CYLCOMED

THE CYBERSECURITY NEXUS OF THE AI ACT AND MDR

Dusko Milojevic

Webinar on Adaptive AI for Pioneering Secure Healthcare Innovation

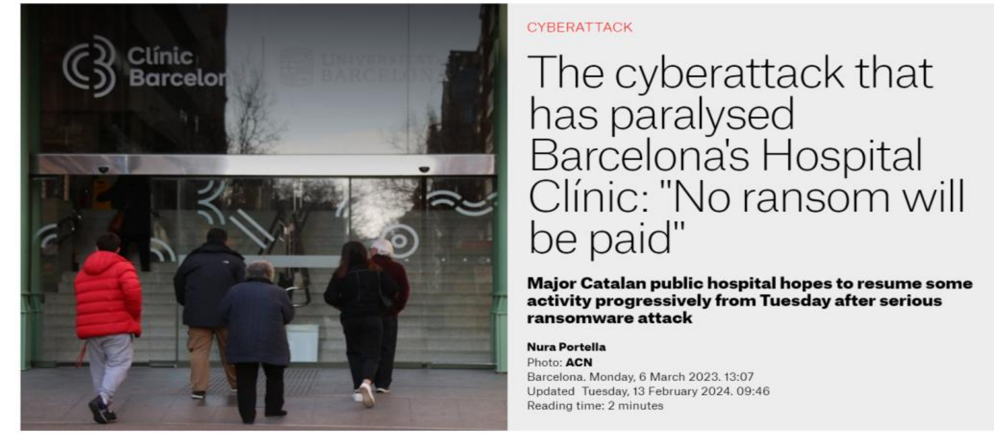
March 18, 2025

AGENDA

CYLCOMED

- Overview of Healthcare cybersecurity challenges and bleak stats
- Project Architecture and Toolbox
- Legal Challenges

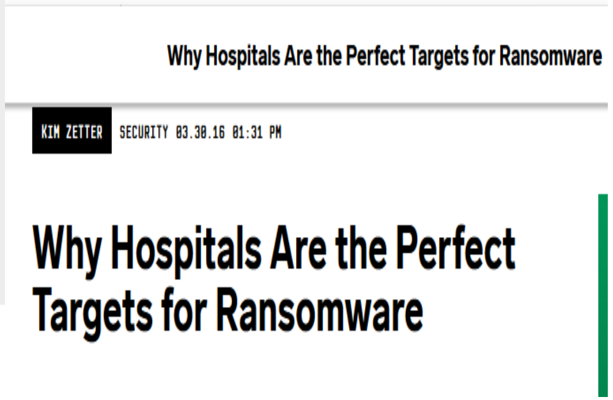
UNIQUE CHALLENGES TO THE HEALTHCARE SECTOR


CYBERATTACK

The cyberattack that has paralysed Barcelona's Hospital Clínic: "No ransom will be paid"

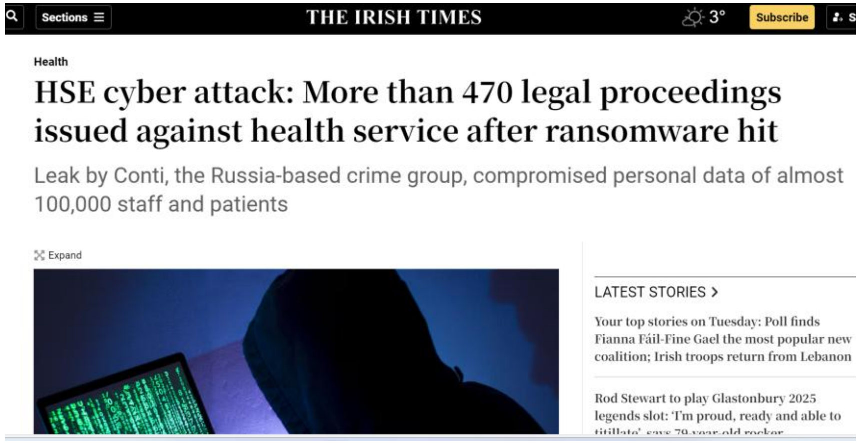
Major Catalan public hospital hopes to resume some activity progressively from Tuesday after serious ransomware attack

Nura Portella
Photo: **ACN**
Barcelona. Monday, 6 March 2023. 13:07
Updated Tuesday, 13 February 2024. 09:46
Reading time: 2 minutes


Why Hospitals Are the Perfect Targets for Ransomware

KIM ZETTER SECURITY 03.30.16 01:31 PM

Why Hospitals Are the Perfect Targets for Ransomware



Health

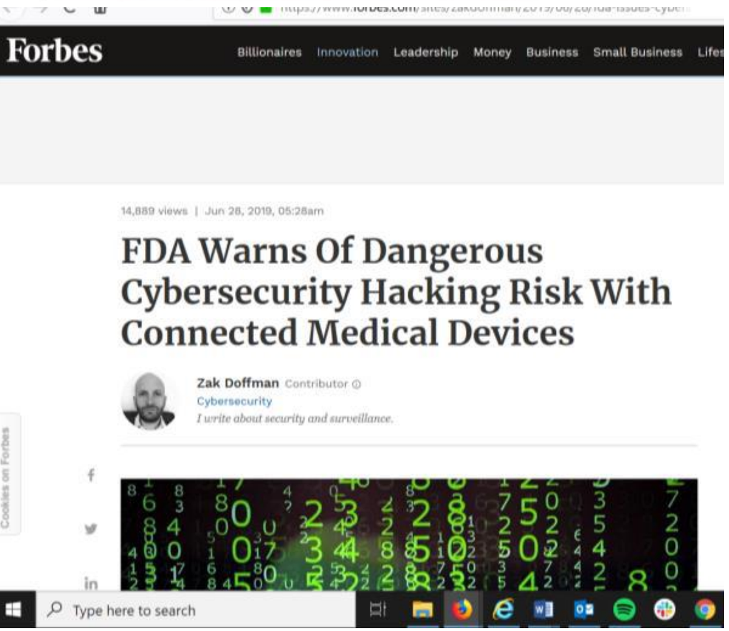
HSE cyber attack: More than 470 legal proceedings issued against health service after ransomware hit

Leak by Conti, the Russia-based crime group, compromised personal data of almost 100,000 staff and patients

LATEST STORIES >

Your top stories on Tuesday: Poll finds Fianna Fáil-Fine Gael the most popular new coalition; Irish troops return from Lebanon

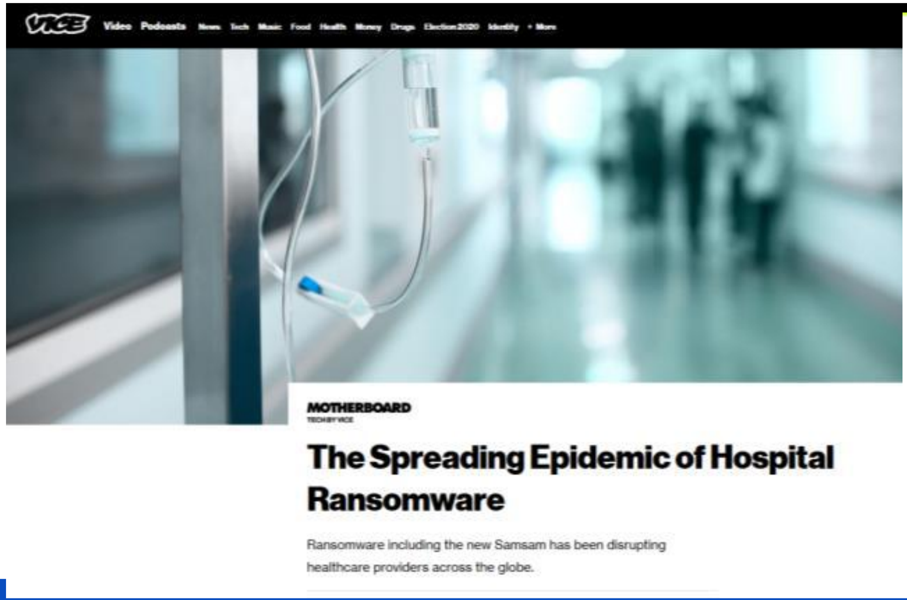
Rod Stewart to play Glastonbury 2025 legends slot: 'I'm proud, ready and able to titillate', says 79-year-old rocker


Forbes
Billionaires Innovation Leadership Money Business Small Business Lifes
Type here to search

14,889 views | Jun 28, 2019, 05:28am

FDA Warns Of Dangerous Cybersecurity Hacking Risk With Connected Medical Devices

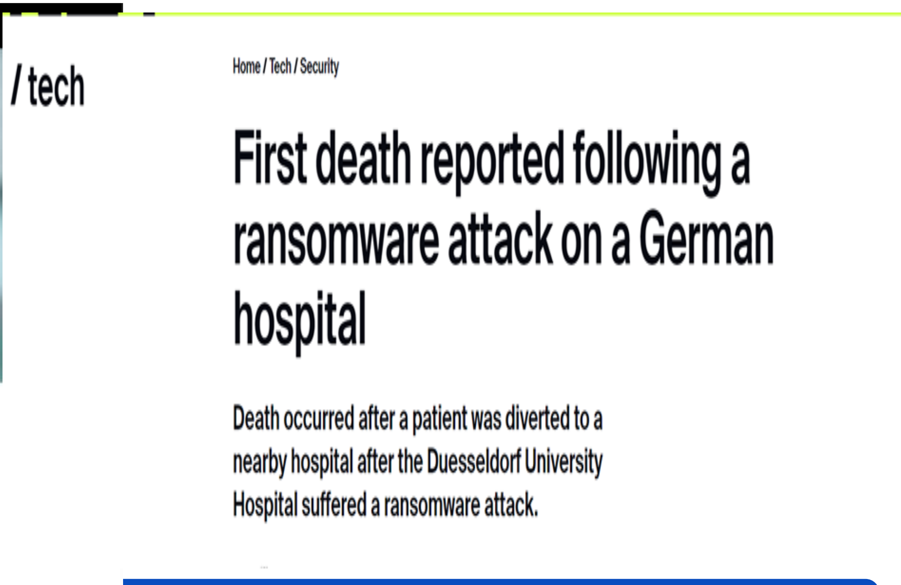
Zak Doffman Contributor
Cybersecurity
I write about security and surveillance.


VICE Video Podcasts News Tech Music Food Health Money Drugs Election2020 Identity + More

MOTHERBOARD
TECH BY VICE

The Spreading Epidemic of Hospital Ransomware

Ransomware including the new Samsam has been disrupting healthcare providers across the globe.


/ tech

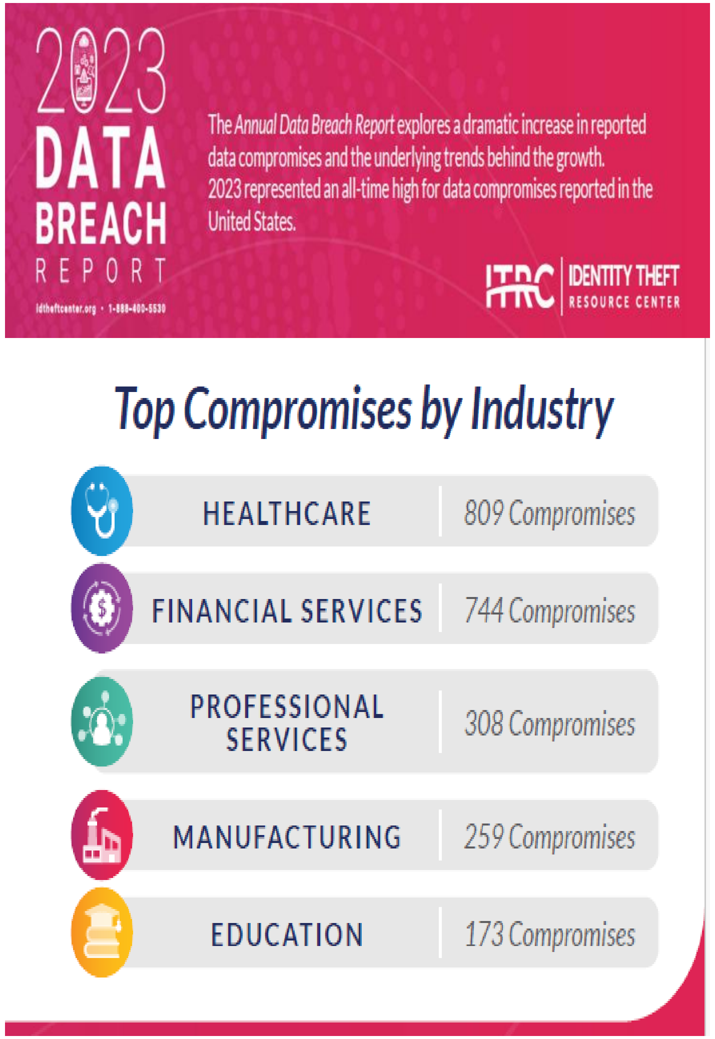
Home / Tech / Security

First death reported following a ransomware attack on a German hospital

Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack.

THE HEALTHCARE SECTOR CYBERSECURITY STATS

CYLCOMED



2023 DATA BREACH REPORT

The *Annual Data Breach Report* explores a dramatic increase in reported data compromises and the underlying trends behind the growth. 2023 represented an all-time high for data compromises reported in the United States.

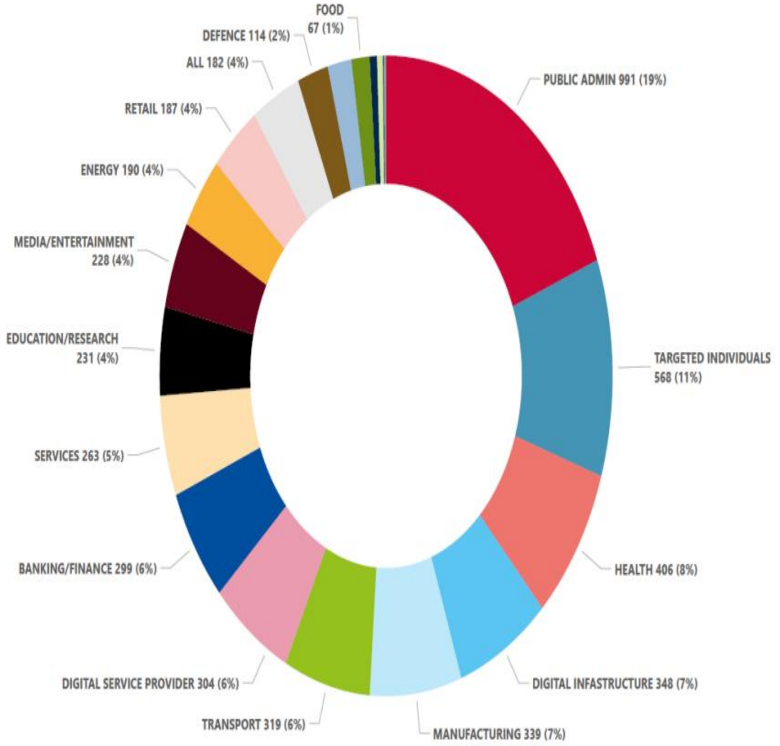
idtheftcenter.org • 1-888-400-5530

ITRC IDENTITY THEFT RESOURCE CENTER

Top Compromises by Industry

HEALTHCARE	809 Compromises
FINANCIAL SERVICES	744 Compromises
PROFESSIONAL SERVICES	308 Compromises
MANUFACTURING	259 Compromises
EDUCATION	173 Compromises

ENISA THREAT LANDSCAPE 2023



THE 2024 STUDY ON CYBER INSECURITY IN HEALTHCARE:

THE COST AND IMPACT ON PATIENT SAFETY AND CARE

Independently conducted by:

Ponemon INSTITUTE

92%

of organizations in this research had at least one cyberattack over the past 12 months

$4.7M

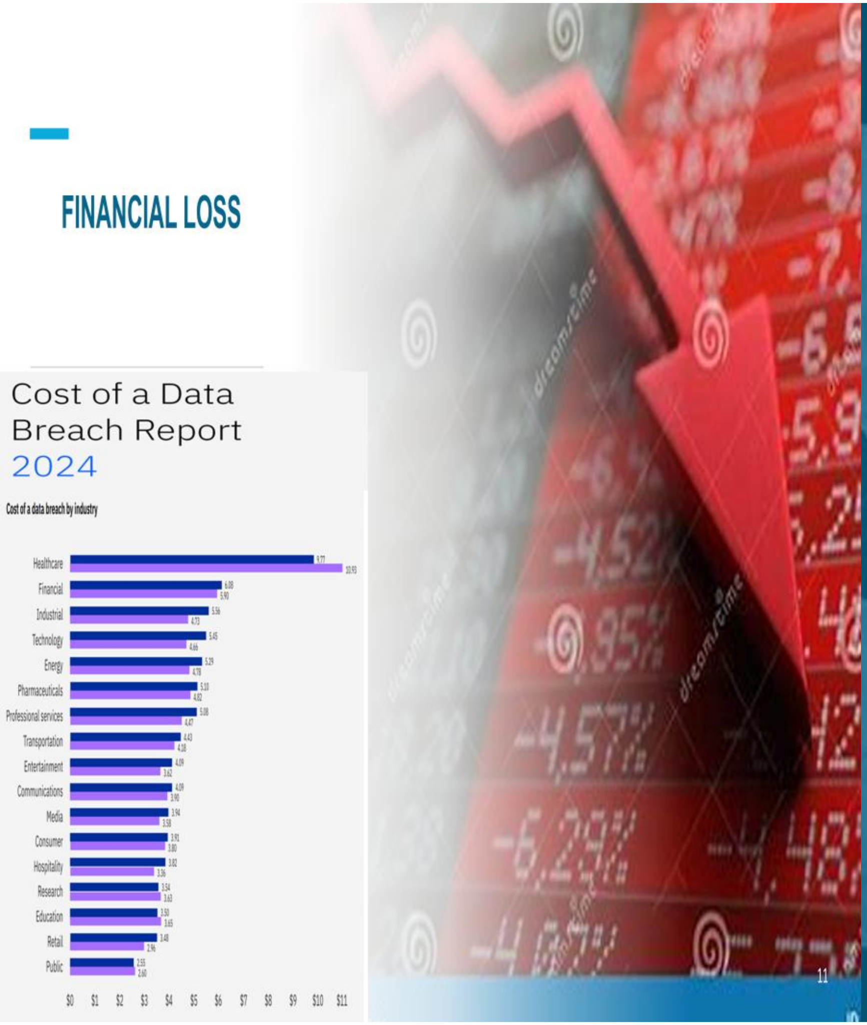
is the average total cost for the single most expensive cyberattack experienced over the past 12 months

$1.47M

in disruption to normal healthcare operations was on average the most significant financial consequence from the cyberattack

WHAT IS AT STAKE?

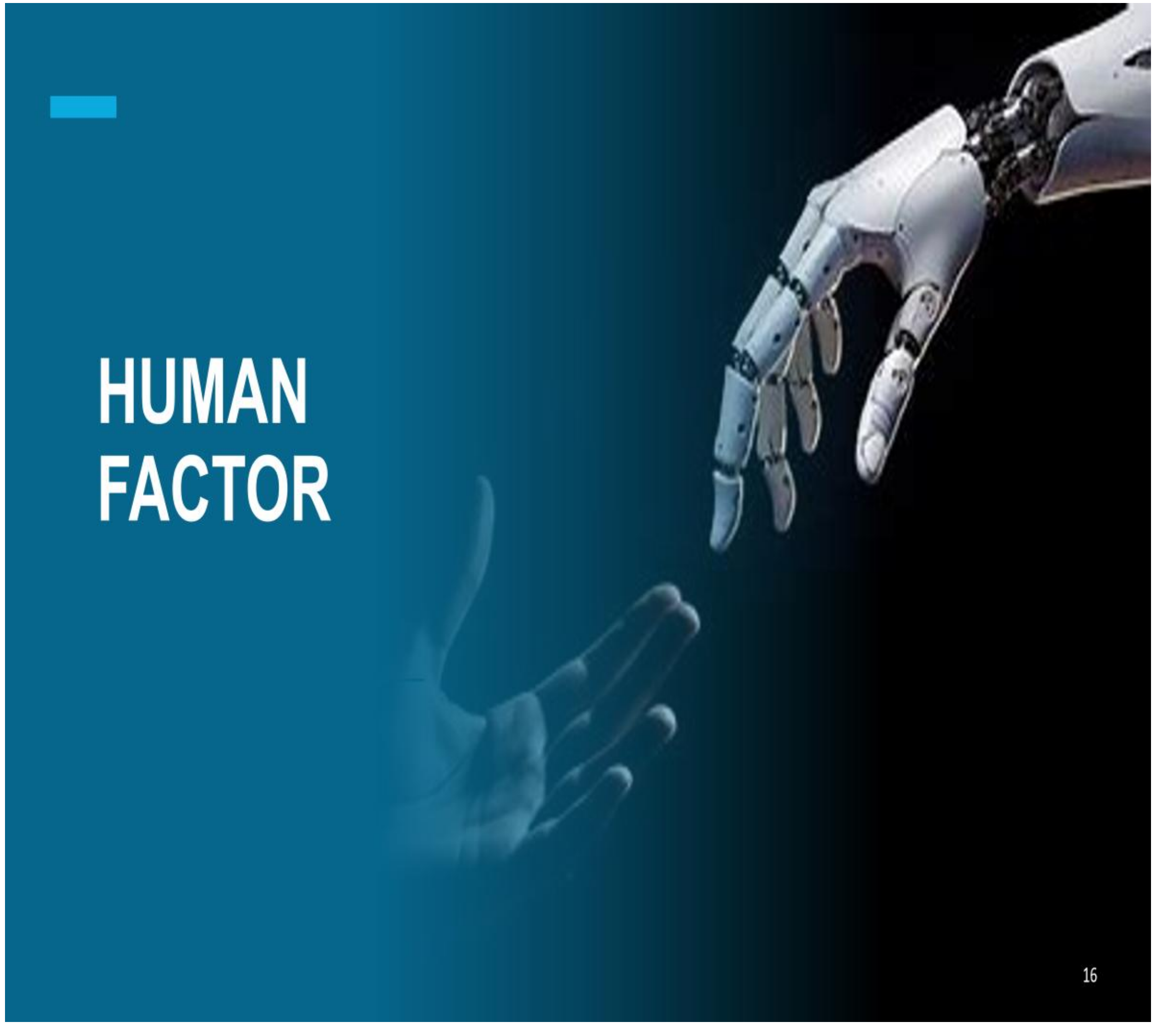
WHAT IS AT STAKE?



WHY IS HEALTH SECTOR VULNERABLE ?

CONNECTED MEDICAL DEVICES (LEGACY DEVICES)

15



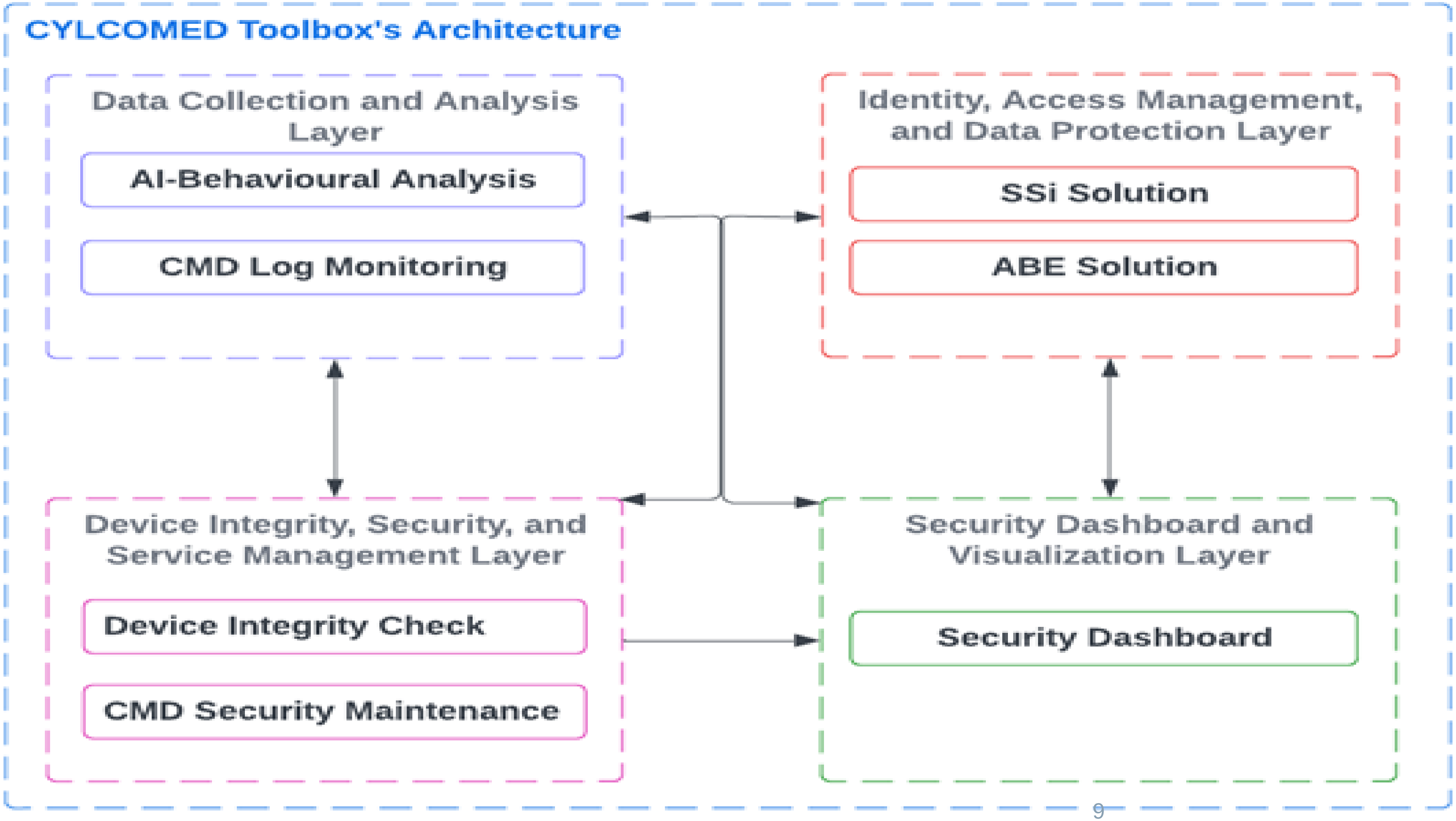
HUMAN FACTOR

16

CYLCOMED OBJECTIVES

Objectives

1	**Identification of ethical, legal and regulatory frameworks and challenges and providing recommendations to extend cybersecurity guidelines for CMDs from the legal and ethical perspective**
2	**Complete review of CMD cybersecurity standards, guidelines and best practices, issuing intermediate and final Recommendations to extend cybersecurity guidelines for CMDs**
3	**Adoption-ready cyber risk management methodology and tools for CMD and novel technologies (AI, 5G, Blockchain, Cloud computing)**
4	End-user driven design and implementation of cybersecurity toolbox for CMDs
5	Toolbox integration and validation in real-world telemedicine and hospital infrastructures
6	Maximise impact through communication, dissemination, exploitation and training for adoption



CYLCOMED Toolbox's Architecture

Data Collection and Analysis Layer

AI-Behavioural Analysis

CMD Log Monitoring

Identity, Access Management, and Data Protection Layer

SSi Solution

ABE Solution

Device Integrity, Security, and Service Management Layer

Device Integrity Check

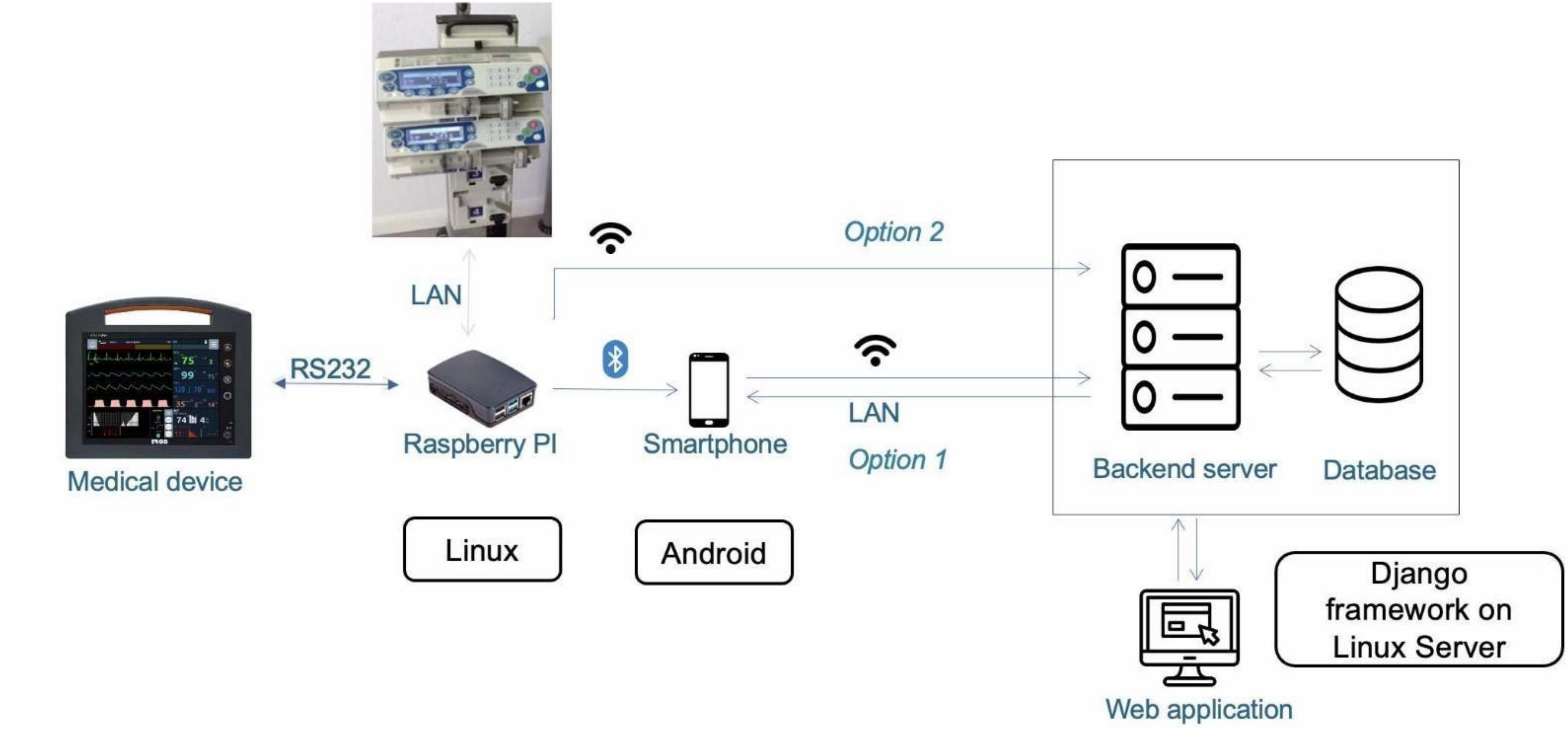
CMD Security Maintenance

Security Dashboard and Visualization Layer

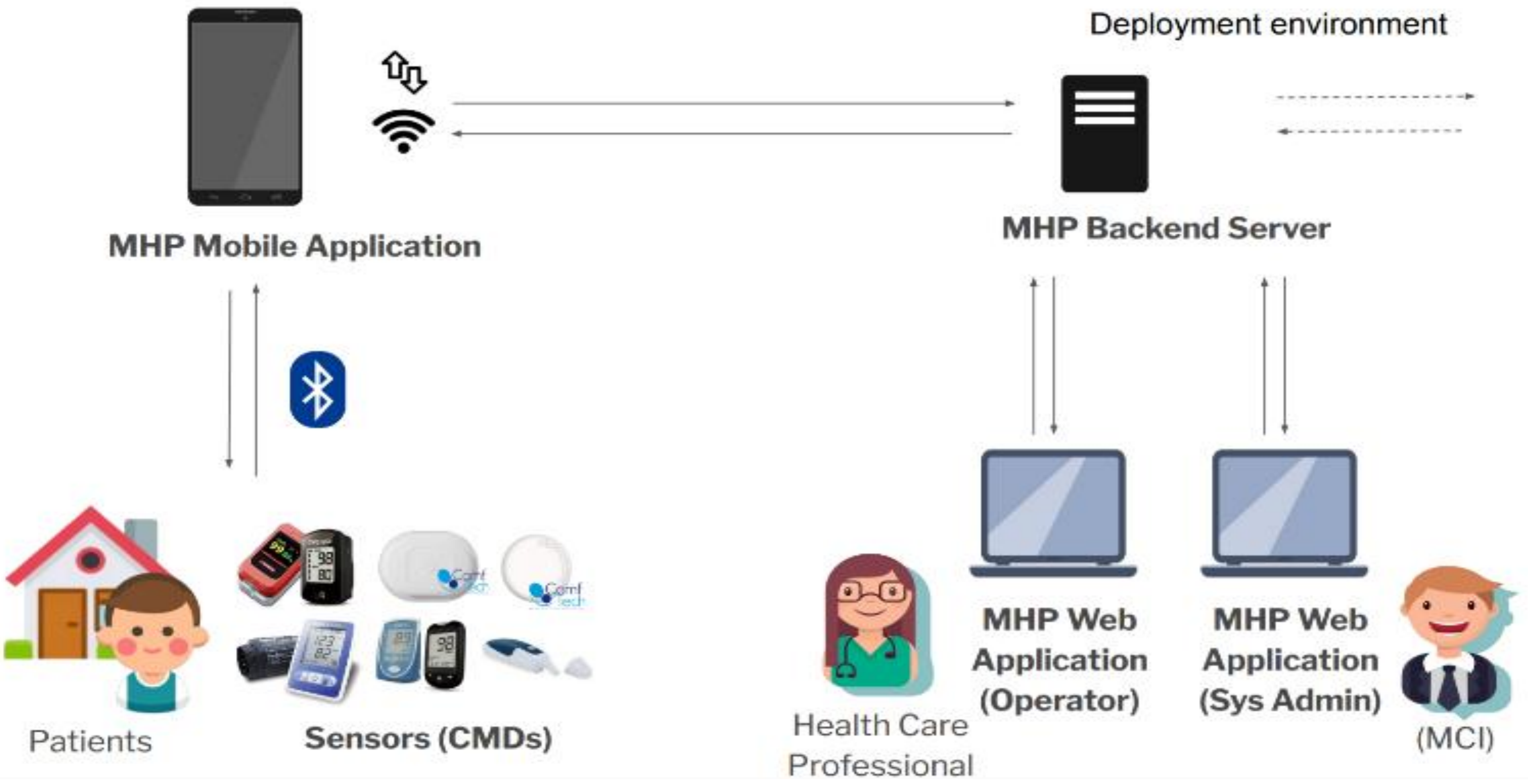
Security Dashboard

PILOT 1 - "CYBERSECURITY IN HOSPITAL EQUIPMENT FOR COVID-19 ICU PATIENTS"

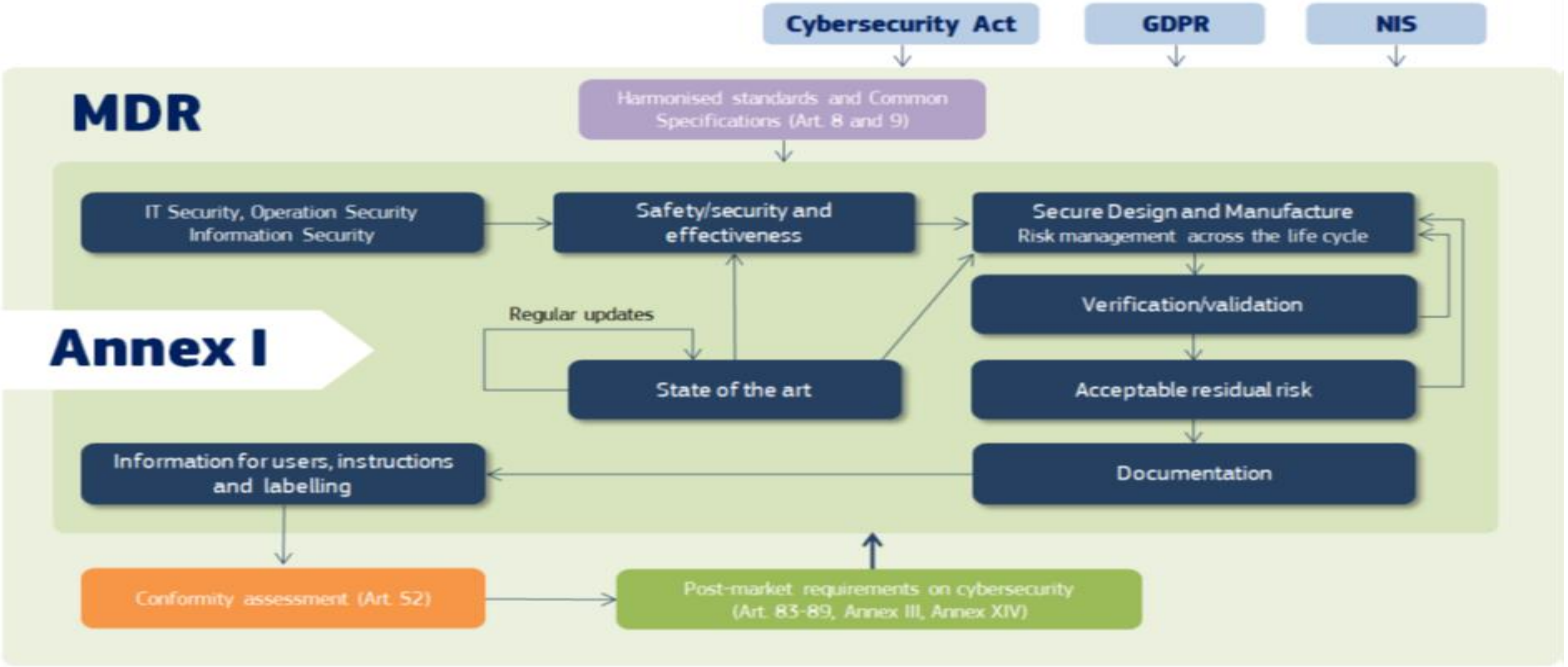
CYLCOMED



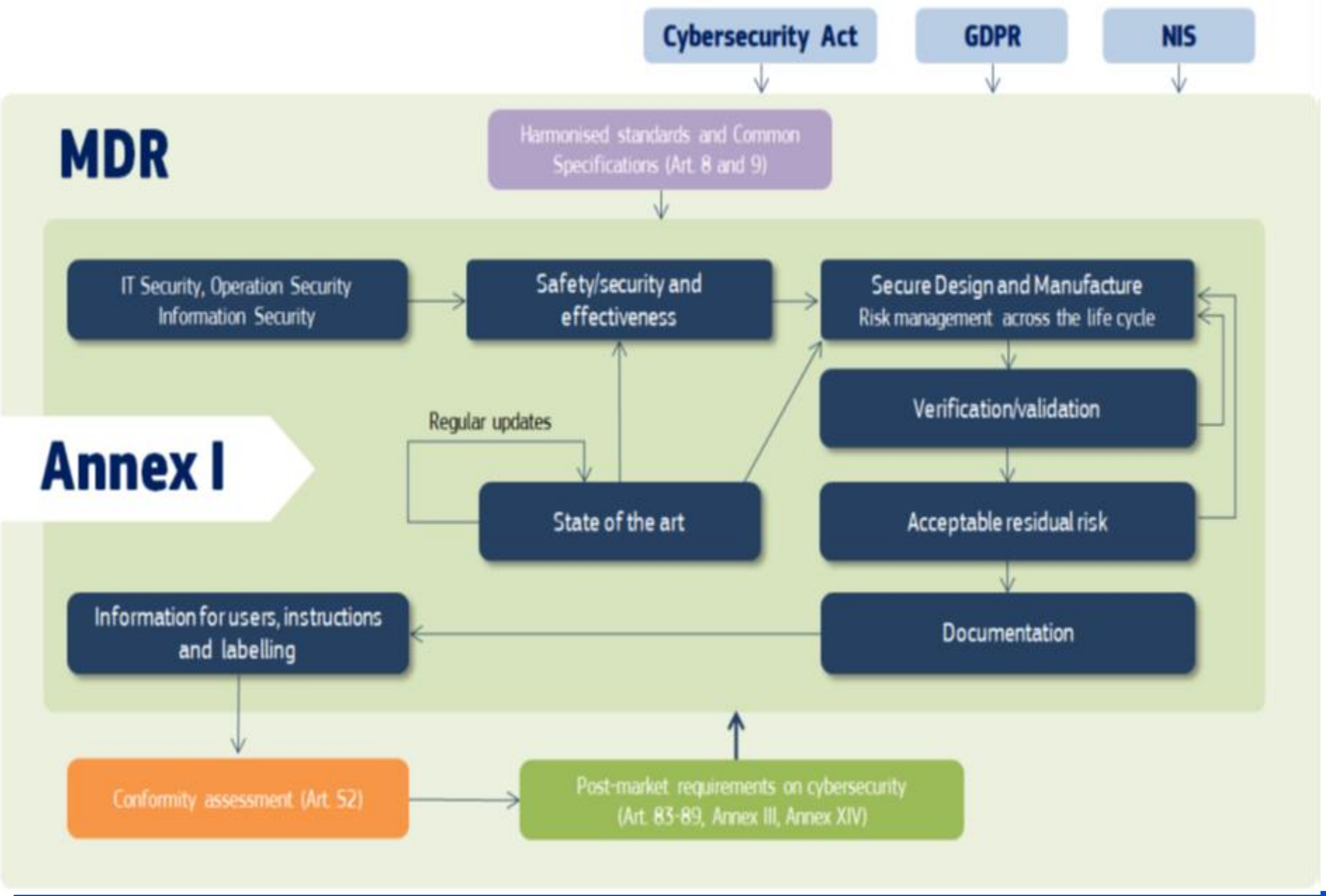
PILOT 2 - *CYBERSECURITY FOR TELEMEDICINE PLATFORMS*



CYBERSECURITY LEGAL FRAMEWORK


Cybersecurity Act
GDPR
NIS
MDR
Harmonised standards and Common Specifications (Art. 8 and 9)
IT Security, Operation Security Information Security
Safety/security and effectiveness
Secure Design and Manufacture Risk management across the life cycle
Regular updates
Annex I
Verification/validation
State of the art
Acceptable residual risk
Information for users, instructions and labelling
Documentation
Conformity assessment (Art. 52)
Post-market requirements on cybersecurity (Art. 83-89, Annex III, Annex XIV)

CYBERSECURITY LEGAL FRAMEWORK


Cybersecurity Act
GDPR
NIS
MDR
Harmonised standards and Common Specifications (Art. 8 and 9)
IT Security, Operation Security Information Security
Safety/security and effectiveness
Secure Design and Manufacture Risk management across the life cycle
Verification/validation
Regular updates
Annex I
State of the art
Acceptable residual risk
Information for users, instructions and labelling
Documentation
Conformity assessment (Art. 52)
Post-market requirements on cybersecurity (Art. 83-89, Annex III, Annex XIV)

NIS2

AI ACT

DATA ACT

EHDS

AI ACT

Horizontal Regulation

Sector Agnostic

Regulatory obligations for Healthcare sector (medical device manufacturers, hospitals, etc.)

Cybersecurity Requirements

INTERPLAY BETWEEN MDR AND AI ACT

MDR

‘**serious incident**’ means any incident that **directly or indirectly led**, might have led or might lead to any of the following:

(a) the death of a patient, user or other person,

(b) the temporary or permanent serious deterioration of a patient's, user's or other person's state of health,

(c) a serious public health threat; (Art.2(65))

AI ACT

‘serious incident’ means an incident or malfunctioning of an AI system **that directly or indirectly leads** to any of the following:

(a) the death of a person or serious harm to a person’s health;

(b) a serious and irreversible disruption of the management or operation of critical infrastructure;

(c) **the infringement of obligations under Union law intended to protect fundamental rights;**

(d) **serious harm to property or the environment; (Art. 3.(49)**

REPORTING OBLIGATIONS

Regulation	Triggering Event	Reporting Responsibility	Deadline	Authority
MDR	Serious incident	Medical devices manufacturers	• Immediately and not later than 15 days • 2 days in the event of a serious public health threat, or "immediately" in the event of death or unanticipated serious deterioration of a person's state of health	relevant competent authorities
AI Act	Serious incident	Providers of high-risk AI systems	• Immediately and not later than 15 days • not later than two days after the provider or, where applicable, the deployer becomes aware of that incident in the event of a widespread infringement • in the event of the death of a person, the report shall be provided immediately	market surveillance authorities
GDPR	Personal data breach	Data Controler	Without undue delay and, where feasible, not later than 72 hours after having become aware of it	Supervisory authority
NIS2	Security incident	Entities affected	Within 24 hours, an early warning Within 72 hours, an incident notification	National authority or CSIRT

Cybersecurity Toolbox for Connected Medical Devices

CYLCOMED

KU Leuven: Legal and Ethical Partner in CYLCOMED Project

- **Role**: Ensures ethical and legally compliant use of innovative solutions to enhance the cybersecurity of connected medical devices (CMDs).
- **Expertise**: Develops an ethical and legal framework addressing privacy, data protection, CMD regulations, and cybersecurity legislation.
- **Track Record**: Renowned for expertise in AI, autonomous systems, data protection, eHealth, ethics & law, intellectual property, media, telecommunications, and cybersecurity. Longstanding partner in large international and interdisciplinary research projects.

CHARITÉ

MEDIACLINICS
Wearable Health Applications

fib
Hospital Infantil Universitario Niño Jesús

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

EVIDEN
an atos business

XLAB

RGB
medical devices

MARTEL
innovate

OSPEDALE PEDIATRICO Bambino Gesù

INOV

Scan to learn more:

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**