

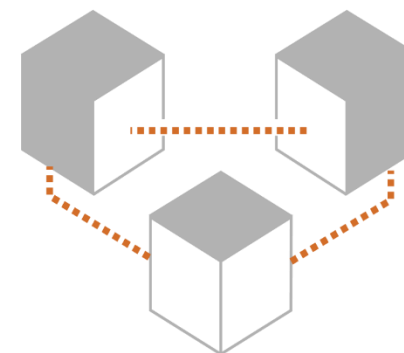
CUREX

SECURE AND PRIVATE HEALTH DATA EXCHANGE

Prof. Christos Xenakis – Project Coordinator

Eleni Veroni – Project Manager

University of Piraeus



Project Information

- **CUREX:** seCUre and pRivate hEalth data eXchange
- **Grant Agreement ID:** 826404
- **Programme:** Improving health information and better use of health data (H2020-EU.3.1.5.1.)
- **Topic:** Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures (SU-TDS-02-2018)
- **Call:** Trusted digital solutions and Cybersecurity in Health and Care (H2020-SC1-FA-DTS-2018-1)
- **Funding Scheme:** RIA - Research and Innovation action
- **Overall budget:** € 4 987 825
- **EU contribution:** € 4 987 825
- **Start Date:** December 1st, 2018
- **End Date:** November 30th, 2021

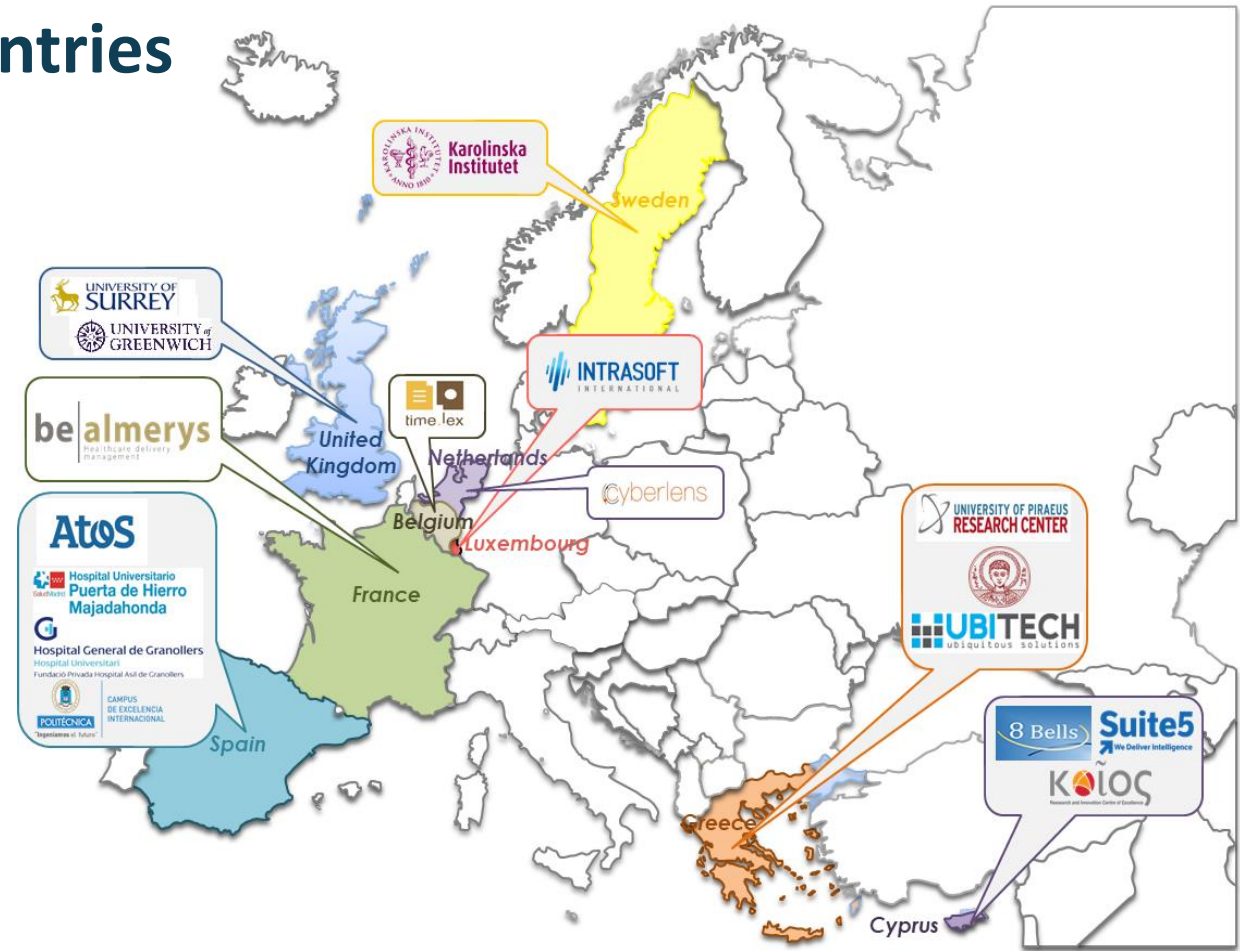


The Consortium

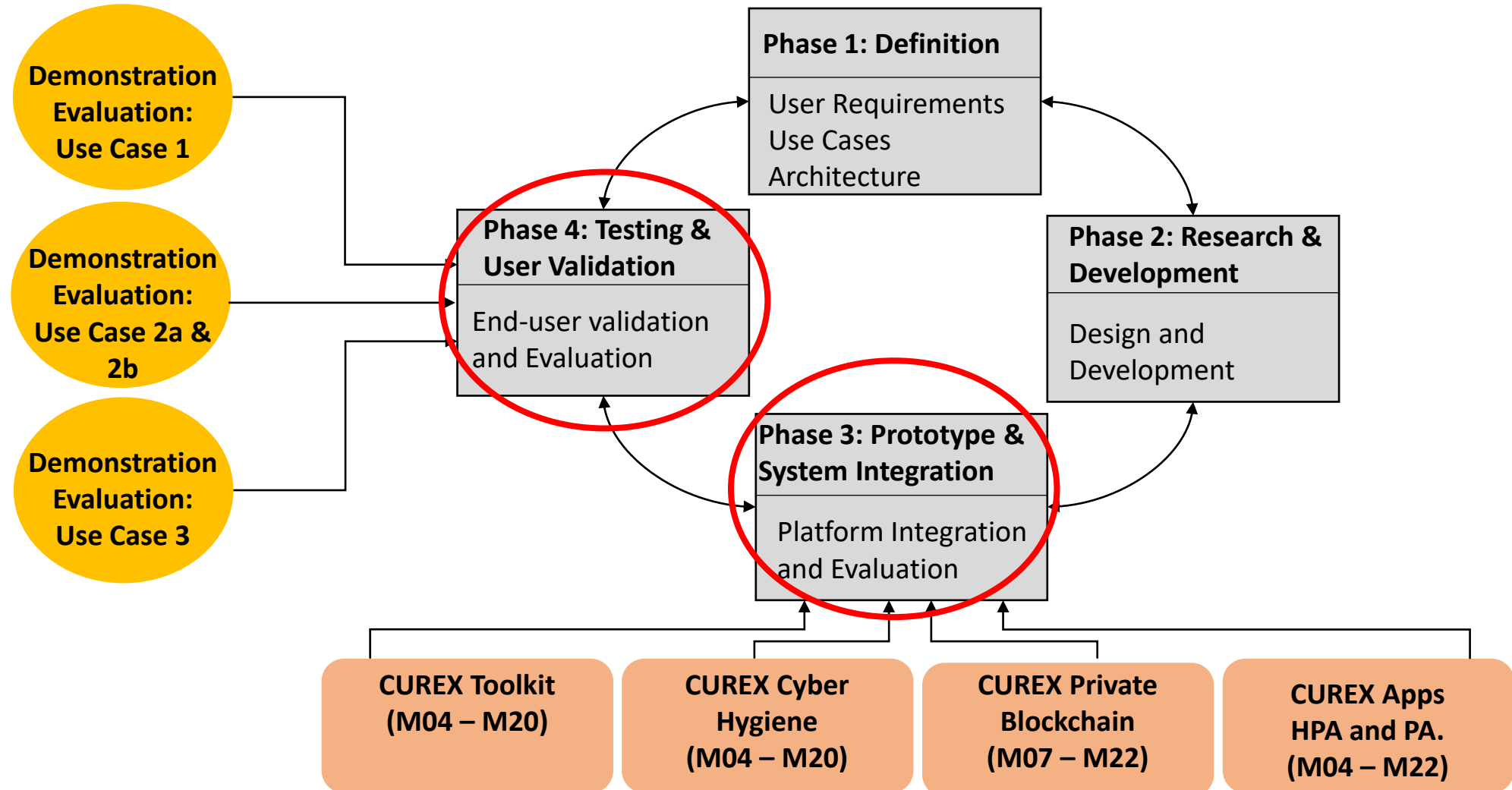
- **17 partners from 9 European countries**

- **2 x Large industries**
- **6 x Dynamic SMEs**
- **6 x Academic partners**
- **3 x End-users/representatives of healthcare industries**

www.curex-project.eu



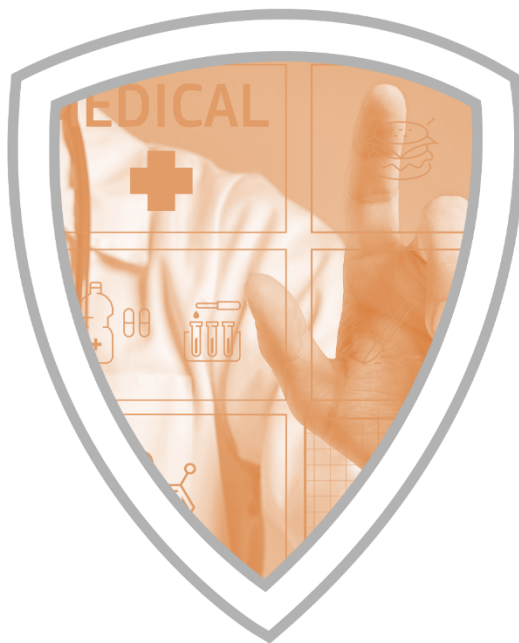
Current status





Use Case 1

**Data
exchange
for
cross-border
patient
mobility**



Use Case 2

**Data
exchange
in
remote
healthcare
services**



Use Case 3

**Data
exchange
for
healthcare
research**

(2a)

Risk Assessment for an
IoT Healthcare Platform

(2b)

Risk Assessment for a
Point of Care System

Digital Transformation

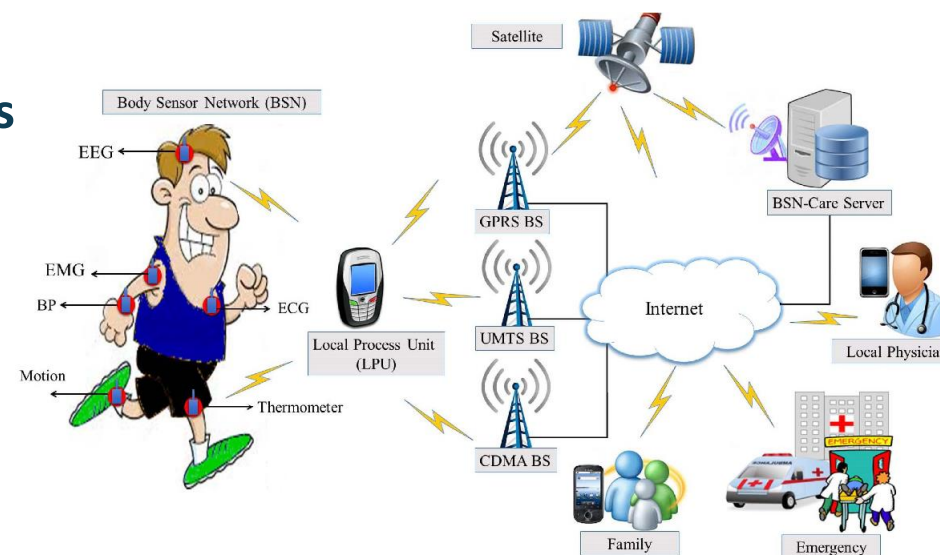
- A **challenge** to balance among **security, regulation** and **human welfare**
 - Electronic Health Records (EHRs) have replaced
 - ✓ **80 percent** of paper-based health records in established markets
 - ✓ **40 percent** in emerging markets
 - This fact raises new **risks, vulnerabilities** and **threats**.
 - But it is also a vehicle for **more secure** and **better healthcare** services




IBM X-Force. Security trends in the healthcare industry (2017)

Modern Healthcare

- Provides **patient-centered healthcare** services
 - Practitioners & patients' **mobility**
 - Usage of **personal & commercial medical devices**
 - Sharing **data** between **stakeholders** and **service providers**
- In such an evolving environment
 - There are **unknown vulnerabilities & new cyber-attacks**
 - **Secure-by-design** devices and services are required
 - A **risk-based approach** should be applied



Challenges in Health Data Exchange (1/2)

- **Health data exchange** takes place during the operation of healthcare services:
 - Within the same organisation (e.g. one clinic to another)
 - In a **cross-organisation** transaction
 - In **cross-border** situations
 - **Current & future healthcare services** will be highly dependent on:
 - **Massive exchange of data**
 - **Increased connectivity** between platforms, devices & organizations
- 



Challenges in Health Data Exchange (2/2)

- **Interconnections create a fairly large attack surface.**
 - Zero-day vulnerabilities
 - Advanced threats (APT)
- **Cyber-attacks targeting health data may:**
 - Put at risk both **patients'** **privacy** and **health**
 - Cause **severe operational disruptions**
 - Major economic losses for **healthcare organizations**
- **Strict legislation** creates additional obligations for organisations that operate on **clinical & medical data (e.g., GDPR).**



CUREX's aim is more relevant than ever

Fri, Apr 3, 2020

Healthcare Cyberattacks Increasing During COVID-19



by Kayla Matthews on May 21, 2020

The healthcare sector has long been a preferred industry for hackers to target. Now that many healthcare systems are under extra strain due to the COVID-19 pandemic, these cyberattacks could prove especially devastating.

Why Do Hackers Focus on the Medical Sector?

The COVID-19 Coronavirus and the Healthcare Sector – A Targeted Sector in Crisis Mode

COVID-19 pandemic spurs cyber-attacks on healthcare sector, says report

According to new research, as the healthcare and pharma sector relies on IT throughout the COVID-19 pandemic, cyber-attacks will be inevitable

By Victoria Rees (European Pharmaceutical Review)

21 April 2020

No comments yet

Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak

The hospital has one of the largest COVID-19 testing facilities in the Czech Republic.



Global Ransomware and Cyberattacks on Healthcare Spike during Pandemic

Liviu Arsene on May 13, 2020

COVID-19-themed cyber attacks hit healthcare bodies

April 15, 2020

INTERNET OF THINGS

MAY 26, 2020 / 8:46 AM / 2 MONTHS AGO

Red Cross urges halt to cyberattacks on healthcare sector amid COVID-19

Cyber-attacks on healthcare facilities 'growing threat' during coronavirus pandemic

Acronis believes it is likely cyber government agencies, healthcare professionals treating patients c

Temporary hospitals are rife with cybersecurity vulnerabilities

Ad hoc COVID-19 medical centers have a unique set of vulnerabilities: They're remote, they sit outside of a defense-in-depth architecture and the very nature of their purpose – care in a time of crisis – means security is a lower priority.

JUN 04 | MORE ON MEDICAL DEVICES

Number of cybersecurity attacks increases during COVID-19 crisis

Hackers are taking advantage of provider distraction to breach health systems.

Cyberattacks against medical, healthcare professionals persist, says Google

Laura Dyrda (Twitter) - Friday, May 29th, 2020 Print

3 JUNE 2020 ANALYSIS

Why are healthcare cyberattacks surging amid Covid-19

By Chloe Kent SHARE

A game of 'cat and mouse': Hacking attacks on hospitals for patient data increase during coronavirus pandemic

Cybercrime targeting healthcare organisations is soaring as a result of the global pandemic. What are the reasons behind this worrying surge, and what can businesses do to protect themselves?

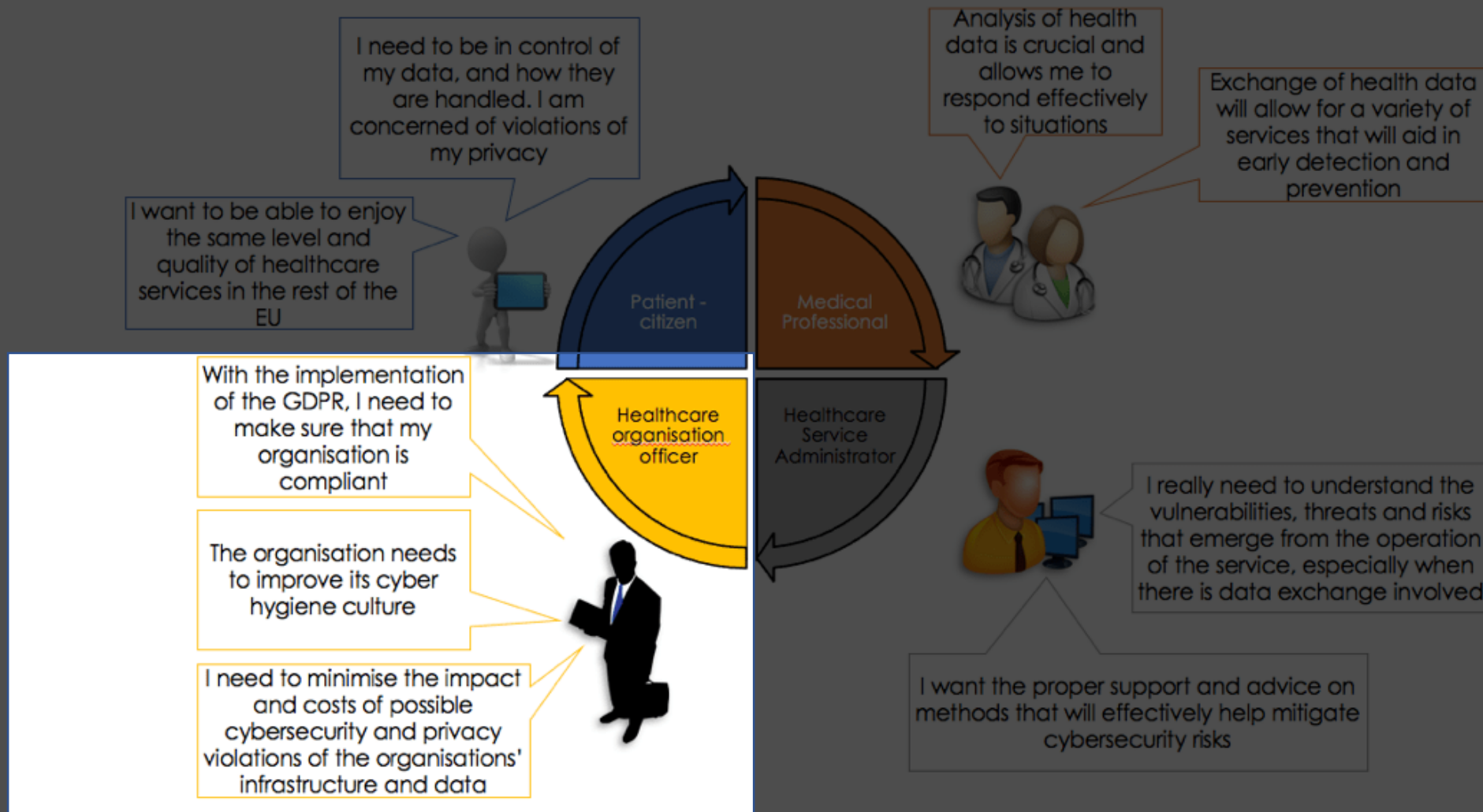
Foreign nation-state hackers are zeroing in on healthcare institutions, pharmaceutical companies and research facilities working on treatments for COVID-19, Ugoretz said. "We have also seen other actors, including nation states, scanning for vulnerabilities, conducting reconnaissance, conducting intrusions, and attempting to steal data from those U.S. universities and research institutions that are really focused on trying to deliver that research in response to the pandemic," she said.

Cyberattacks in healthcare up to steal COVID-19 treatment, vaccine research

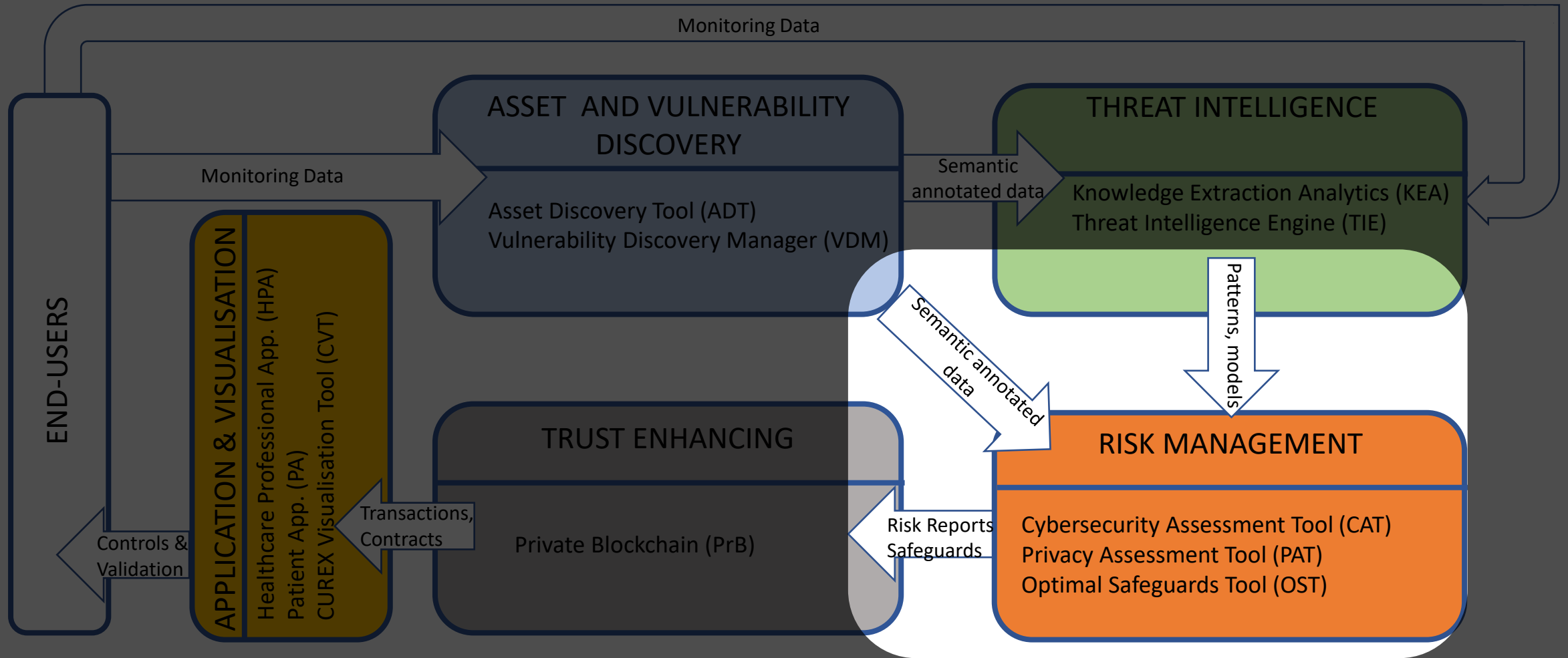
Laura Dyrda (Twitter) - Thursday, June 18th, 2020 Print



End User Requirements in Healthcare

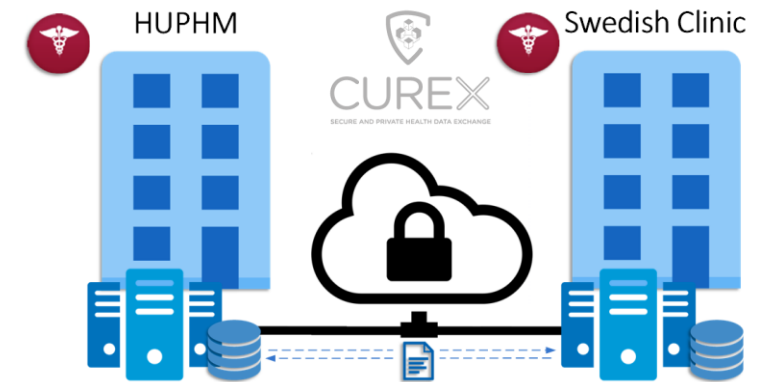


CUREX High Level View Architecture



Risk Management for Health Data Exchange

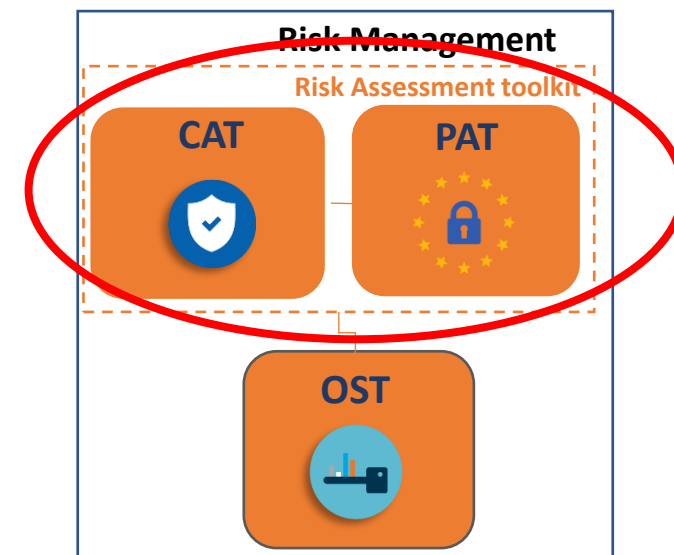
- The risk management in CUREX emphasizes on **the risks that are propagated all the way to the data** that is exchanged between hospitals and care centers.
- **Inherent risks** of a healthcare organisation **endanger the health data** that is shared with said organisation.
- **CUREX's** role is to **inform both parties about the risks posed** to each other's data, prior to the health data exchange.



The CUREX solution

■ Three main pillars and key project results:

- The delivery of the **cybersecurity and privacy risk assessment toolkit**.
 - ✓ Cybersecurity Assessment Tool (CAT) & Privacy Assessment Tool (PAT)
- The recommendations on **optimal safeguards** including their performance and budgetary constraints.
 - ✓ Optimal Safeguards Tool (OST)
- The creation of human-centric strategies and methodologies for raising **cybersecurity and privacy awareness** in a healthcare institution.
 - ✓ Cyber Hygiene



Cybersecurity and Privacy Risk Assessment Toolkit

- CUREX has created a **cybersecurity and privacy risk assessment toolkit** tailored for different types of healthcare organisation infrastructures and services.
- The toolkit is comprised of:
 - **Cybersecurity Assessment Tool (CAT)**, which assesses risks related to cybersecurity threats and vulnerabilities as modelled by the CUREX vulnerability discovery process and the threat intelligence functionality.
 - **Privacy Assessment Tool (PAT)**, which based on every business process that concerns the processing and exchange of data, assesses the degree of compliance of the healthcare organisation with the GDPR, by providing an indicative privacy score.



Cybersecurity Assessment Tool (CAT)

The **Cybersecurity Assessment Tool (CAT)** is a software component in charge of analysing data coming from multiple sources and assessing the risk level of an organization.

Real Time Evaluation



- Evaluation is performed **on demand** or **automatically** every time a change in the system is detected

Quantitative Risk Analysis



- Quantification of the risk caused by a **wide variety of threats** during data exchange
- R model used to obtain quantitative cyber security scores (i.e., **monetary values**)

Qualitative Risk Analysis



- Qualitative assessment of the risk based on the DEXi model (**low, medium, high**)
- Scores per organization, per risk model, and per asset

Risk Mitigation Measures



- Identification of existing and planned controls for **on-the-fly risk treatment**
- R model used to obtain quantitative cyber security scores (i.e., monetary values)

Blockchain Storage



- CAT scores are stored in the **CUREX Private Blockchain (PrB)**
- CAT and PAT scores are merged into a single score for CUREX for **cyber optics**

Visualization of Risk Scores



- Graphical interface to display CAT global and individual **scores**
- Connection with **CUREX Visualization Tool (CVT)** to display CAT results

Providing business impact values (qualitative and quantitative scores)

Determining potential cascading effects of cyber threats

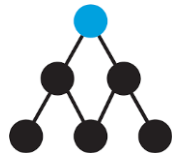
Suggest mitigation measures to reduce scores to acceptable levels

Decision Support tool

Privacy Assessment Tool (PAT)

The **Privacy Assessment Tool (PAT)** measures the **privacy level** of an organisation with the goal to support compliance with the GDPR for protecting patients' privacy.

Modeling Asset & Risk Interdependencies



- Graphical representation of **asset dependencies**
- Models vulnerable and privacy risky asset **paths**

Contributes to GDPR Compliance



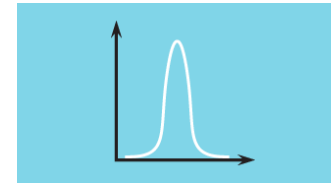
- Keeps track of personal and sensitive **data flows**
- Keeps track of the assets used to **process** personal and sensitive **data**
- Uncovers **risky data processing** activities due to vulnerable assets

Privacy impact scoring system



- Merges the **cybersecurity** impact with the **privacy** impact
- Assists organizations with **prioritizing** privacy risk **mitigation**

Privacy Quantification Engine



- The **criticality** of an identified vulnerability and the privacy impact assessment output is merged for quantifying the **privacy risk level**

Visualization of Risk Scores



- GDPR data flow reports, Global Privacy Risk, Asset Privacy Risk, Processing Activity Privacy Risk, Indicative statistics and reports
- Connection with CUREX Visualization Tool (CVT) to display PAT results

It performs privacy risk calculations

It can be used in combination with cyber risk assessment scores

Stores Privacy Risk Scores in the PrB

Challenges

- Both tools receive input from the vulnerability discovery process that takes place prior to the risk assessment.
- CAT also correlates this information with data coming from threat intelligence sources, both internal and external.
- The greatest challenge:
 - The closed nature of the healthcare domain due to its criticality, complexity and strict regulation, which disallows the information sharing between organizations and the community in general.
 - Repositories containing information specifically for software and hardware used in the domain are not currently widely available and care centers – especially public ones – are rarely in position to support proprietary cybersecurity solutions.





Thank you!

www.curex-project.eu

 www.facebook.com/CUREXH2020

 www.twitter.com/CUREX_H2020

 www.linkedin.com/in/CUREXH2020

Prof. Christos Xenakis

Eleni Veroni

University of Piraeus



This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404