infrastructure and tooling for SBOM generation, etc. Early-stage technical efforts and regulatory submissions are resource-intensive, hence the largest share here.
- **~25% (about €1.25M) for Manufacturing Setup and Inventory:** These funds go toward setting up the supply chain and initial production. For example, investing in tooling or NRE with our contract manufacturer, purchasing initial component stock in bulk (to mitigate lead times and negotiate better prices), and setting up quality assurance systems. It also includes logistics setup (packaging, fulfillment) as we start delivering units.
- **~25% (about €1.25M) for Sales, Marketing and Pilot programs:** This covers the costs to acquire and support customers. It includes marketing campaign costs, conference exhibitions, travel for sales to meet OEMs, and running the Lighthouse pilot program (which may involve sending engineers on-site, providing free/discounted hardware, and co-marketing expenses). We consider this an important investment to seed the market and build our brand.
- **~10% (about €0.5M) for Working Capital:** This reserve ensures we can manage cash flow timing differences – e.g., manufacturing might require upfront cash to buy components months before we get paid by customers. It also provides a buffer for any unexpected costs or delays. Essentially, it's for day-to-day operational liquidity (inventory, receivables, and a cushion for safety).

We plan a mix of funding sources to meet this €5M need, balancing non-dilutive and dilutive capital:

- **Horizon Europe / Public Grants:** We will pursue follow-on EU funding (for example, EIC Transition or other Horizon programs that support bringing research to market). These grants can provide several hundred thousand euros up to low millions, and we have a good position to win them given our Horizon project background. National innovation grants (e.g., cybersecurity or med-tech grants in Italy or the EU Digital Europe program) are also on our radar.
- **Venture Capital (Equity Investment):** We anticipate raising venture capital from investors who specialize in med-tech or deep tech. Likely, we would do a Seed/Series A round to raise a significant portion of the €5M (since grants alone likely won't cover it all). We will target VCs with healthcare and IoT cybersecurity focus. This injection not only provides capital but also connections and guidance. We already have interest from some investors (one sits as an advisor) which is promising.
- **Strategic Partners (Corporate Investment):** It's possible that an OEM or a healthcare technology company might invest in CYLCOMED as a strategic move. We are open to strategic partnerships where, for example, a large device manufacturer or a hospital network invests funds in exchange for an equity stake or exclusive access in some domain. This can bring smart money and early customers in one go.
- **Debt/Loans:** We will explore venture debt or loans for specific needs like hardware inventory or working capital once we have customer orders in hand. For instance, an Italian Innovation Fund-backed loan could provide low-interest capital for manufacturing once we show firm contracts. We likely won't rely on debt for R&D, but for scaling production or bridging cash flow, it could be useful (and keeps equity dilution lower).

Funding Timeline: We intend to draw down the investment in tranches tied to milestones. This not only instills confidence in investors (funds are deployed when certain goals are met) but also ensures we don't take on more capital than needed at any point (minimizing dilution). The planned tranches are:

- **Tranche 1 (Q1 2026):** Released upon completion of CE/FDA submission. This is a critical de-risking milestone (it shows we have a product ready for approval). Funds from this tranche will primarily fuel pilot deployments and manufacturing setup.
- **Tranche 2 (Q3 2026):** Upon conclusion of successful pilot deployments (e.g., we have referenceable results from pilots and maybe initial LOIs from those customers). At this stage, funds are used for scaling go-to-market (hiring sales, building inventory for launch).
- **Tranche 3 (Q4 2026):** Upon commercial launch and first orders. This final tranche can support scaling production and possibly initial expansion to new markets.

By structuring the raise this way, if any milestone is delayed, we adjust spending accordingly. Also, it provides clear checkpoints for investors to see progress.

We aim to balance equity and non-dilutive funding to retain control and upside. Ideally, grants and loans can cover a substantial part of needs so that the equity we issue is minimized. Any equity raised will of course dilute existing owners, but we intend to keep enough ownership among the founding team and consortium so that strategic direction remains with us (no single outside investor should command a majority or force us off mission). We anticipate perhaps a single round of VC in the €2–3M range and the rest from grants to reach €5M. Should more capital be offered or needed (if opportunities to scale faster arise), we will carefully evaluate against the value it unlocks.

Final recommendations by the Expert

Issues	KER1 — AI Toolkit (Food Manufacturing)	KER2 — Green Deal Index (GDI)
Asssessment and Recommendations		
Maturity of the KER	Where you are: TRL 6→7; pilots done; certification and hardening ahead. Readiness: CRL 3–4, IRL 3–4. Next: finish DVT→PVT, submit CE/FDA, ship an OEM reference kit.	Where we are: TRL 5–6; pilots starting; core workflows ready. Readiness: CRL 2–3, IRL 2–3. Next: add SSO/RBAC and audit export, prove 2 paid pilots with adoption KPIs.
Market definition	Customers: ICU/OR device OEMs and hospital clinical engineering/CISOs. Competitors: IoMT network monitors, GRC/ERM tools, bespoke gateways. Tighten: name 10 OEMs + 10 hospital groups, build a bottom-up TAM, publish a 1-page battlecard.	Customers: hospital risk/quality teams and OEM RA/QA. Competitors: spreadsheets, generic ERM, single-framework tools. Tighten: two buyer plays (hospital vs OEM), procurement-ready checklist, clear outcomes (cadence, time-to-mitigation, closure rate).
Unique Value Proposition definition	One line: “Secure legacy and new devices and speed CE/FDA without firmware changes.” Proof: show MTTD/MTTR improvement, % of device requests governed, audit time saved.	One line: “Framework-agnostic risk workspace that raises review cadence and speeds mitigation.” Proof: before/after cadence charts, exec dashboard, method transparency.
IPR/Intellectual assets management	Status: hardware design + policy/analytics code + compliance tooling. Do next: background IP register, contributor agreements, trademarks, select patent filings (enforcement patterns, update chain), defensive publications.	Status: software + method + evidence schemas. Do next: trademark/name, contributor and data licences, publish mapping change-log, consider defensive publication for cross-org evidence flow.
Use/business model	Charge: board sales + annual subscription per 100 devices + first-integration NRE; fixed-fee services; premium SLAs. Packages: OEM Core, OEM Plus, Hospital Add-On, Enterprise. Do next: publish price card and ROI calculator.	Charge: subscription by workspace + external collaborator seats; onboarding/connector bundles; premium support. Packages: Essentials, Collaboration, Enterprise. Do next: price card + 90-day pilot offer with conversion credit.

Exploitation Risks	Main risks: hard integration, parts shortages, security findings, data-sharing delays. Mitigate: reference kit, dual-source BOM + ISO 13485 partner, vuln SLAs + pentests, signed pilot DPAs and access rules before shipping.	Main risks: “stickiness” of spreadsheets, legal friction, missing connectors, weak value proof. Mitigate: activation playbook + import wizard, standard DPA/ToS, connector roadmap with SLAs, exec view tied to cadence/closure KPIs.
Planning of next steps	90 days: DVT complete, golden-path demo, 2 signed pilot charters (with KPIs), compliance matrix + SBOM/VEX samples. 180 days: PVT run, CE/FDA submitted, 2 pilot conversions, 1 OEM design-in LOI, distributor kit ready.	90 days: SSO/RBAC + audit export, 2 signed pilot charters (hospital + OEM) with activation KPIs, import wizard v1. 180 days: 2 paid pilots live, first connectors (Jira/ServiceNow + file store), adoption dashboard, 5 named champions.
Financial plan (revenues/costs)	Shape: hardware + ARR + services; aim for blended gross margin 50–60% by Y3. Improve: show bookings vs billings vs ARR, attach-rate model per OEM family, COGS/yield and inventory buffer plan.	Shape: ARR-led; services ≤25% of ACV; margin target 70–80%. Improve: base/VC/stretch scenarios, seat economics, pilot→paid payback, NRR target >110%.
Team	Now: strong R&D/regulatory. Gaps: OEM Technical Account Manager, Compliance/Quality Engineer, Customer Success Lead. Actions: hire TAM now; add compliance engineer; set up clinical/reg advisory panel.	Now: product/engineering core in place. Gaps: Head of Customer Success, Solutions Engineer, Product Marketing, Security Officer. Actions: hire CS lead; add hospital + OEM advisors with buyer clout.
Funding opportunities	Best fits: EIC Transition (use Horizon results), DIGITAL Europe hospital-cyber deployments, EIC Accelerator after paid traction, Smart&Start + SIMEST (Italy), EIT Health for validation.	Best fits: DIGITAL Europe (deploy and skills), Horizon Europe Cluster 3/4 cyber topics, EIT Health Bridgehead/THI, Eurostars for SME R&D.
Creation of startup/spinoff	Advice: proceed with a focused spin-out. Model: open-core adapters, proprietary control plane. Do: shareholder agreement, IP assignment, 10–15% ESOP, clear partner commercial terms.	Advice: start inside the CYLCOMED vehicle to share GTM; consider spin-out when ARR > €1M or a distinct buyer segment emerges. Keep strong data ownership and tenant isolation.
Further support	Needs: independent security audit, ISO 13485 manufacturing	Needs: legal review of claims/liability, DPIA templates, procurement packs,

	partner, pricing workshop, SI partner kit, EIC/EIB coaching.	analyst briefings, auditor/consultancy partner program.
[other elements]	Security and sales: MTTD/MTTR delta, % device requests governed, audit-hours saved, OEM design-ins per family, yield and lead-time SLA.	Adoption and value: time-to-first-risk, weekly active seats, on-time tasks, review cadence, pilot→paid conversion, export completeness and auditor acceptance.