Improving Patients Privacy with Pseudonymization

MIE 2008

Thomas Neubauer
Secure Business Austria
A-1040 Vienna
Introduction

• The health care sector is at a crossroads. Aging and very expensive programs put more and more pressure on the health care systems.
  – 9% of gross domestic product (GDP) in Europe, US 15%
  – growing at 6% p.a., faster than the GDP

• Increase in the need for electronic healthcare records. The EHR promises to …
  – reduce costs and time necessary for handling medical data,
  – reduce the number of adverse drug events,
  – improve the quality of clinical trials.

• Patients and commissioners for data protection have legitimate concerns about privacy and confidentiality of the stored medical data.

• It is the patient’s right to demand privacy (HIPAA, EC Directives,..)
Existing approaches

- **are based on encryption**, which is too time-consuming for medical images (x-ray = 6 MB, mammogram = 24 MB, computer tomography = several hundreds of MB)

- **are based on pseudonymization**, but rely on weak security, e.g.
  - a centralized patient list for re-identification,
  - a reversible algorithm with secrets kept inside the system

- Pseudonymization is an approach that provides a form of traceable anonymity. The association between patient’s data and their medical data can only be accomplished under specified and controlled circumstances.
Trade Off

- **Privacy**
  - Classified attributes are removed
  - Identifier is removed

- **Transparency**
  - Difficult reversal of data
  - No reversal of data

- **Depersonalization**
  - Identifier is replaced with pseudonym
  - Not applied

- **Privacy**
  - Reversible under strictly controlled conditions
  - Direct link between data and identifier

- **Transparency**
  - Normal Secondary Use
  - Normal Secondary Use
We have developed a new approach for the pseudonymization of medical data.

We have introduced this approach in some previous publications [Riedl/Neubauer2007].

This approach is already patented in Austria and we also made an international /US patent application.

Based on a hull architecture. The user has to know the secret of one hull to get access to the next inner hull.
PIPE Architecture

Outer Hull authentication layer

Inner Hull user permissions layer

Concealed Data (CD)

Relative (B)
- dB
- eB

KB
- d'B
- e'B

Patient (A)
- d'A
- e'A

KA

Health Care Provider (C)
- dC
- eC

Operator 2 (O)
- d'O2
- e'O2

Operator 1 (O)
- d'O1
- e'O1

PSN

PSN

PSN

NC

MIE 2008, S. Fenz
In the outer hull every user owns a smart cards.

This smart cards contains the users outer asymmetric key pair.

Another key pair in the inner hull and symmetric key.

The public key of the outer key pair is used for encrypting the users inner private key. The users inner public key is used to encrypt the user symmetric key.

The symmetric key provides access to the pseudonym and the pseudonymized datasets.
Further Work

- Implement the system in medical environments
- Conduct case studies
- Implement standards (e.g., DICOM, HL7)