Pseudonymization of Information for Privacy in E-Health (PIPE)

A Min Tjoa
TU Wien
& SBA

One side of Privacy

„No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence nor to unlawful attacks on his honor and reputation“

„Everyone has the right to the protection of the law against such interference or attacks“

(Universal Declaration of Human Rights, 1948)

The other side of Privacy

- Telekom: „Data from 17 million customers stolen” (Die Zeit, 04.10.08)
- „Soupnazi stole data relating to 170M credit cards”, (derStandard, 18.08.09)
- The National Health Service (GB): The unencrypted medical histories of 2,300 cancer patients were compromised (The Independent, 25.05.09)

Motivation – A Medical Scenario

- Symptoms of weakness, fatigue, weakness, severe shortness of breath,congestion and cough
- Lung X-Ray shows congestion in lung
- Echocardiogramm rules out chronic obstructive pulmonary disease and congenial heart disease
  The diagnosis is **acute bronchitis**
- **Statistical Analayis** of echocardiogram reveals right side of heart enlarged, left side reduced – **only apparent when compared to hundreds of other echocardiograms**
- **Statistical Analysis** suggests **primary pulmonary hypertension (PPH) –** the only right diagnosis

www.wrongdiagnosis.com/p/primary_plumonary_hypertension/intro1.htm

Cited by Laura Haas, IBM Director Computer Science Research [2009]

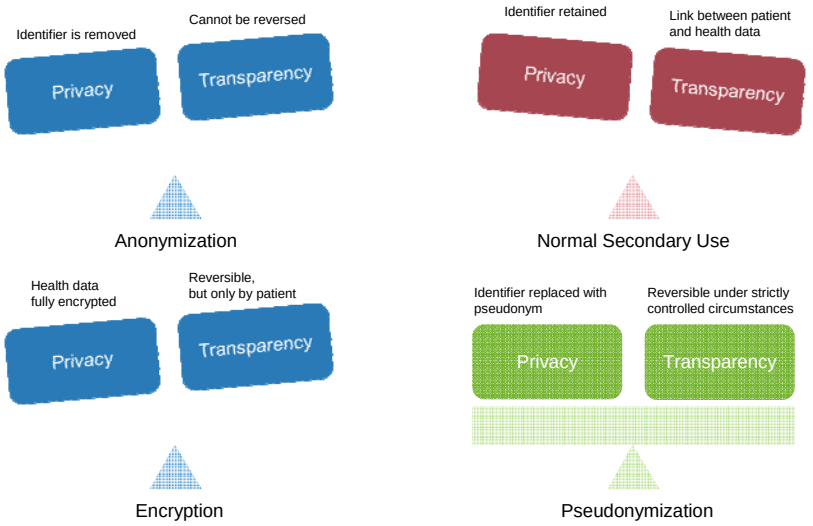
Motivation - Personalized Medicine

- Gathering knowledge of impact of lifestyle and genetic factors
- Application of therapy-planning not in a trial and error way

Three Pillars of Privacy

- **Regulation/Legislation, e.g.,**
  - Health Insurance Portability and Accountability Act (HIPAA)
  - European Directive 95/46/EC
  - Data Protection Act
  - Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom
- **Self Regulation , e.g.,**
  - TRUSTe
  - TÜV
- **Privacy Enhancing Technologies (PET)**

Approaches for protecting patients‘ privacy



The need for pseudonymization

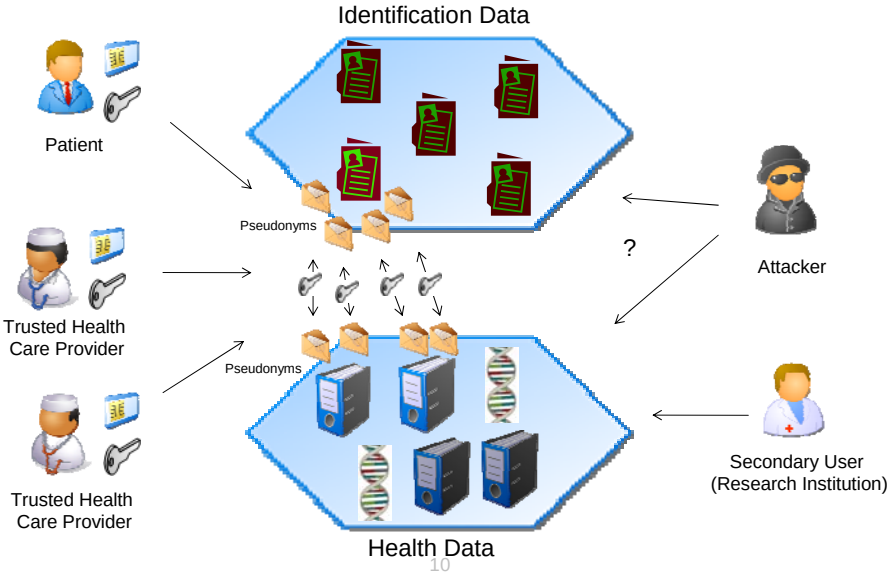
- Patients and commissioners for data protection have legitimate concerns about privacy and confidentiality of the stored medical (esp. genomic) data.

Genomic data clearly identifies a person.

The PIPE Approach

- The PIPE approach is a pseudonymization approach based on cryptographic operations.
- Data is divided into personal data and pseudonymized medical data.
- Access is handled with smartcards (e.g., ecard).
- Patient as data owner may grant data access authorizations to trusted relatives and health care providers.
- An operator-principle acts as a secure fall-back mechanism for lost or destroyed smartcards.

The PIPE Approach



FIT-IT Project PIPE 1/2

The aim of this project is

- (a) to broaden the PIPE approach to support **(semi-) structured meta data**,
  - we need to ensure that the storage structure does not reveal any association between meta data and patients or health care providers.
  - patients and health care providers should be able to query meta data to efficiently search within medical records.
- (b) to develop **alternative secure storage and retrieval** techniques,
  - Exísting approaches have been determined to be insecure or raise performance problems with smart cards.
  - We reduce processing needs at the client by developing dedicated rather than general purpose storage and query techniques.

FIT-IT Project PIPE 2/2

The aim of this project is

- (c) to provide a **secure viewer** that prevents man-in-the-middle attacks,
  - The authorization mechanism has to guarantee that only trusted person are granted access to the patient's health data.
- (d) to demonstrate our system in the context of **genome analysis**, storage, and retrieval.
  - As genomic data per se identifies a person, anonymization is not enough to guarantee privacy.
  - Case studies in the area of genomic data serve a basis for the extension to the application to hospital information systems or electronic health records.

Security Issues – Principal Idea

- Minimize (Optimize) the size of the Trusted Computing Base (TCB) to decrease the number of possible attackers
- Distribute trust amongst multiple parties to enforce collusion
  (Most intruders act alone)

Security Issues

E-health systems demand the holistic consideration of security.

- System level, e.g.,
  - Malicious Code
  - Social Engineering
- Database level, e.g.,
  - Logging Attack
  - Database Theft
- Communication level
  - Replay Attacks
  - Man-in-the Middle Attacks

Challenges

- The public health sector deals with many important but complex issues such as integrating legacy systems, guaranteeing the security of data and robustness of workflow processes as well as political issues with many different parties and interests.

- Therefore, one of the main challenges currently and in the future is and will be to integrate as many stakeholders as possible into the technical discussions to create commonly accepted approaches and concepts.
- The consideration of security issues is fundamental precondition for the acceptance and, thus, the success of e-health systems.