Security and Privacy by Design for Health Care

Andrés Castillo - Haris Mouratidis
Paediatric Hospital Niño Jesús, Spain - University of Brighton, UK

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

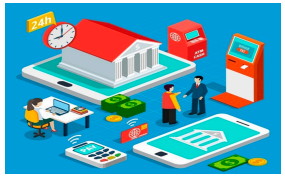
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787068.

University of Brighton
Centre for Secure, Intelligent and Usable Systems

DEFeND

AIM

Deliver an innovative data privacy governance platform, which facilitates scoping and processing of data and data breach management and supports organisations towards GDPR compliance.



OBJECTIVES

1. Design and development of a successful, **MARKET-ORIENTED, PLATFORM** to support organizations towards GDPR compliance
2. Develop a **MODULAR SOLUTION** that covers different aspects of the GDPR
3. **AUTOMATED** methods and techniques to elicit, map and **ANALYZE DATA** that organizations hold for individuals
4. Advanced modelling languages and methodologies for privacy-by-design and **DATA PROTECTION** management
5. Specification, management and enforcement of **PERSONAL DATA CONSENT**
6. Integrated **ENCRYPTION AND ANONYMIZATION** solutions for GDPR
7. **DEPLOYMENT** and **VALIDATION** of the DEFeND platform in real operational environments

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

Health Care Challenges

1

Tracking of changes and cancellation of consents

2

Management of health data for research;

3

Sharing of health data with other hospitals inside and outside EU (travellers, tourists, derivations);

4

Getting health data from sensors and wearables from patients at home into the hospital (telemedicine contexts);

5

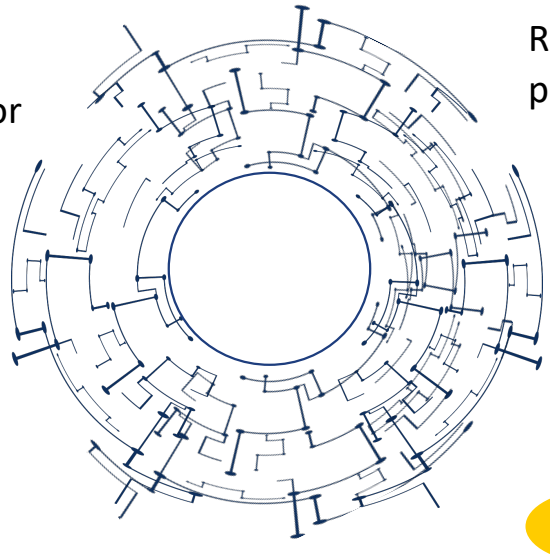
Transfer of health data to and from third parties to the hospital (e.g. labs, insurance);

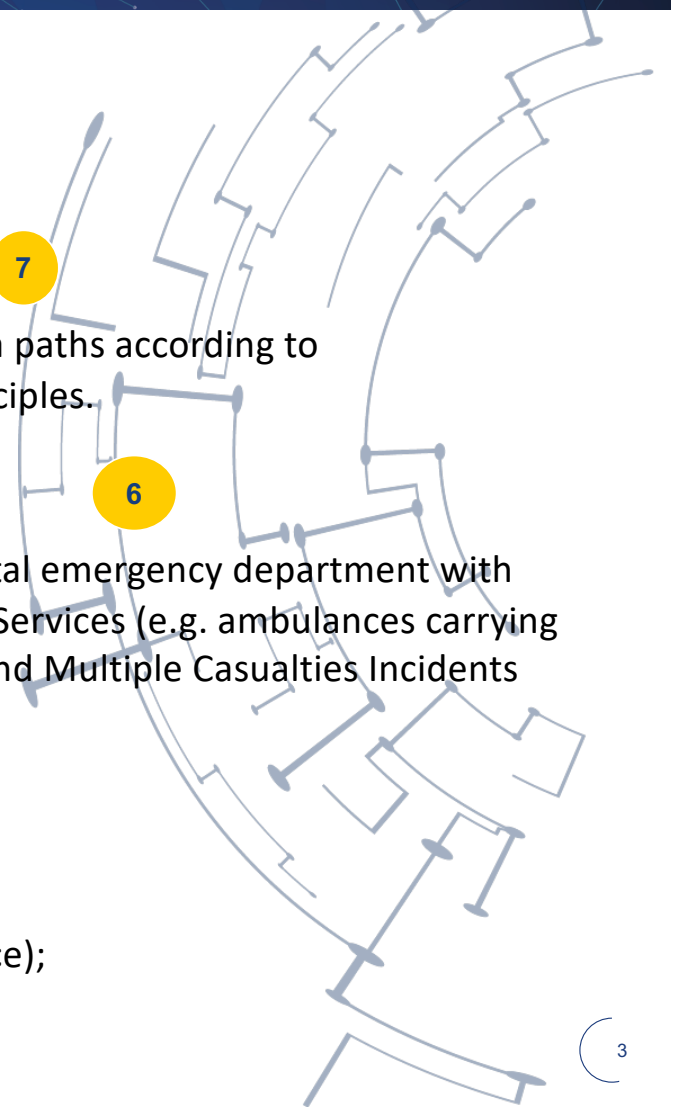
6

Connecting In-hospital emergency department with Emergency Medical Services (e.g. ambulances carrying COVID-19 patients and Multiple Casualties Incidents victims);

7

Redesign hospital data paths according to privacy by design principles.





DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

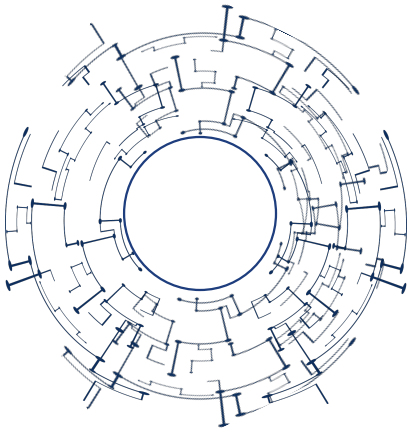
Technical Challenges

1

How can we transform privacy (social and legal concept, deliberately vague, contextual and subjective) to a technical requirement?

2

How can we derive technical requirements from GDPR?



5

What methods and techniques we need to build systems that support continuous GDPR compliance

3

How can we deal with conflicts between privacy and other concepts?

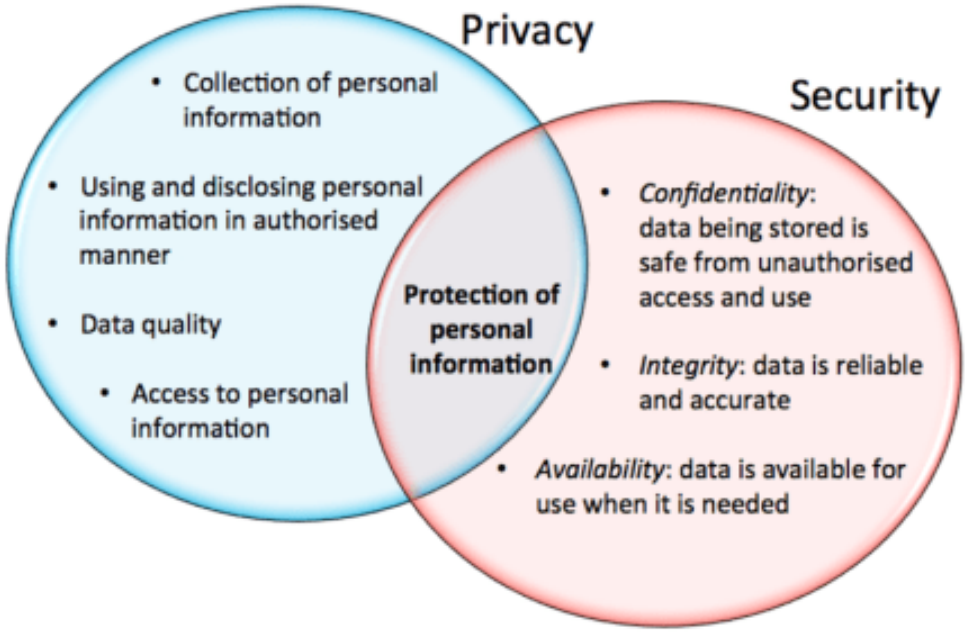
4

What is the relationship between privacy and security in that context?

DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

Security vs Privacy

- Security proposals balance tangible harms
- Privacy proposals protect intangible harms that an intrusion on privacy would cause
- Implementation level: Interconnection between them
  - Security mechanisms are used as the basis for privacy implementation
- Requirements level: often there is conflict
  - Security requirements might conflict privacy requirements



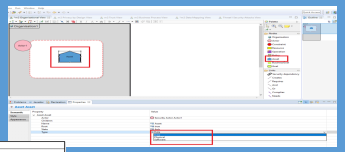
DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

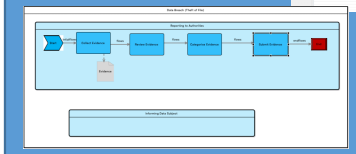
DEFeND Security and Privacy by Design

Data Assessment Model

SbD/PbD

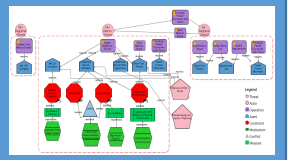
Requirements





Threats

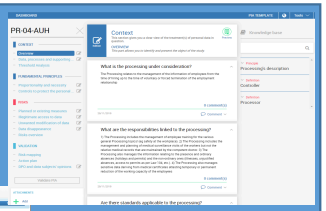
Privacy/Security Properties/Controls

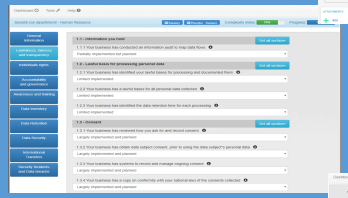


Data Privacy/Security Model

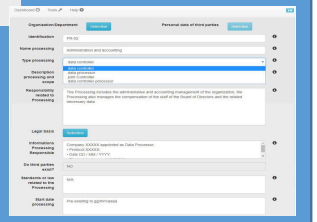
Elicitation

Privacy Impact Assessments





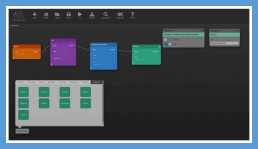
Organisational Questionnaires

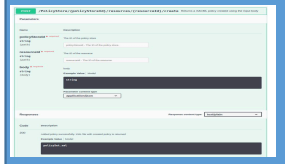


Processing Activities and Data

Implementation

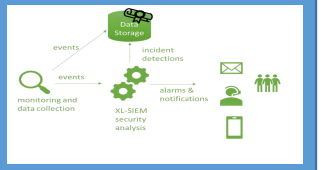
Privacy Controls Implementation





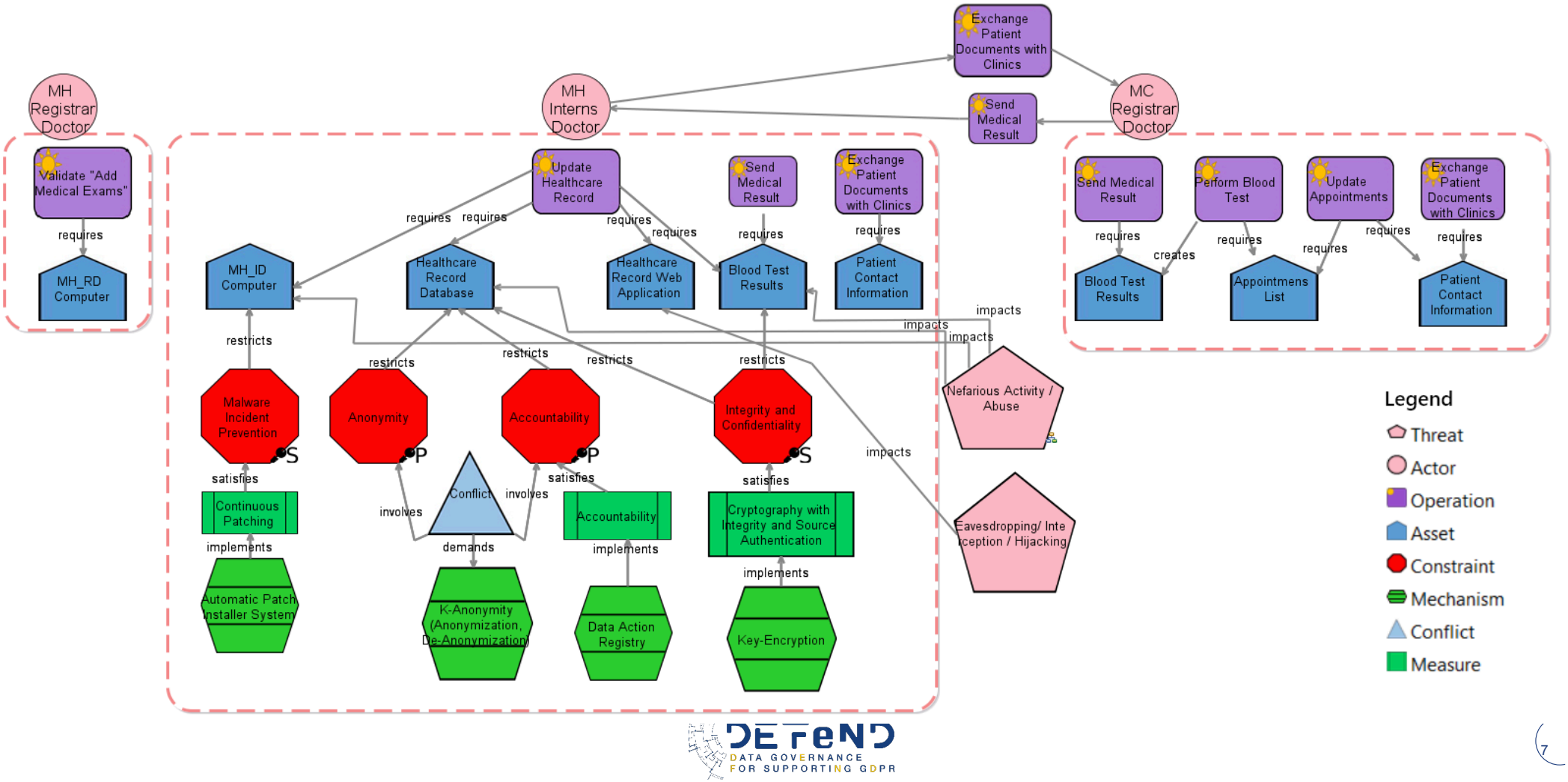
Security control Implementation

Management



DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

SbD/PbD Modelling Language



DEFeND
DATA GOVERNANCE FOR SUPPORTING GDPR

THANK YOU

DEFeND

DATA GOVERNANCE FOR SUPPORTING GDPR

More info:

Haris Mouratidis, UoB,

H.Mouratidis@brighton.ac.uk

info@defend.eu | www.defendproject.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme *under grant agreement No 787068.*