

Towards Privacy by Design in Personal e-Health Systems

George Drosatos¹,
Pavlos S. Efraimidis², Garrath Williams³ and Eleni Kaldoudi¹

¹School of Medicine, Democritus University of Thrace, Greece

²Dept. of Electric and Computer Engineering, Democritus University of Thrace, Greece

³University of Lancaster, UK

First step towards privacy by design

- Analyze the personal e-Health systems
 - ↳ *Modeling their functionalities*
- Identify the arising privacy issues
 - ↳ *Based on modeled system's functionality*
- Present some possible privacy-enhancing techniques
 - ↳ *e.g. encryption, anonymization, pseudonyms ...*

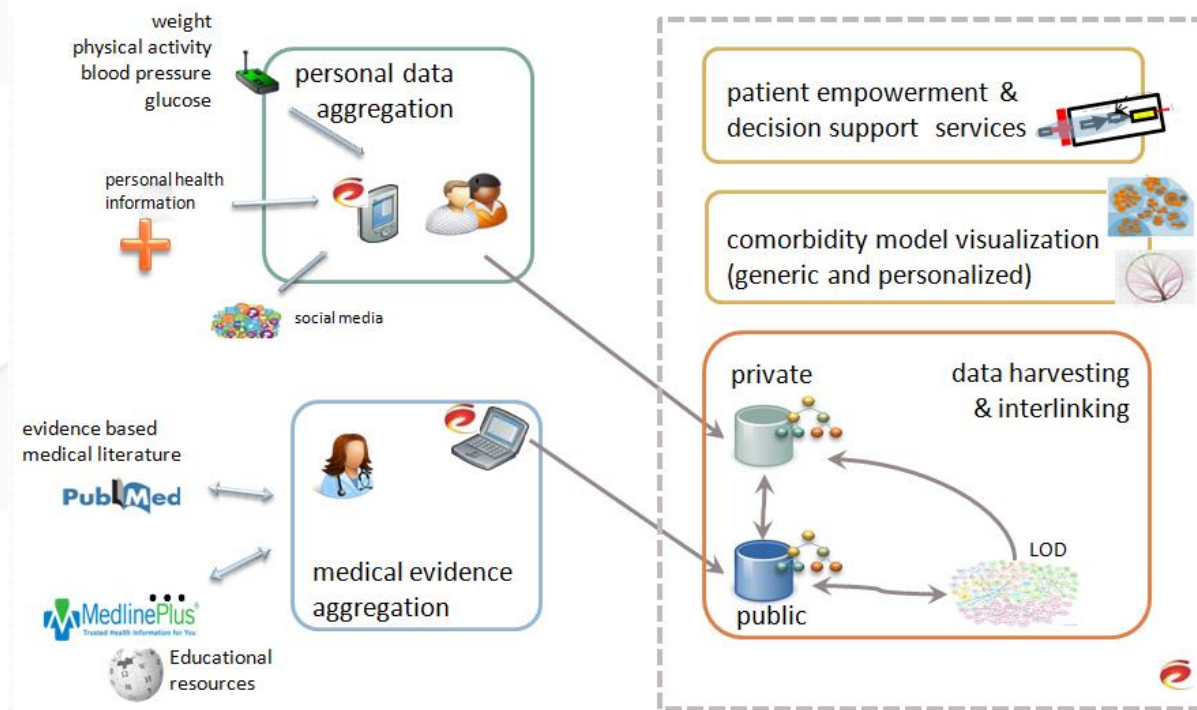
Next steps:

- ↳ Develop a methodology for engineering privacy
- ↳ Organize practical guidelines

CARRE Project

<https://www.carre-project.eu>

- It is a **EU** co-funded project in the area of **cardiorenal** with focus to provide **personalized health**
- **Personal data**: Sensor data (e.g. activity and blood pressure), PHR and patient's intentions (travel, diet, diseases, etc)



Privacy principles and concerns

Privacy \equiv The right to informational self-determination

↪ *Individual consent*

↪ *Individual control*

Privacy **concerns**:

↪ *User identification*

↪ *Personal data leakage*

Privacy **principles**:

↪ *Data minimization*

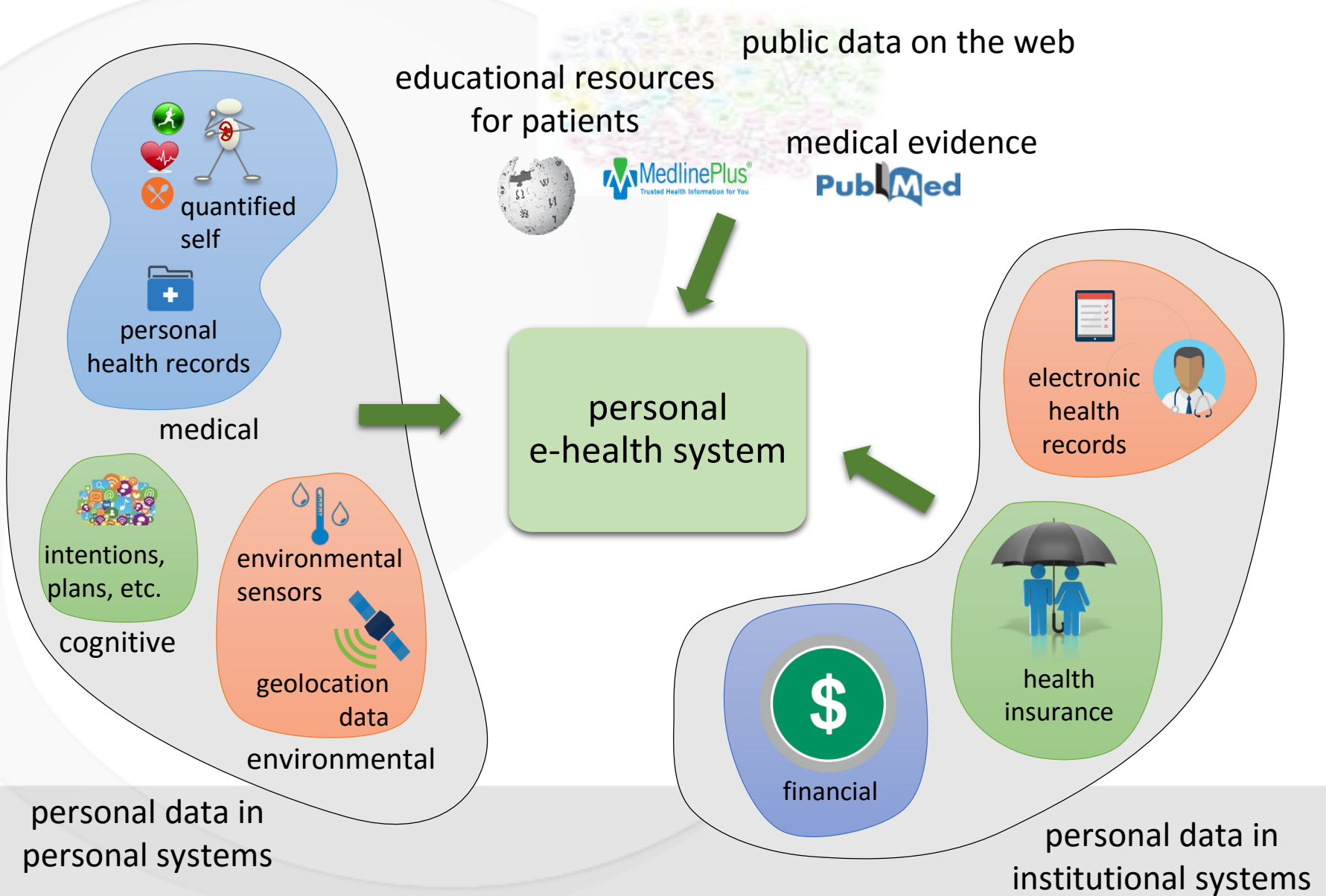
↪ *Data protection by design*

↪ *Data protection by default*

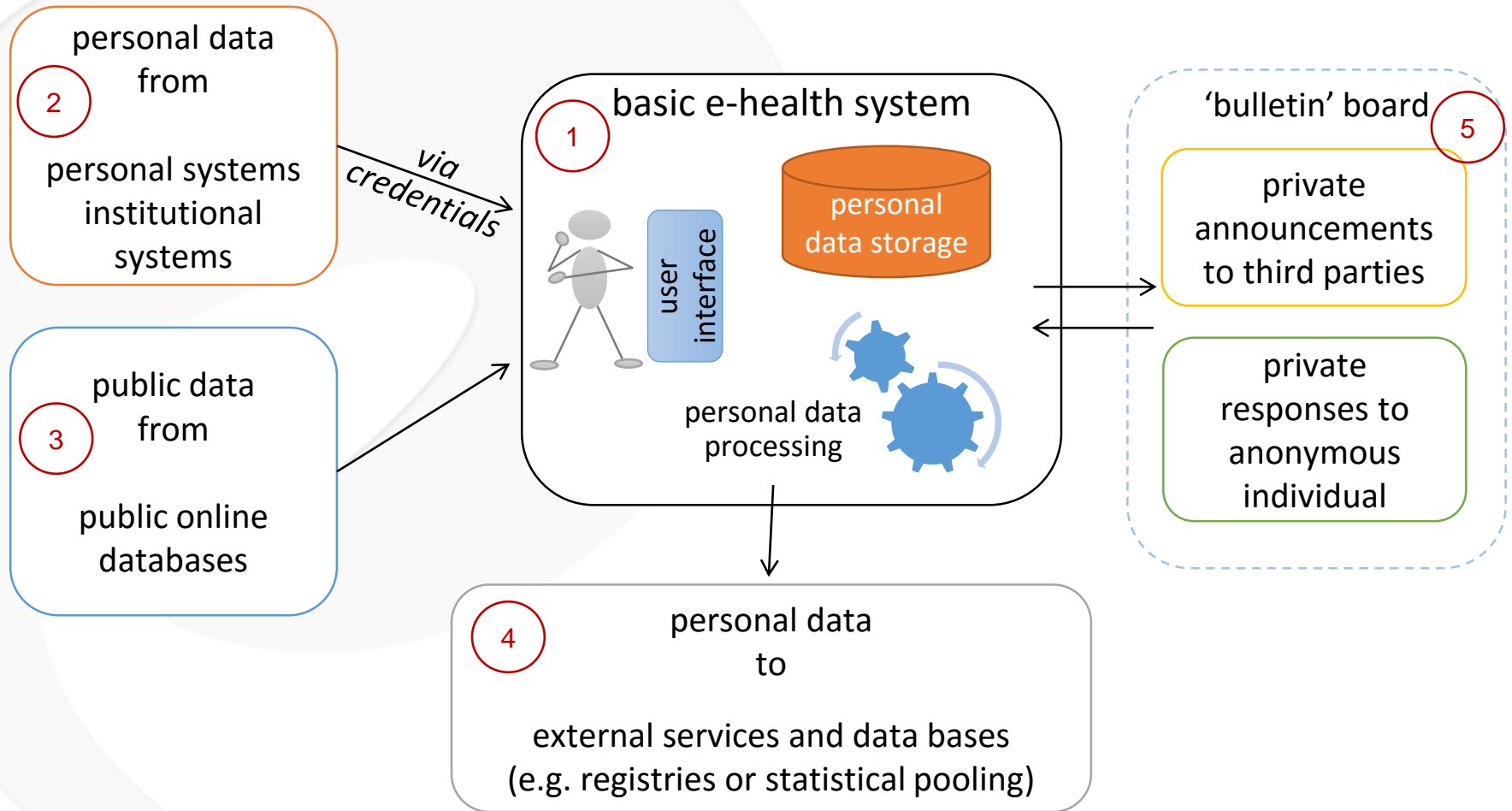
1. Directive 95/46/EC. In Official Journal L 281, 0031-0050 (1995)

2. Green Paper on Mobile Health (“mHealth”) (SWD(2014) 135 Final)

Data requirements for a personal e-Health system



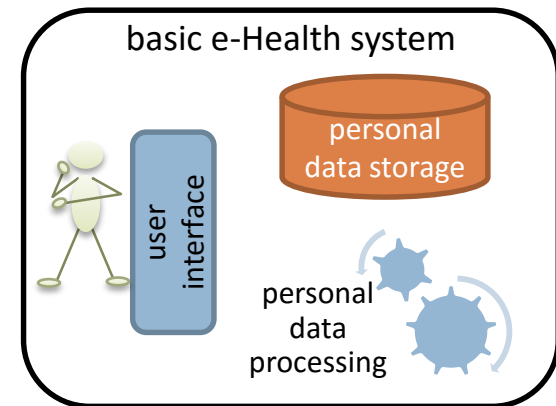
Basic personal e-Health systems functionalities



(1) Personal data storage and processing

Privacy issues arise when these operations happens on remote service

- Countermeasures of data storage:
 - ↪ Cryptographic techniques
- Countermeasures of processing:
 - ↪ There is not general solution
 - ↪ Processing in encrypted data require a lot of assumptions
 - Pre-processing before encryption
 - Computational cost
 - Not possible to be applied to all cases



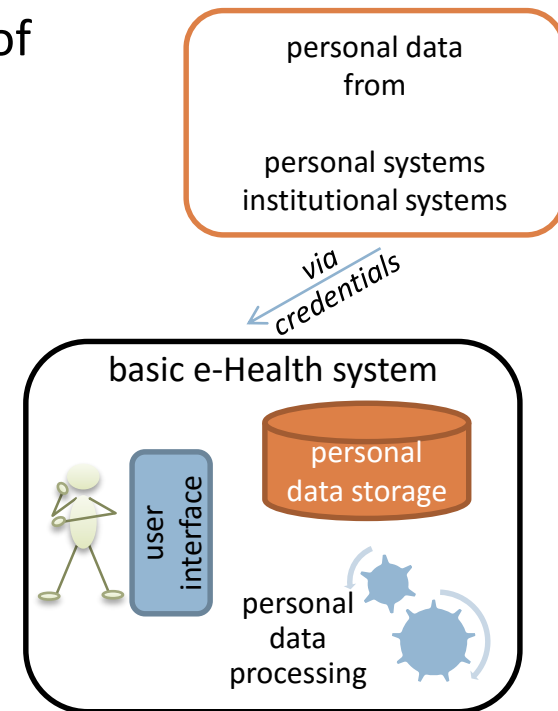
(2) Personal data exchange with 3rd party systems

– Privacy issues:

- ↪ Linkability among the different user's accounts
- ↪ Linkability with the physical person (in case of interaction with institutional systems)
- ↪ Increase privacy concerns when combine partial personal data together

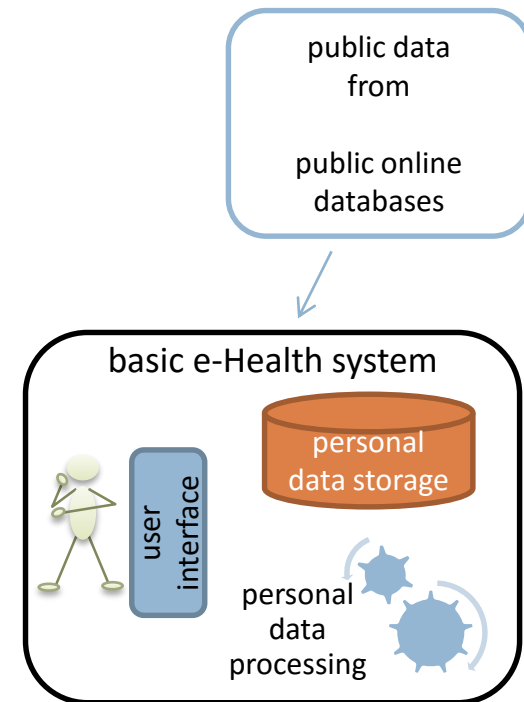
– Countermeasures:

- ↪ There is not direct measures to this problem
- ↪ An obvious solution involves building dedicated middleware in the user-side that will act as a proxy for all personal systems



(3) Integration of personalized public data

- **Privacy issues:**
 - ↪ Linking particular public data to specific user
 - ↪ Revealing the user's needs to public service
- **Countermeasures:**
 - ↪ Altering (expanding or generalizing) the initial request
 - ↪ Cooperation of a group of users in the system to conceal one another's requests
 - ↪ Using anonymous network technologies (such as TOR)



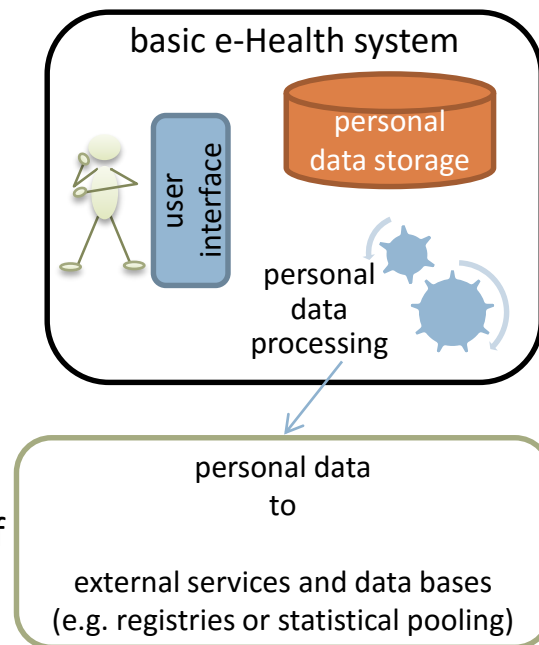
(4) Exporting personal data for public use

– Privacy issues:

- ↪ **Medical registries:** User identification of ‘critical mass’ of pooled anonymized personal data
- ↪ **Statistical data pooling:** User identification if number of participants is small

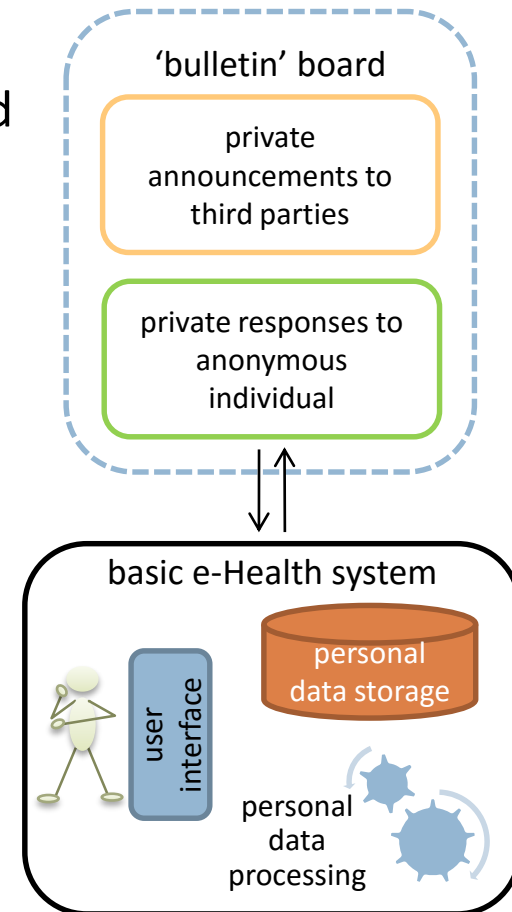
– Countermeasures:

- ↪ **Medical registries:** Minimizing and stripping all the identifiable parts
- ↪ **Statistical data pooling:**
 - Privacy preserving cryptographic techniques
 - The appropriate technique depends on the location of storage and the form of statistical processing



(5) Exchange of private personal data messages

- **Privacy issues:**
 - ↪ Conceal the user's identity from the system and (selectively) from the receiver of the message
 - ↪ Conceal the actual message from the system
- **Countermeasures:**
 - ↪ Anonymous credential techniques
 - ↪ Cryptographic techniques
 - ↪ Unlinkably exchanging messages



Conclusions & Next steps

- **Analyze** the personal e-Health systems, **identify** the arising privacy issues and **present** some possible privacy-enhancing techniques
- Based on the arising privacy issues and propose possible countermeasures
 - ↪ Develop a methodology for engineering privacy and present practical guidelines
 - ↪ Apply the developed methodology to CARRE

Acknowledgement



This work was supported by the FP7-ICT project CARRE (No. **611140**), co-funded by the **European Commission**.



CARRE Project: Personalized patient empowerment and shared decision support for cardiorenal disease and comorbidities.