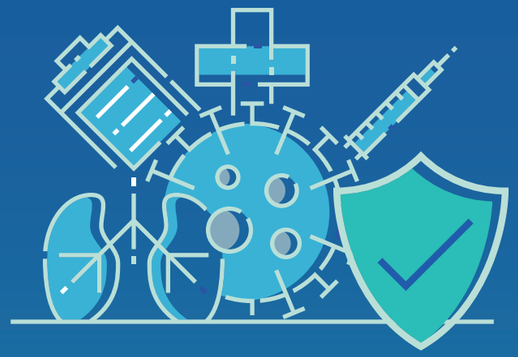
CYLCOMED

ON A MISSION TO ENHANCE CYBERSECURITY IN HEALTHCARE

CYLCOMED will provide a methodological and technical cybersecurity framework designed for healthcare services that use Connected Medical Devices (CMDs).



The issue at hand

Healthcare ranks among the top three sectors targeted by cyberattacks, according to the European Union Agency for Cybersecurity (ENISA). Patient data, especially electronic health records, is a prime target. Cyberattacks can disrupt hospital operations, compromise patient safety, and in extreme cases, endanger lives. Despite increased focus, healthcare still lags in cybersecurity preparedness compared to other industries.

Legal and Ethical Compliance

KU Leuven, as the legal and ethical partner, will guide consortium members in aligning with these regulations to ensure compliance, privacy protection, and ethical cybersecurity practices for Connected Medical Devices (CMDs).

The CYLCOMED project must navigate a complex legal framework involving multiple EU regulations. The Medical Devices Regulation (MDR) establishes strict requirements to ensure the safety and performance of medical devices, including cybersecurity standards. The General Data Protection Regulation (GDPR) focuses on safeguarding personal data, particularly sensitive health information, by requiring robust technical and organizational measures. The Cybersecurity Act (CSA) introduces an EU-wide certification framework, promoting consistent cybersecurity standards across digital products and services, including medical devices. Similarly, the NIS2 Directive emphasizes risk management and reporting obligations for essential and important entities, including medical device manufacturers, to strengthen cybersecurity resilience. Finally, the AI Act imposes additional obligations on AI-powered medical devices, requiring compliance with rules related to data governance, human oversight, and cybersecurity, further increasing regulatory complexity.

Overcoming Cybersecurity Challenges

Healthcare's focus on patient care often leaves cybersecurity overlooked, creating vulnerabilities. The rapid evolution of cyber threats adds to the complexity faced by healthcare professionals. Human error remains a leading cause of breaches, underscoring the need for continuous training and awareness to strengthen cybersecurity defenses.

The CYLCOMED Toolbox for CMD Security

CYLCOMED's modular toolbox enhances cybersecurity for Connected Medical Devices (CMDs). It addresses device security, integrity, and data protection through four key layers: Data Collection and Analysis, Device Integrity and Security, Identity and Access Management, and a Security Dashboard for real-time monitoring and visualization.

Pilots and Real-World Testing

CYLCOMED's solutions will undergo testing in two pilots. Pilot 1 focuses on ICU equipment, leveraging digital twins to assess device integrity. Pilot 2 evaluates telemedicine platforms, emphasizing data integrity and patient protection. These pilots will validate the toolbox's effectiveness in both simulated and real-world environments, showcasing its adaptability and innovation.

DISCOVER MORE ON OUR WEBSITE

OR FOLLOW US

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

CHARITÉ UNIVERSITÄTSMEDIZIN BERLIN · EVIDEN an atos business · MEDIACLINICS Wearable Health Applications · XLAB · MARTEL innovate

Fundación para la Investigación Biomédica Hospital Infantil Universitario Niño Jesús · OSPEDALE PEDIATRICO Bambino Gesù · RGB medical devices · INOV inesc · KU LEUVEN CiTiP CENTRE FOR IT & IP LAW

cylcomed.eu