Security challenges and technical solutions in the domain of remote patient monitoring

Prof. Dr. Milan Petković
Philips Research
Eindhoven University of Technology
Toulouse, 7 et 8 juin 2010
Outline

• Importance of security and privacy
• Security and privacy requirements
  • Ethics, legislation
  • Technical requirements
• Detailed explanation of security issues in remote patient monitoring
• Technology solutions
  • Confidentiality and privacy
  • Authenticity and trustworthiness
• Conclusions
Health Net of Connecticut sued for failing to secure patient health records and financial information of nearly 446,000 plan members.

A portable computer disk drive with unencrypted information disappeared from Health Net's Shelton office.
The incident in question occurred when a disgruntled **ex-staff member** involved in a dispute with a supervisor decided to draw attention to a poorly secured internal Kaiser web site...
Mistakes in the delivery of Healthcare

- 44,000 to 98,000 people die in USA hospitals each year as result of medical errors
- 800,000 (6.1%) people in the Netherlands had wrong medical treatment - “Fouten worden duur betaald”
  - Financial effect – euro 1.4 billion
- Main reasons: availability and correctness of medical record
Security and privacy issues

- Security/privacy breaches
  - lost/stolen portable devices
  - insider attacks
  - broken security mechanisms
  - viruses…
- Related to the consumers
  - privacy preferences
  - usage/purpose control
- Related to service providers and consumer safety
  - authenticity
  - trustworthiness…
Consumer/patient rights

- Fundamental ethical requirements for confidentiality of medical data
- Legislation: EU Directive 95/46/EC, HIPAA, etc.
  - use limitation principle: personal data should not be disclosed, made available or used for **purposes** other than those specified
  - on the basis of the consent of the person concerned
  - right of access to data that has been collected
  - right to know who is accessing collected data
  - right to make **exceptions** wrt the ones that can access data
Requirements

• Confidentiality
• Integrity
• Authenticity
• Availability
• Access
• Reliability

…but also…

• Purpose control
• Usage control
• Disclosure control…
Internet of Things setting

• From the ‘walled fortress’
  – physical isolation (paper-based documentation in closed bookshelves)
  – physical security measures to defend data and systems
  – Security as a protection measure

• To the ‘open metropolis’
  – open, interconnected, interoperable
  – sharing EHR data and resources
  – security and trust as an enabler
Specific issues in the Home Healthcare domain

- Wrong user
- Incorrect use of devices
- No control on disclosure
- Unauthorized modification
- Unauthorized access/use

- PHR/EHR Storage server
- Disease management service
- Not authentic, uncalibrated device
- Observation devices

Patient

Doctor
Technology solutions

• Confidentiality and privacy
• Authenticity and trustworthiness
Technology solutions

• Confidentiality and privacy
• Authenticity and trustworthiness
Data sharing

- Patient/consumer
- PHR storage server
- Consumer privacy preferences
- Doctor
- Nurse
Information-centric protection

Patient/consumer

Doctor

Nurse

PHR/EHR Storage Server

Consumer privacy preferences

Medical system
Ciphertext-policy attribute based encryption

Patient/consumer

Doctor OR (Nurse AND Psychiatry)

Encrypt

Storage server

PK
MSK

Key authority

1 OR (0 AND 0)=1
0 OR (1 AND 0)=0

SK_{Alice}
Attributes:
Doctor, Cardio,

SK_{Bob}
Attributes:
Nurse, Radiology, MMC

1
Technical solutions

- Attribute-based encryption scheme supporting
  - Policy update
  - User/attribute revocation
  - Attribute-based signatures

REFERENCES
- Luan Ibraimi, Milan Petković, Muhammad Asim, An Encryption Scheme For a Secure Access Policy Updating, Secrypt 2010
Technology solutions

• Confidentiality and privacy
• Authenticity and trustworthiness
Combined patient and device authentication

Biometric authentication

Data + SigK

Home Hub

Bob - K

Data + SigK

MD1

Bob

MD1

Telehealth record

GP Record

REFERENCE


Jorge Guajardo, Muhammad Asim, and Milan Petković, Towards Reliable Remote Healthcare Applications Using Combined Fuzzy Extraction, LNCS, Dagstuhl, 2010
Quality Indication

Qualifiers (quality indicators)

Home Hub

Data + Quality indication
80/120

GP Record

Patient reputation

What do we achieve:
1. Cost reduction
2. Error reduction
How to calculate trust?

REFERENCES
• Ton van Deursen, Paul Koster, Milan Petković, “Reliable Personal Health Records” Medical Informatics Europe (MIE), published in eHealth Beyond the Horizon – Get IT There, IOS Press, 2008, pp.484-489.
Conclusions

• To get Remote Patient Monitoring right you better pay attention to security and privacy!

Further reading:
• Book: Security Privacy and Trust in Modern Data Management
Motivation
Objectives
Topics of Interest
Paper Submission
Important Dates
Organizing Committee
Program Committee

SDM 2010 (Call for papers – deadline May 31)