NAVIGATING CYBERSECURITY CHALLENGES IN HEALTHCARE: CYLCOMED PROJECT

Dusko Milojevic & Maja Nisevic

Isparta, Turkey (Online Conference)

2-3 December, 2024

AGENDA

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

Sections THE IRISH TIMES 3° Subscribe

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

Expand

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

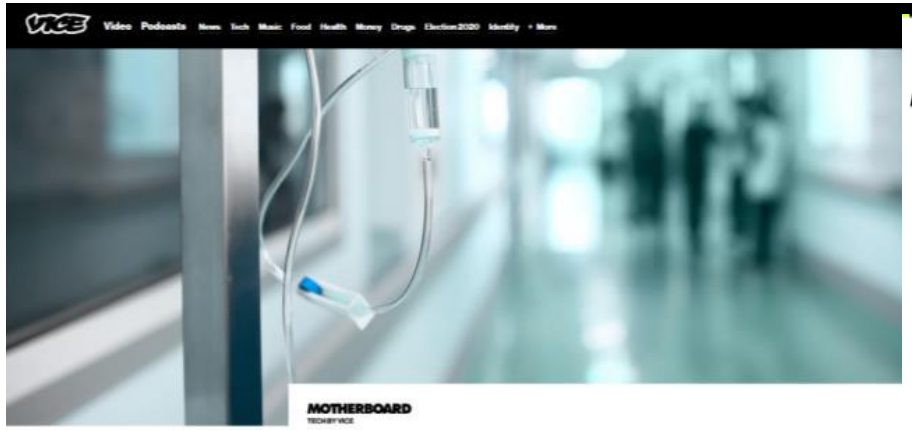
Forbes Billionaires Innovation Leadership Money Business Small Business Lifes

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.

Type here to search



MOTHERBOARD

The Spreading Epidemic of Hospital Ransomware

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

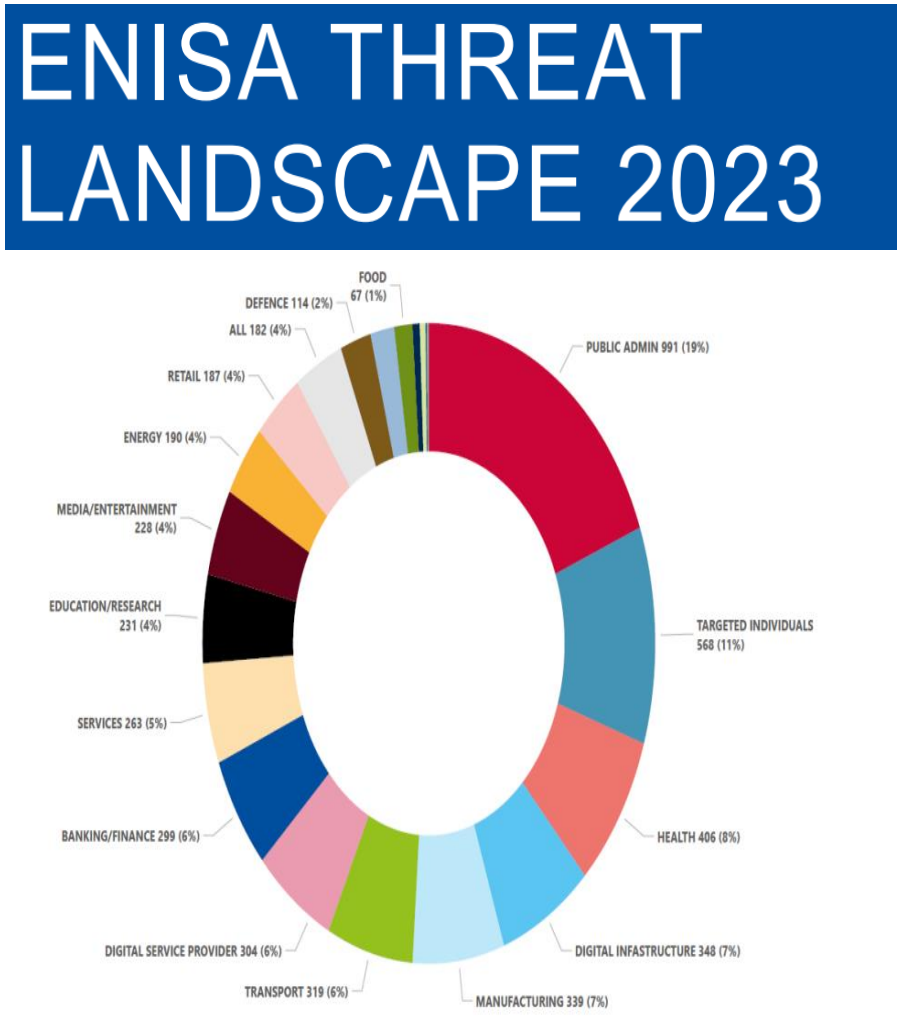
/ tech

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



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 THE STAKE? DIRE CONSEQUENCES OF CYBERATTACKS

- BREACH OR THEFT OF DATA
- DISRUPTION OF HEALTHCARE SERVICES
- PATIENT/HEALTHCARE PROFESSIONAL SAFETY
- REPUTATIONAL HARM
- FINANCIAL LOSS

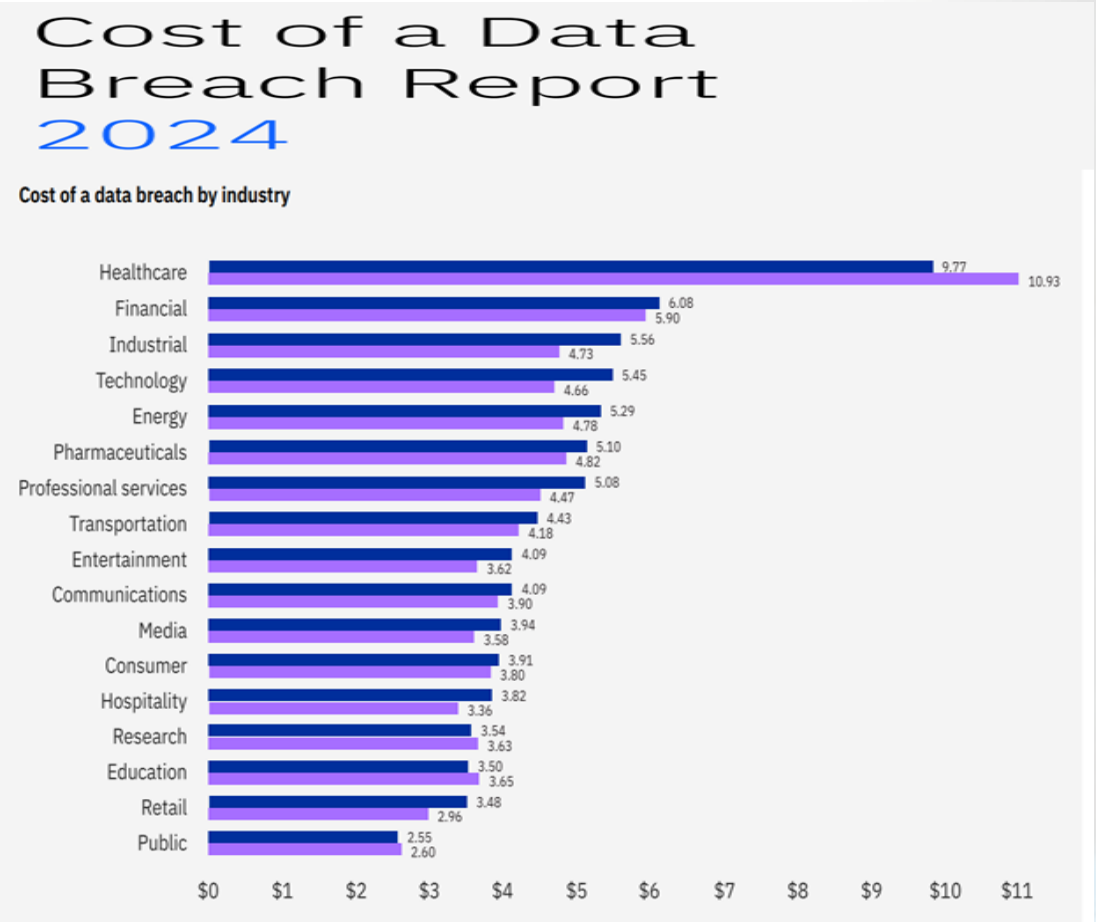
BREACH OR THEFT OF DATA

DISRUPTION OF HEALTHCARE SERVICES

PATIENT SAFETY

REPUTATIONAL HARM

FINANCIAL LOSS



WHY HEALTH SECTOR ?

WHY IS HEALTH SECTOR VULNERABLE ?

- Financial Gain
- Easy Target
- Connected Medical Devices (Legacy Devices)
- Human Factor

FINANCIAL GAIN

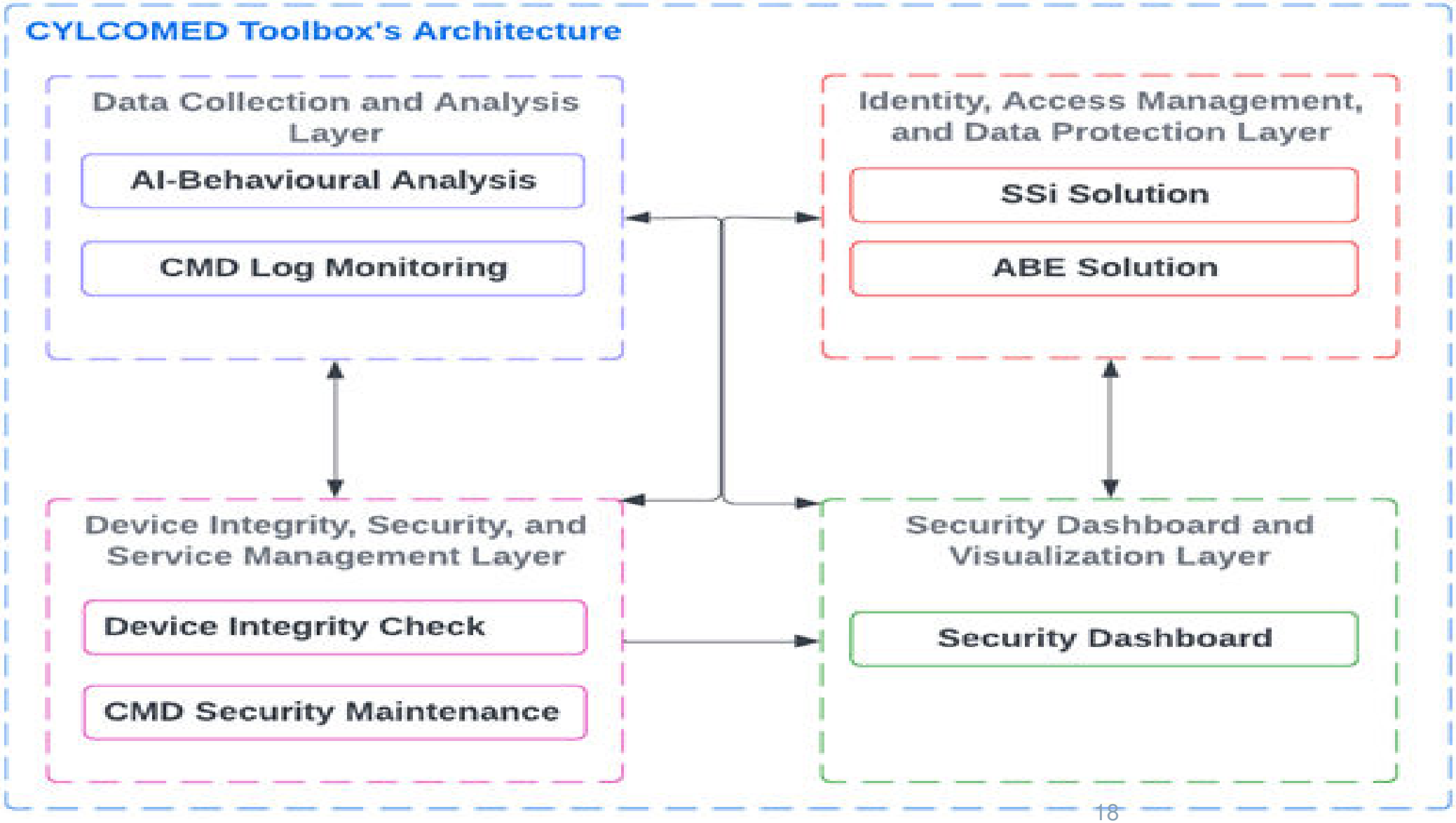
EASY TARGET

- **CONNECTED MEDICAL DEVICES (LEGACY DEVICES)**

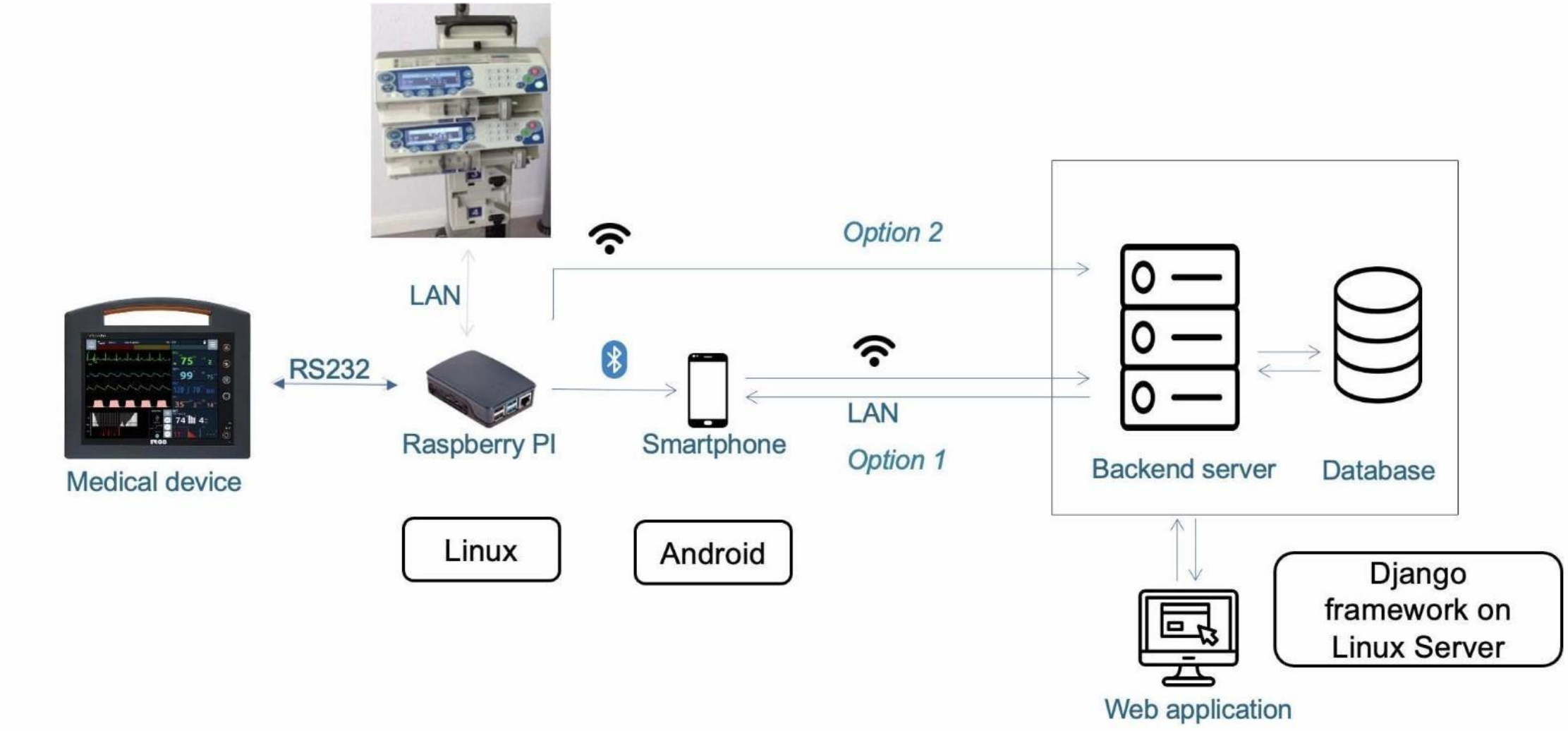
HUMAN FACTOR

Objectives

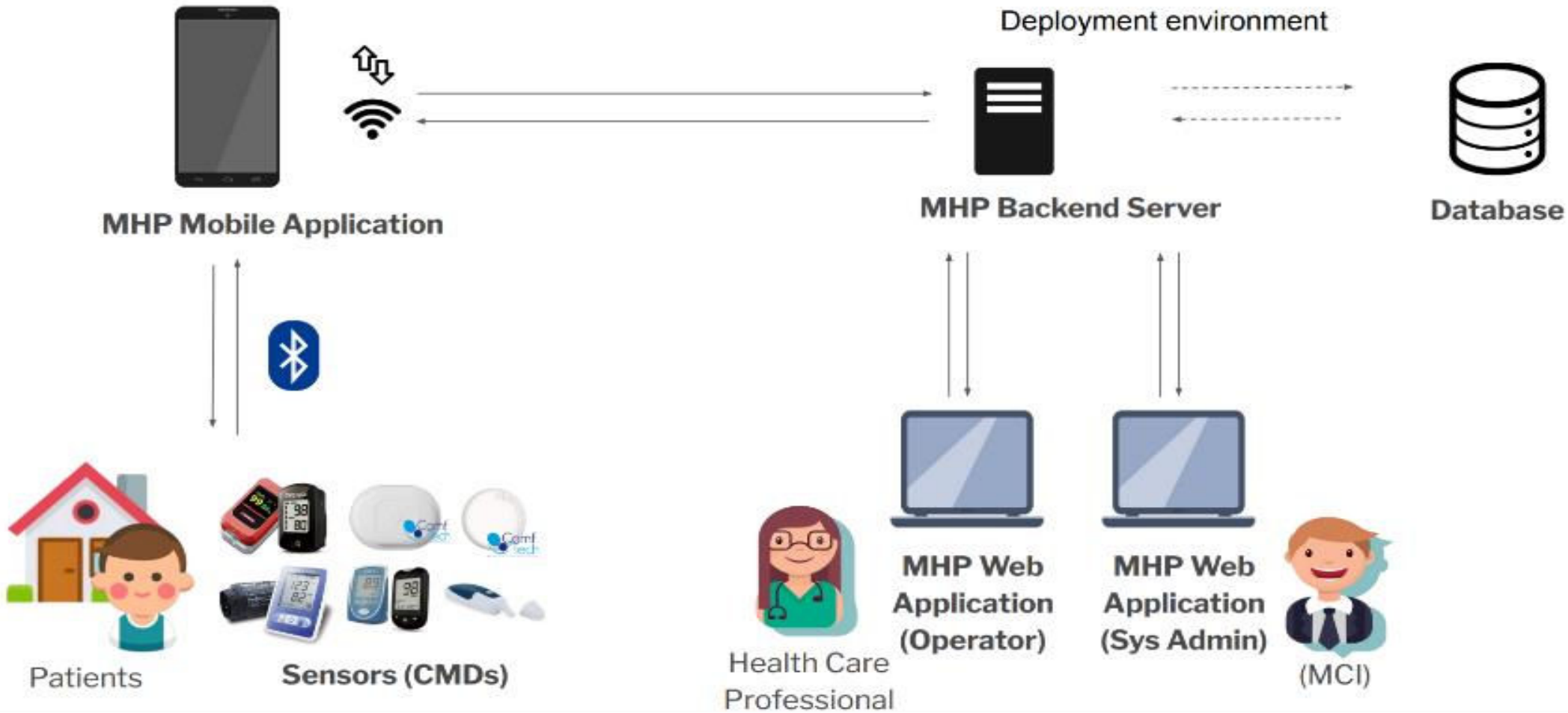
1	**Identification of ethical, legal and regulatory frameworks and challenges and providing recommendations to extend cybersecurity guidelines for CMDs from the legal and ethical perspective**
2	**Complete review of CMD cybersecurity standards, guidelines and best practices, issuing intermediate and 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”



PILOT 2 - *CYBERSECURITY FOR TELEMEDICINE PLATFORMS*



PILOT 2 - *CYBERSECURITY FOR TELEMEDICINE PLATFORMS*

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

CYLCOMED

Overview of Legal and Ethical Frameworks CYLCOMED

Data Laws	Cybersecurity Laws	AI Law	Medical Devices Laws
Data Protection Law (**GDPR**)	Cybersecurity Act (**CA**)	Artificial Intelligence Act (**AI Act**)	Medical Device Regulation (**MDR**)
Data Act	Network and Information System Directive **(NIS2)**	Soft Law Instruments (e.g AI HLEG)	In Vitro Medical Device Regulation (**IVDR**)
European Health Data Spaces Proposal (**EDHS**)	Radio Equipment Directive (**RED**)		Soft Law Instruments (e.g MDCG)
	Cyber Resilience Act (**CRA**)		

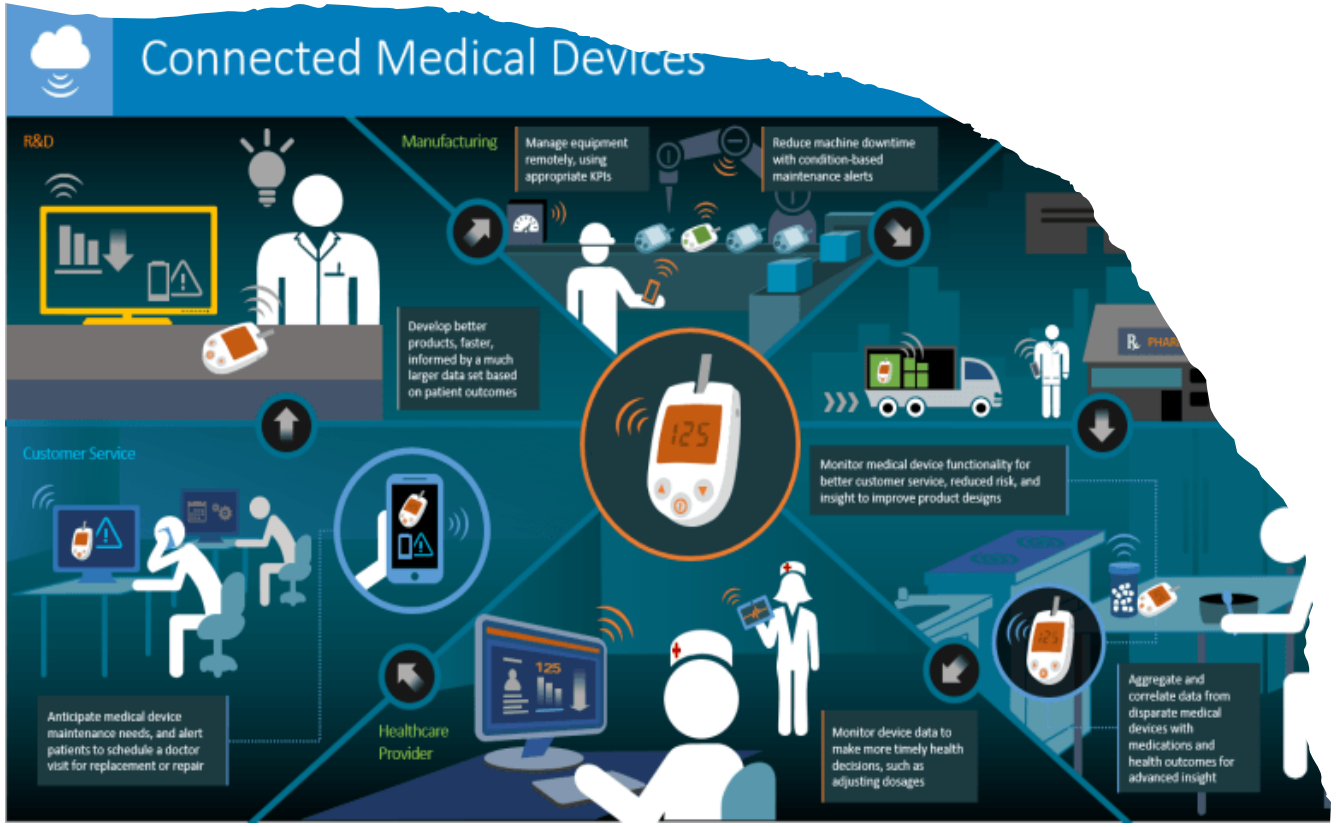
Ethical Requirements

Principles of Bioethics, Declaration of Helsinki, ICH GCP, CIOMS, CTR

LEGAL CHALLENGES

- Complex and fast evolving regulatory landscape
- Regulatory overlapping
- Fragmentation risks
- Regulatory uncertainty

MDCG 2019-16 GENERAL OBSERVATIONS



- Not legally binding
- Superficially addresses connection between soft law instrument and hard law
- does not include explicit definitions nor reference to terms such as "cybersecurity," "security-by-design," and "security-by-default."
- Fails to further clarify notion of “Cybersecurity is shared responsibilities”
- No reference to ethics
- “Outdated”

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 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