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

Healthcare IT News
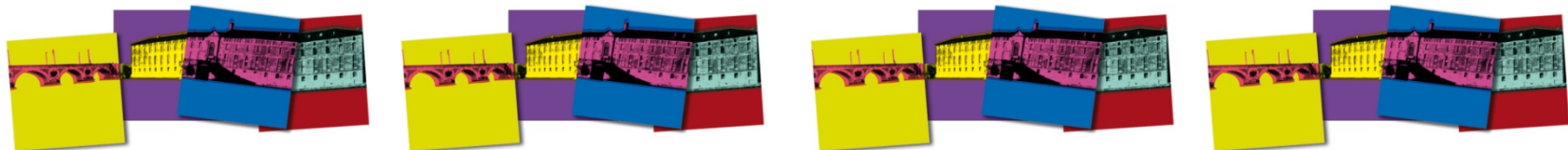
Home » News » Industry News

CONNECTICUT AG SUES HEALTH NET OVER SECURITY BREACH   E-mail to a Friend   Print

Connecticut AG sues Health Net over security breach

January 13, 2010 | Bernie Monegain, Editor

HARTFORD, CT – Connecticut Attorney General Richard Blumenthal has filed a lawsuit against Health Net of Connecticut, alleging patient medical records and financial information pric

Health Net of Connecticut sued for failing to secure patient health records and financial information of nearly **446,000** plan members.

Blumenthal filed the suit on Wednesday, calling it "hi asserts that Health Net failed to promptly notify consumers endangered by the security breach, which involved 446,000 Connecticut enrollees.

A portable computer disk drive with **unencrypted** information disappeared from Health Net's Shelton office.

centers

capital management

The lawsuit also names UnitedHealth Groupm Inc. and Oxford Health Plans,

rites   Tools   Help

anente fined $200,000 in security breach ...

…one sent straight to your inbox! Join over 90,000 healthcare pros who subscribe to FierceHealthcare for FREE!

Enter email   Sign me up

health and well-being all in one place.

◄ rollover to discover more

GetInsideHea

Philips' exclusive guide to Health and Well-

Kaiser Permanente fined $200,000 in security breach

June 2., ..5   8:01pm ET

California's Department of Managed Health Care fined Kaiser Permanente $200,000 for allowing the confidential personal information of 150 of its patients to be published on the Internet. The fine is one of the largest yet assessed to a health care provider for an error involving privacy rules. The incident in question occurred when a disgruntled ex-staff member involved in a dispute with a supe... decided to draw attention to a poorly se...... ...iser web site.

TOOLS

✉ Email
🖨 Print
☞ Contact Author
Reprint
b Buzz up!
Digg
Reddit

TAGS

Department of Justice (DOJ)

Kaiser Permanente

MOST POPULAR STORIES

Most Read | Most Emailed

Lilly exec will explore links to industry at Harvard

Furor, demand for answers, spreads over rising healthcare premiums

'Stories of Success!' highlight 16 organizations us HIT to improve quality

UnitedHealthcare's cancer protocol reports essent 'policing' docs

Mass. governor wants veto power over most medi rates

WellPoint's Angela Braly CEO Compensation

…ed Drivers up to 20%.

…sta del Sol Fast Quote

…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…

- see this story from the San Jose Mercury News (reg. req.)

Internet

nbox - Microsoft... | Usecases | HL7 Track | Inbox - Outlook ... | 2010 Belgrade C... | Kaiser Permanen... | HITRUST : News... | Microsoft Power... | PowerPoint Slide... | Microsoft Active...

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
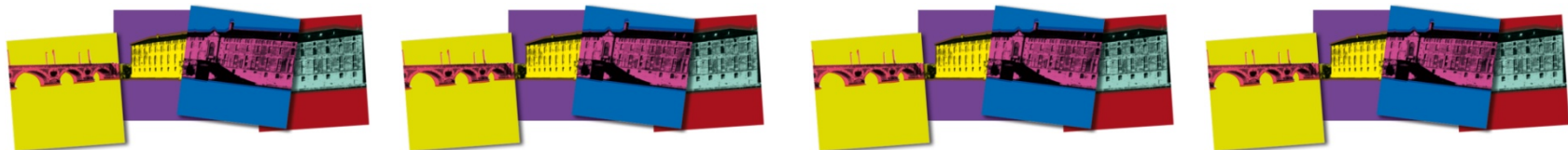 - right to make **exceptions** wrt the ones that can access data

Requirements

- **C**onfidentiality
- **I**ntegrity
- **A**uthenticity
- 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

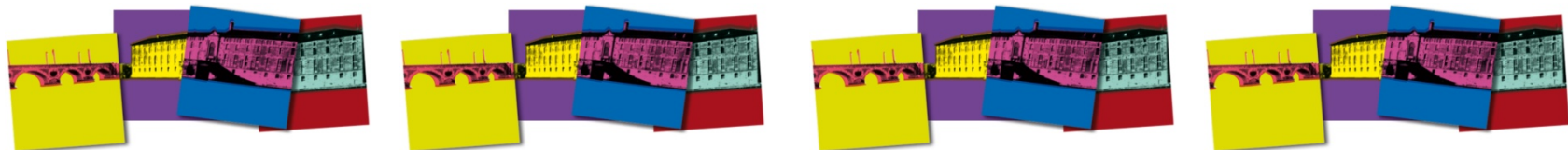 - security and trust as an enabler

HACKER

Health data

Specific issues in the Home Healthcare domain

Wrong user

Incorrect use of devices

No control on disclosure

Unauthorized modification

Unauthorized access/use

Patient

Observation devices

Not authentic, uncalibrated device

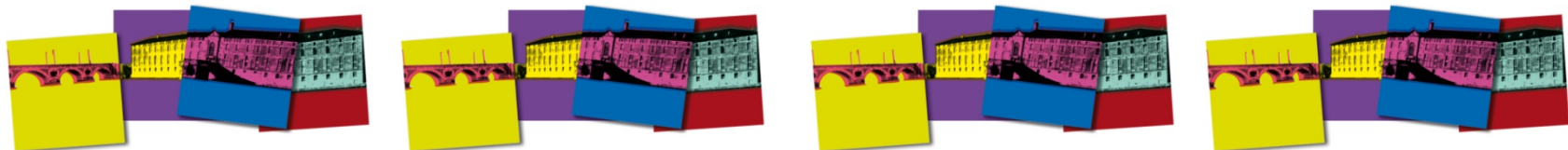Disease management service

PHR/EHR Storage server
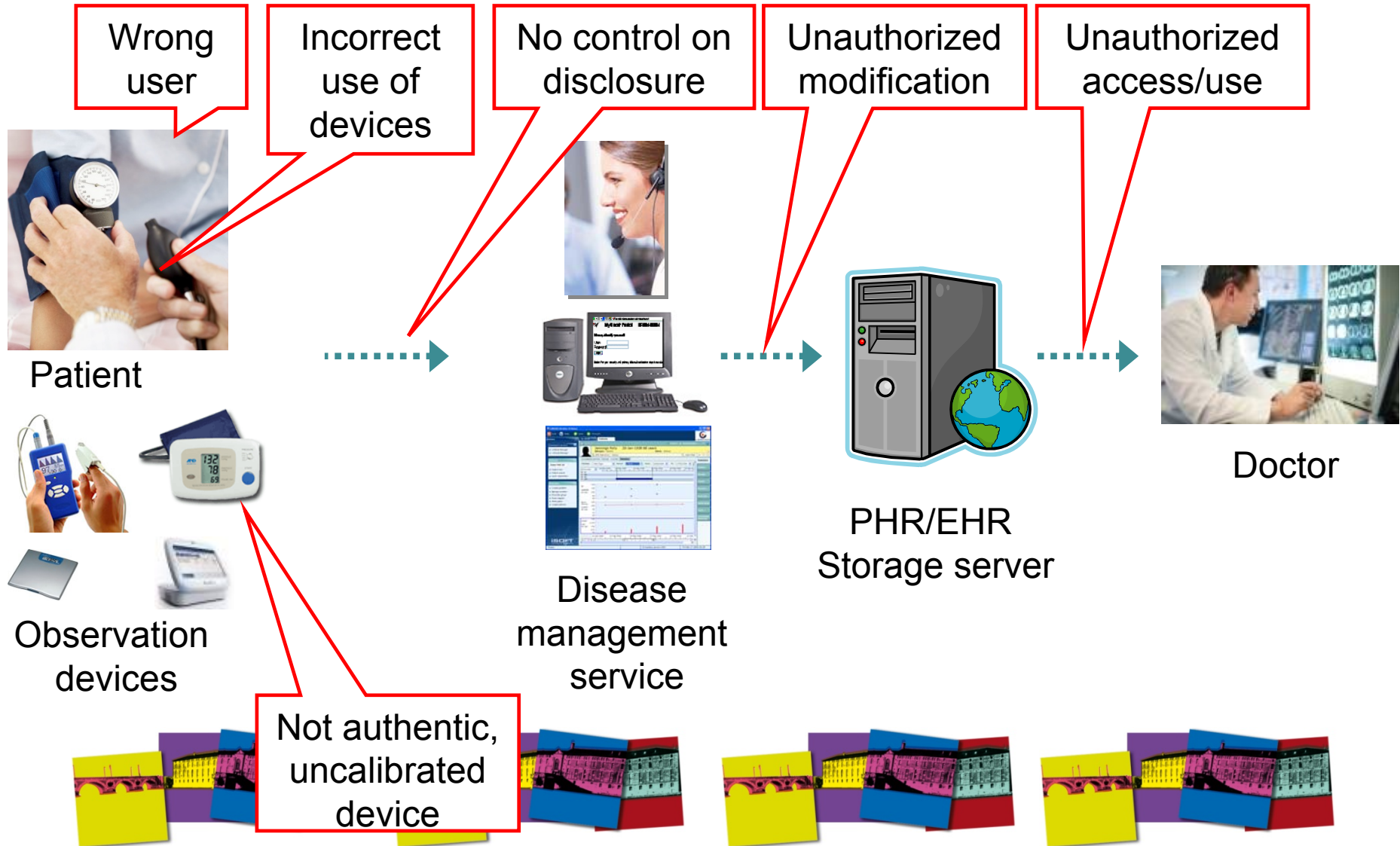
Doctor

Technology solutions

- Confidentiality and privacy
- Authenticity and trustworthiness

Technology solutions

- Confidentiality and privacy
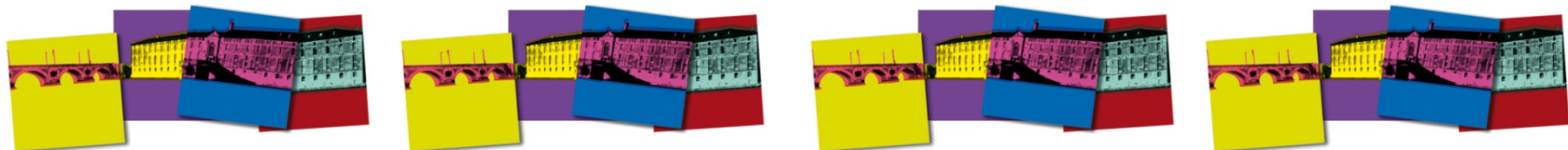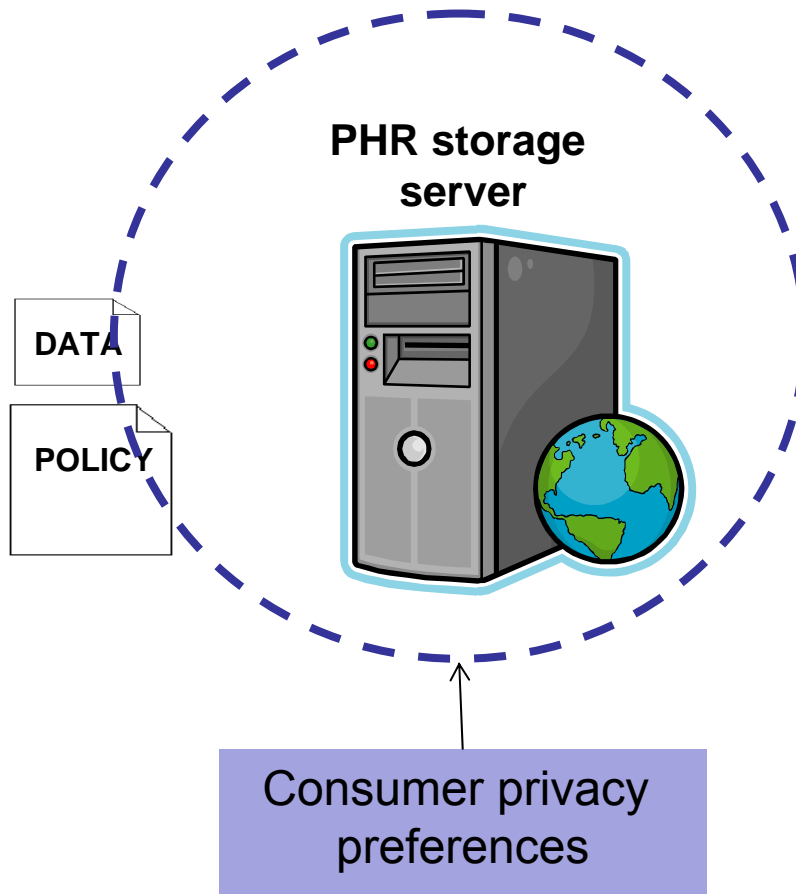- Authenticity and trustworthiness

Data sharing

PHR storage server

Patient/consumer

DATA

POLICY
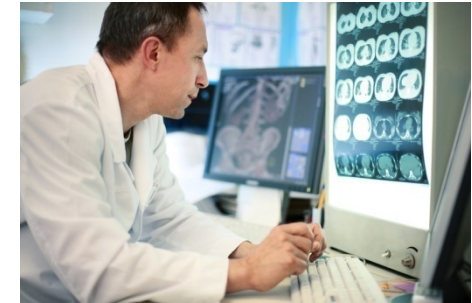
Doctor

Nurse

Consumer privacy preferences

Information-centric protection

Patient/consumer

PHR/EHR Storage Server

Doctor

DATA

Medical system

Consumer privacy preferences
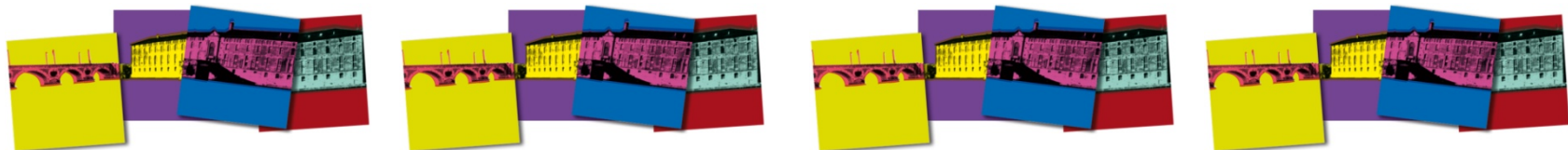
Nurse

Ciphertext-policy attribute based encryption

Patient/consumer

Key authority

Doctor OR (Nurse AND Psychiatry)

PK

MSK

Encrypt

Storage server
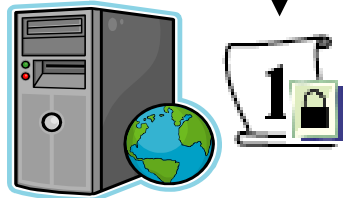
1 OR (0 AND 0)=1

0 OR (1 AND 0)=0

SK$_{Alice}$
Attributes:
Doctor, Cardio,

SK$_{Bob}$
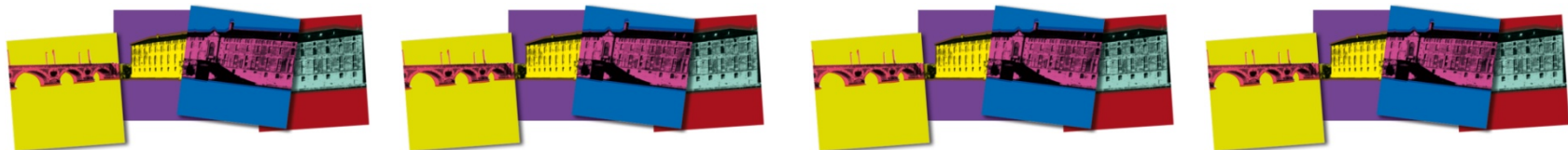Attributes:
Nurse, Radiology, IMC

Technical solutions

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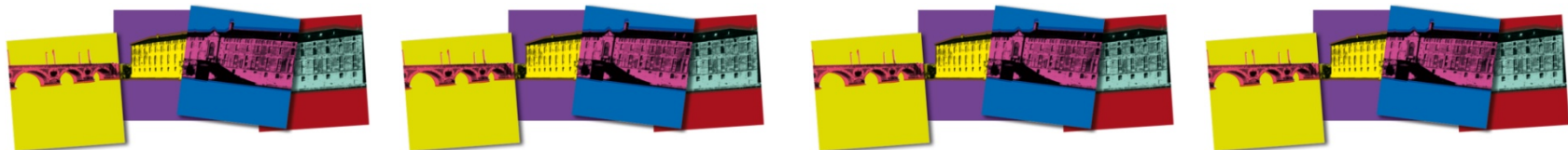 - Attribute-based signatures

REFERENCES
• Luan Ibraimi, Milan Petković, Muhammad Asim, An Encryption Scheme For a Secure Access Policy Updating, Secrypt 2010
• Luan Ibraimi, Muhammad Asim, Milan Petković, Secure Management of Personal Health Records by Applying Attribute-Based Encryption, pHealth, IEEE Press, 2010
• Luan Ibraimi, Milan Petković, Svetla Nikova, Pieter Hartel, and Willem Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application", in H.Y. Youm and M. Yung (Eds.): WISA 2009, LNCS 5932, Springer, Heidelberg, 2009, pp. 309-323.
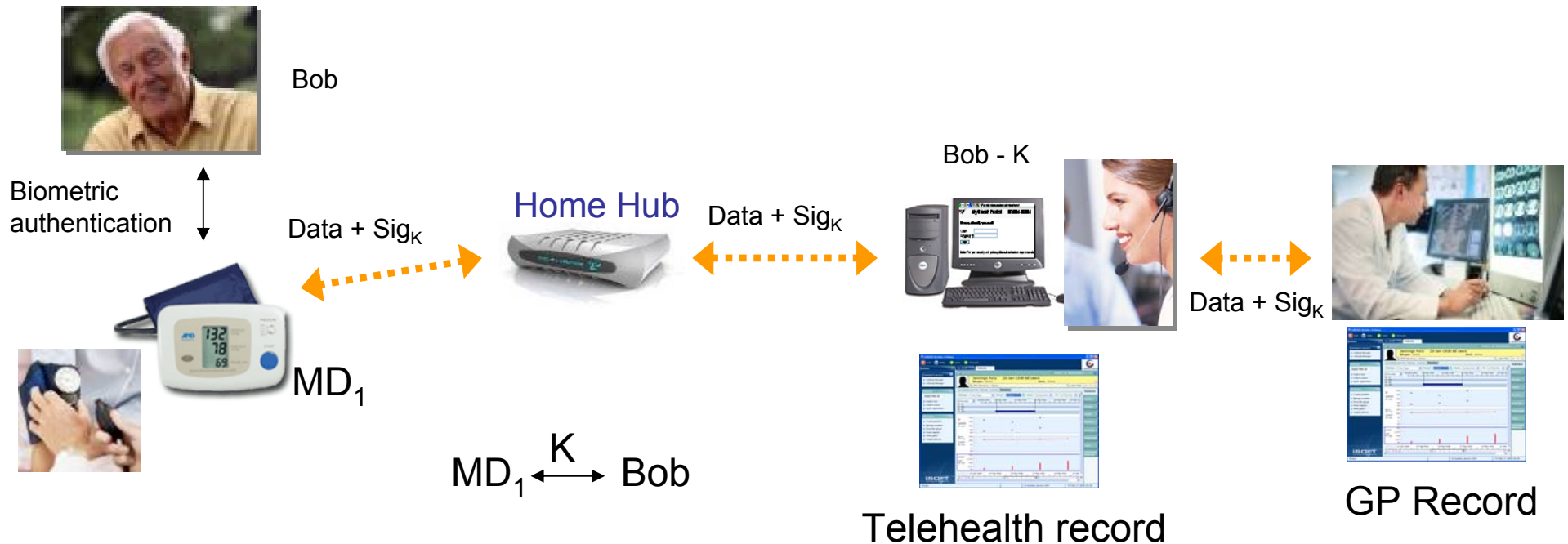
Technology solutions

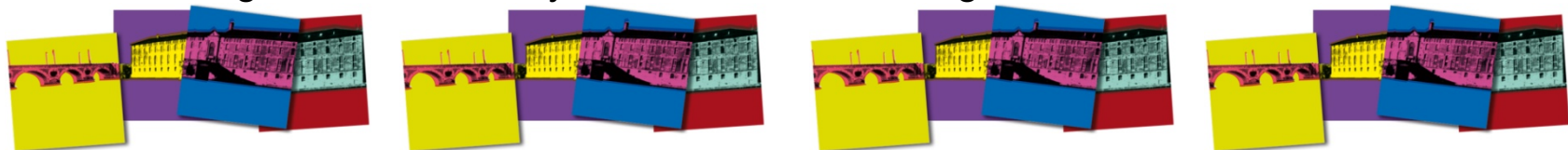- Confidentiality and privacy
- Authenticity and trustworthiness

Combined patient and device authentication

Bob

Biometric authentication

Data + Sig_K

Home Hub

Data + Sig_K

Bob - K

Data + Sig_K

MD₁

$MD_1 \xleftarrow{\quad K \quad} Bob$
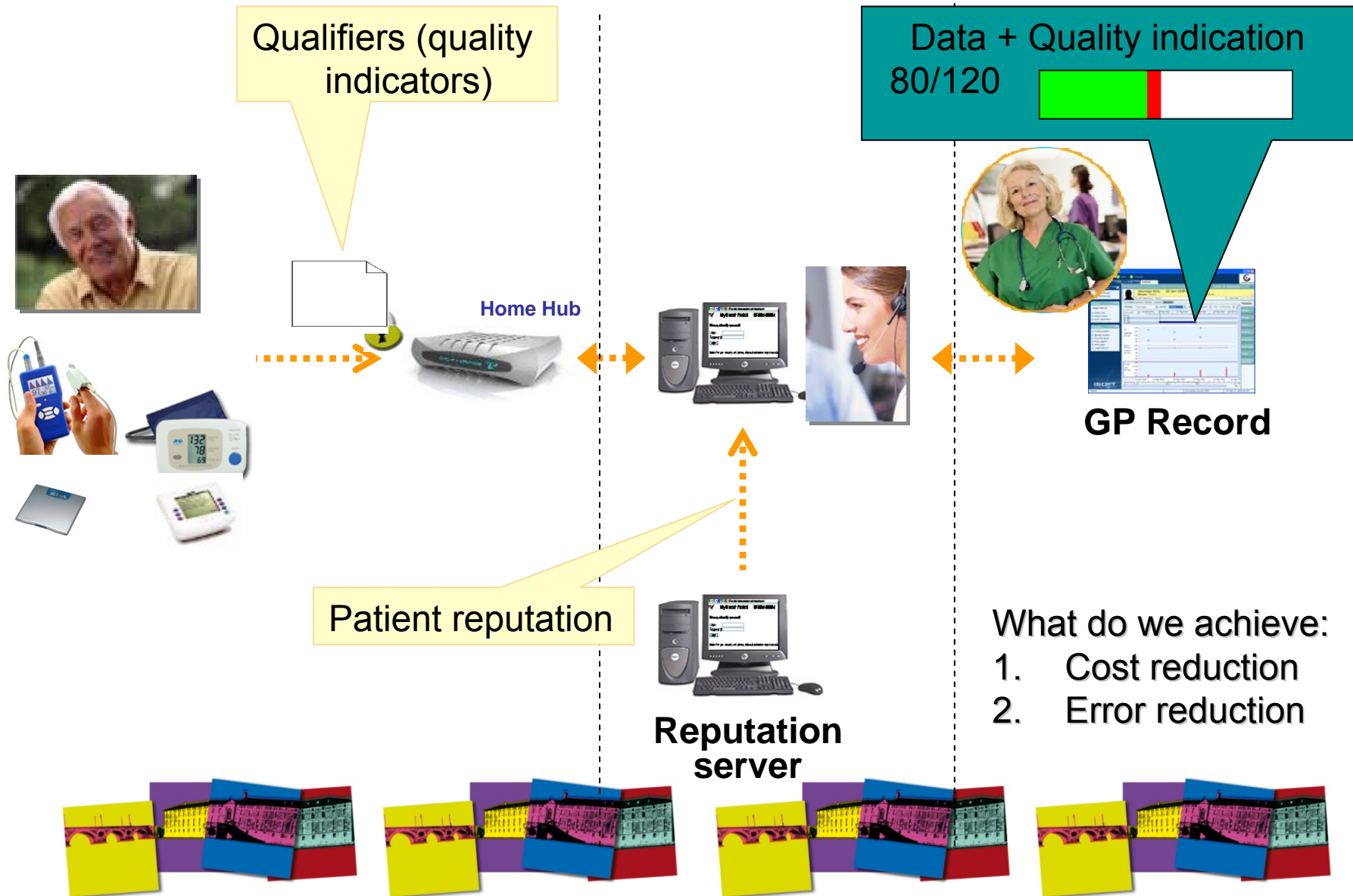
Telehealth record

GP Record

REFERENCE
Milan Petković, "Remote Patient Monitoring: Information Reliability Challenges", 9th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, IEEE Press, 2009, pp. 295-301
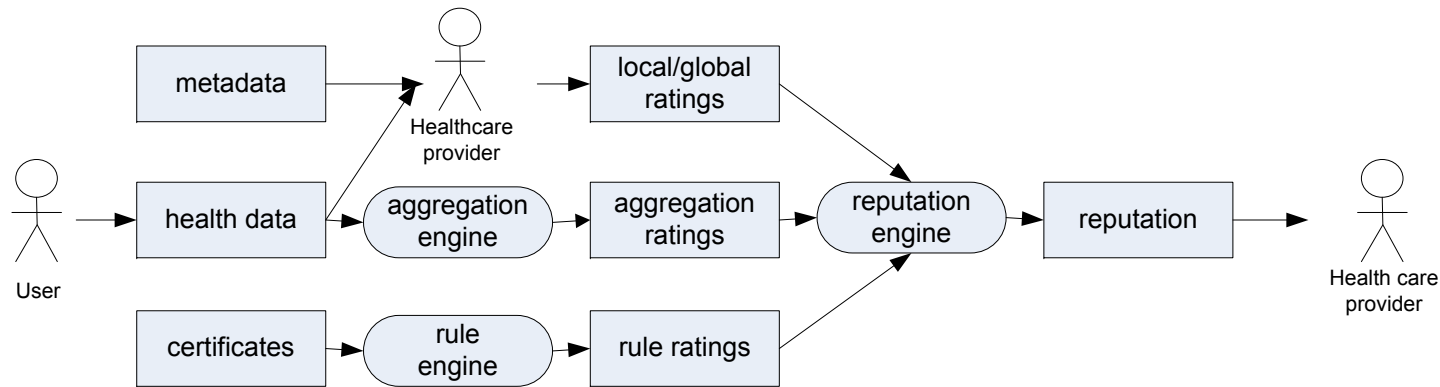Jorge Guajardo, Muhammad Asim, and Milan Petković, Towards Reliable Remote Healthcare Applications Using Combined Fuzzy Extraction, LNCS, Dagsthul, 2010

Quality Indication

Qualifiers (quality indicators)

Data + Quality indication 80/120

Home Hub

GP Record

Patient reputation

Reputation server

What do we achieve:
1. Cost reduction
2. Error reduction

How to calculate trust?

REFRENCES
• Ton van Deursen, Paul Koster, Milan Petković, Hedaquin: A reputation-based health data quality indicator, Electronic Notes in Theoretical Computer Science, Elsevier, 2008, Vol.197(2):159-167.
• 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.
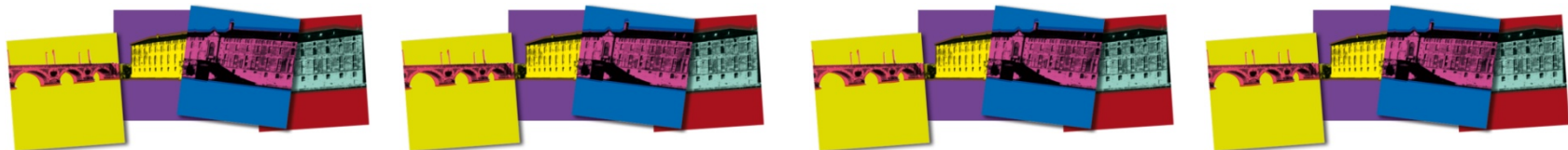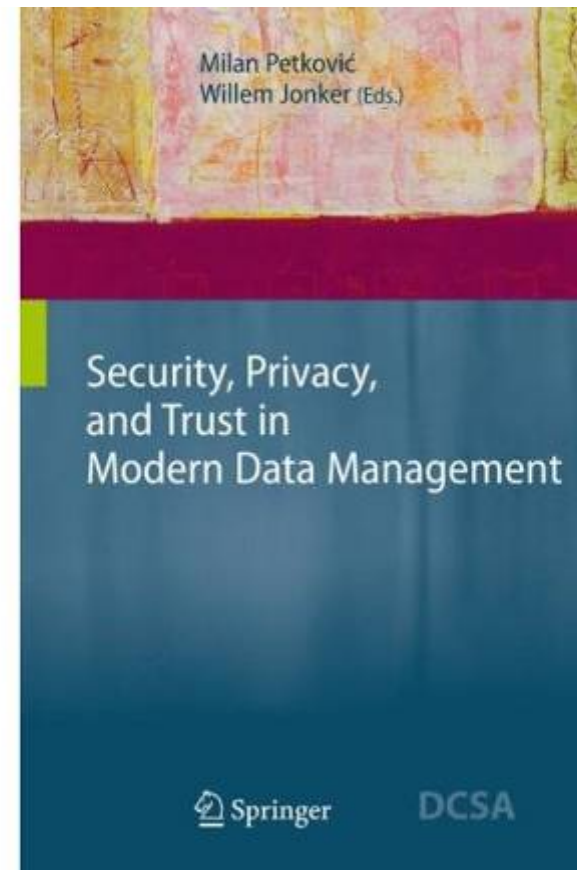
Conclusions

- 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

7th VLDB Workshop on
SECURE DATA MANAGEMENT - SDM 2010
- with a special session on security and privacy in healthcare -

Singapore, September 17, 2010

- **Motivation**
- **Objectives**
- **Topics of Interest**
- **Paper Submission**
- **Important Dates**
- **Organizing Committee**
- **Program Committee**

SDM 2010 (Call for papers – deadline May 31)