

European Projects Insight Report

10 June 2025



5 European Projects in Focus: CYLCOMED, EDiHTA, ENTRUST, FLUTE, Gravitate-Health, IDERHA, MedSecurance, NEMECYS, ONCOVALUE, SHAIPEd, TRUMPET, and XiA

The following section highlights twelve EU-funded projects that exemplify the diversity, ambition, and strategic relevance of European digital health research and innovation. Each initiative addresses critical dimensions of system transformation—from cybersecurity and AI governance to citizen empowerment, interoperability, and digital skills development—while contributing validated tools, stakeholder engagement models, and policy-aligned frameworks.

Together, they reflect the collective potential of European projects to strengthen the foundations of a trusted, inclusive, and interoperable digital health ecosystem.

Additional project details—including consortia composition, technical strategies, and progress updates—are provided in Appendix of this Insight Report. All information has been provided directly by the project consortia representatives.

CYLCOMED

CYLCOMED (Cyber securitY toolLbox for COnnected MEdical Devices), a 36-month Horizon Europe RIA (1 Dec 2022- 30 Nov 2025), aims to boost the cybersecurity of connected medical devices, in vitro diagnostic and software as medical devices (CMDs, IVDs, SaMD). It provides training, tools, and risk guidance, addressing human factors and data protection.

CYLCOMED is an EU-funded project seeking to enhance the cybersecurity of connected, in vitro diagnostic and software as medical devices (CMDs, IVDs, SaMD), maintaining their performance and safety for patients and preserving or enhancing the confidentiality, integrity and availability of the private data they exchange.

Key Areas: Cybersecurity of Connected Medical Devices (CMDs), Technical Cybersecurity Solutions, Compliance & Regulatory Alignment, Training & Capacity Building, Stakeholder Engagement & Multi-disciplinary Collaboration.

8 Appendix: Detailed Information About European Projects

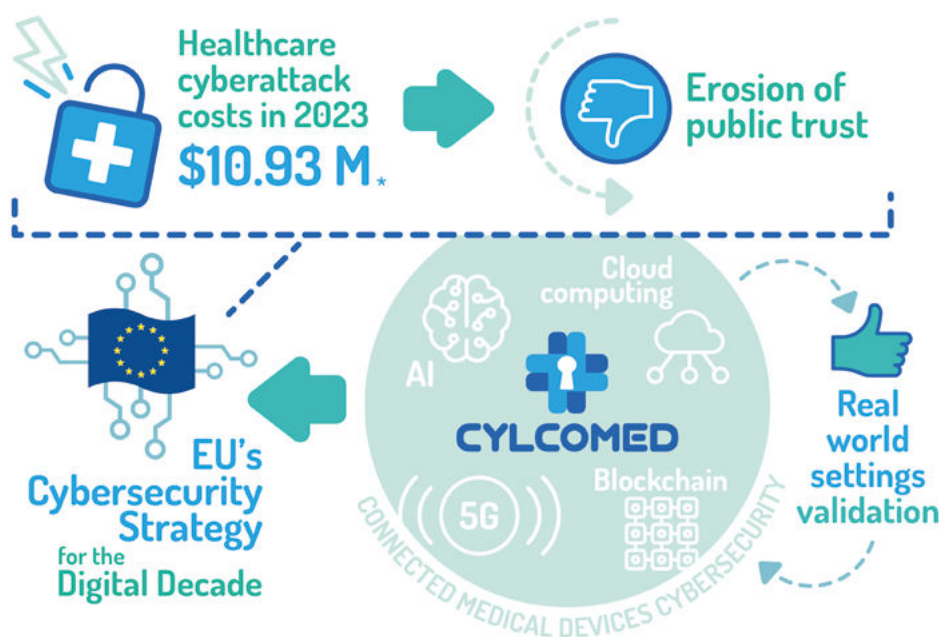
CYLCOMED



CYLCOMED: Strengthening Cybersecurity for Connected Medical Devices in Europe's Digital Future

The following project summary has been provided by the CYLCOMED consortium and reflects their own description of the initiative's goals, activities, and results.

As healthcare systems across Europe accelerate their digital transformation, connected medical devices (CMDs), in vitro diagnostics (IVDs), and software as medical devices (SaMDs) are becoming integral to patient care. However, this increased interconnectivity exposes critical vulnerabilities, making cybersecurity a growing concern.



* Source: World Economic Forum

Securing Europe's Digital Healthcare

CYLCOMED's urgency is underscored by the rising frequency and impact of cyberattacks on healthcare institutions, which can result in operational disruptions, data loss, patient harm, and eroded public trust. According to the World Economic Forum, healthcare experienced average data breach costs in 2023 at \$10.93 million—nearly double that of the financial sector.



CYLCOMED aims to strengthen CMDs cybersecurity through targeted updates to EU regulatory guidance (e.g., MDCG 2019-16) and by developing risk management methodologies and practical tools. The project supports secure-by-design principles in CMDs development, integrating novel technologies such as AI, cloud computing, 5G, and blockchain. Tools are validated in real-world settings, ensuring they are robust, interoperable, and regulation-compliant.

Mission-driven Innovation Aligned with Europe's Cyber Agenda

CYLCOMED's long-term ambition is to foster AI-driven, healthcare-specific security ecosystems that move beyond generic rule-based solutions. CYLCOMED envisions secure, automated CMDs management across hospitals, including legacy systems, enabling cross-border data exchange and resilient care delivery through decentralised identity tools. Aligned with EU efforts such as the Cybersecurity Strategy for the Digital Decade, the European Health Data Space (EHDS), and regulatory frameworks like the AI Act and MDR, CYLCOMED contributes directly to enhancing the cybersecurity of healthcare infrastructures.

Advanced Technologies for Safer Healthcare and Use Cases

CYLCOMED leverages containerisation (Docker) to standardise deployment and simplify inter-component communication, secure updates and remote management (Mender), and advanced encryption (FE4MED) to secure data communication and storage. AI-powered tools like LOMOS (Log monitoring system) and LADS (live anomaly detection system) provide real-time threat detection and proactive security postures. These methodologies support compliance with ISO and MDCG standards, enhancing the overall security framework for CMDs.

A key use case involves Spanish partner RGB Medical Devices' multi-parameter monitoring device, which, when used in intensive care settings, automates drug dosage via an infusion pump based on real-time relaxation level analysis. To integrate advanced cybersecurity features, the system uses a Raspberry Pi 4 mini-computer as a secure intermediary between the device and cloud-based Hospital Information Systems (HIS). This setup ensures encrypted data transmission, overcomes legacy hardware limitations, and protects sensitive patient data by enabling authorised-only access and maintaining operational compatibility in clinical environments.

In a second deployment, Italian partner Ospedale Pediatrico Bambino Gesù is validating the CYLCOMED cybersecurity toolbox in real-world telemedicine scenarios, through a clinical trial involving 16 patients. As part of Deployment A of Pilot 2, this use case involves cardiological patients enrolled in a clinical trial using wearable devices for remote monitoring. The trial leverages the MediaClinics Health Platform (MHP) to collect data from devices via a backend server hosted within the hospital, equipped with AI-driven cybersecurity tools, including continuous log monitoring, real-time anomaly detection, and risk assessment.

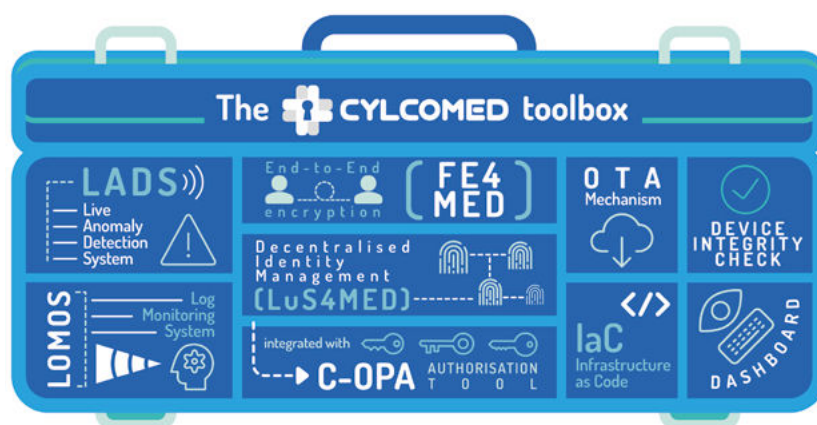
Robust identity management, access controls, and encryption are integrated to ensure privacy, compliance, and a resilient digital security framework capable of meeting future challenges. Furthermore, Pediatric Hospital Niño Jesús of Madrid is testing the project's dashboard (another key toolbox component) in emergency medical services ambulances. The dashboard supervises the cybersecurity status of the 5G connection used to send the clinical parameters of a child in critical condition from the ambulance to the hospital.

Human at the core: Co-creation with Patients and Professionals

CYLCOMED involves healthcare professionals, IT staff, SMEs, and patients in its co-creation process. Professionals benefit from secure device integration, patients gain stronger data protection, and SMEs contribute to and benefit from cybersecurity innovation. While regulators are not directly involved, the project aligns with existing EU compliance pathways. Capacity-building activities include targeted training sessions on ISO standards, webinars on advancing cybersecurity in healthcare, and presentations at key EU events. Workshops and clinical trials further engage stakeholders and ensure practical alignment with hospital workflows and ethical standards. Dr. Diana Ferro, who participated in the 2025 HIMSS co-creation workshop with other EU projects, stated: “Presenting CYLCOMED at HIMSS 2025 was an exciting opportunity to share how we’re advancing secure and explainable AI for healthcare. Being part of the EU Projects Pavilion and contributing to the panel on value co creation was a great way to highlight the real-world impact our work is having on both patients and healthcare systems.”

Key Outputs and Results

CYLCOMED has delivered a specialised cybersecurity toolbox integrating AI-driven network and log anomaly detection (LADS and LOMOS, respectively), end-to-end encryption (FE4MED), and decentralised identity management (LuS4MED). The latter is integrated with the authorisation tool C-OPA, based on user attributes and roles. These tools collectively monitor abnormal system behaviour, ensure fine-grained access control, and secure patient data during transmission and storage.



Preliminary results from Ospedale Pediatrico Bambino Gesù confirm the solution's ethical integrity, technical robustness, and practical relevance, supporting safer, regulation-compliant CMDs use. Further, stakeholders recognise the increasing importance of cybersecurity in healthcare, particularly in pediatric contexts, and emphasise the need for tools that are both robust and user-friendly.

Sustainability and Future Outlook

CYLCOMED's long-term sustainability strategy focuses on refining and adapting its AI-driven detection systems, such as LADS and LOMOS, to counter evolving cyber threats. This includes ongoing model training with real-world data from pilot environments. In addition, the secure identity management solutions (LuS4MED) and data protection mechanisms (FE4MED) will be further optimised for seamless integration across diverse healthcare IT infrastructures, ensuring scalability and ease of deployment. Further, the project aims to contribute to broader standardisation efforts in medical device cybersecurity, sharing its findings and best practices to influence future regulatory frameworks. Finally, the modular architecture of the CYLCOMED security dashboard is designed for long-term extensibility, allowing for the incorporation of new tools and functionalities as cybersecurity needs in healthcare evolve. Our commitment is to foster a more resilient and secure digital health ecosystem.

Consortium and Governance

CYLCOMED comprises 10 beneficiaries across 7 European countries including 1 associate partner, blending technical expertise, regulatory insights, and clinical validation capabilities. The project is coordinated by Charité Universitätsmedizin Berlin and includes partners Eviden, RGB Medical Devices, INOV, Ospedale Pediatrico Bambino Gesù, Fundacion Para la Investigacion Biomedica Hospital infantil Universitario Niño Jesus, KU Leuven, XLAB, MediaClinics Italia, and Martel Innovate.

Project Website: cylcomed.eu

Contact: info@cylcomed.eu