nano-tera.ch
swiss scientific initiative in health / security / environment systems

ISyPeM2 RTD 2013

FNSNF

Privacy Preserving Interoperability for Personalized Medicine

A. Dubovitskaya[1,2], V. Urovi[1], M. Vasirani[2], K. Aberer[2], A. Fuchs[3], T. Buclin[3], Y. Thoma[4], M. I. Schumacher[1]

[1]Applied Intelligent Systems Laboratory, HES-SO VS
[2]Distributed Information Systems Laboratory, EPFL
[3]Division of Clinical Pharmacology, CHUV and University of Lausanne
[4]Reconfigurable and Embedded Digital Systems Institute, HEIG-VD

How to share and aggregate medical data for research purposes while preserving the patients' privacy?

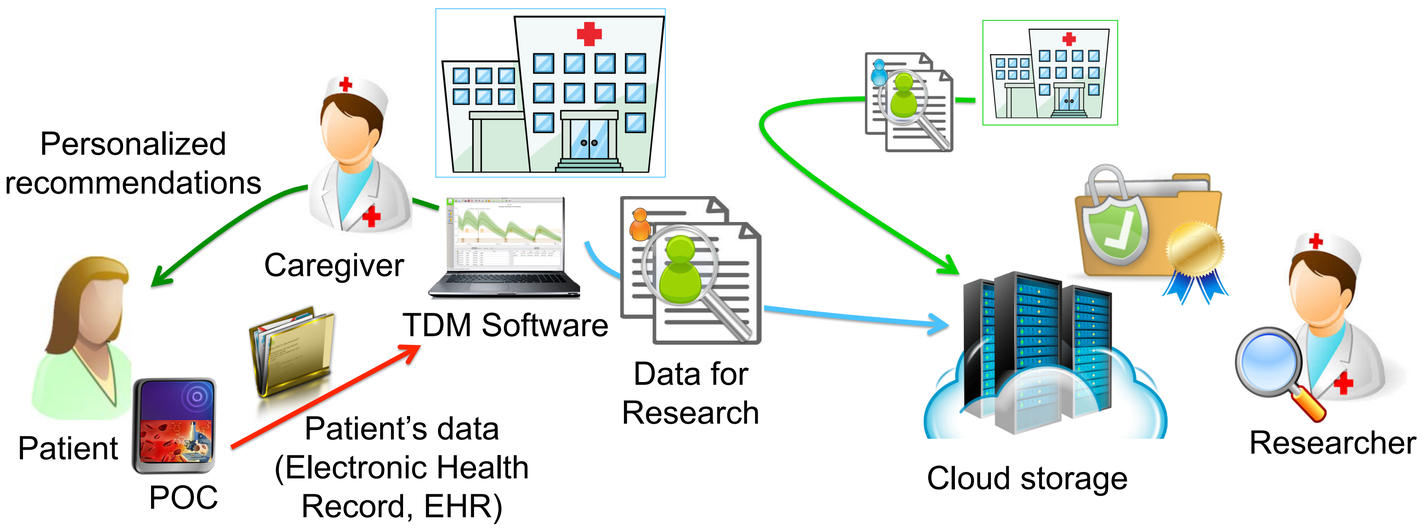
Towards Personalization of the Treatment

Why do we need personalization?

- Some drugs have a narrow therapeutic range and a poorly predictable relationship between the dose and the blood drug concentration, that may also vary greatly among individuals

Therapeutic Drug Monitoring (TDM) aims at improving patient care by monitoring drug levels in the blood to *individually* adjust the dosage in order to target drug concentration in the therapeutic interval. Bayesian TDM ensures a better prediction of the relationship between dose and drug concentration and is based on studies in the general or special populations. This requires population health data (covariates, dosages, drug concentrations) to be collected and analyzed by the researchers.

Dataflow Overview



POC – Point-Of-Care system, that will be able to:

- Perform and collect measurements of the drug concentration in the blood samples
- Provide the medical doctor with all necessary data about the patient
- Share drug intake information and concentration measurement records for research purposes

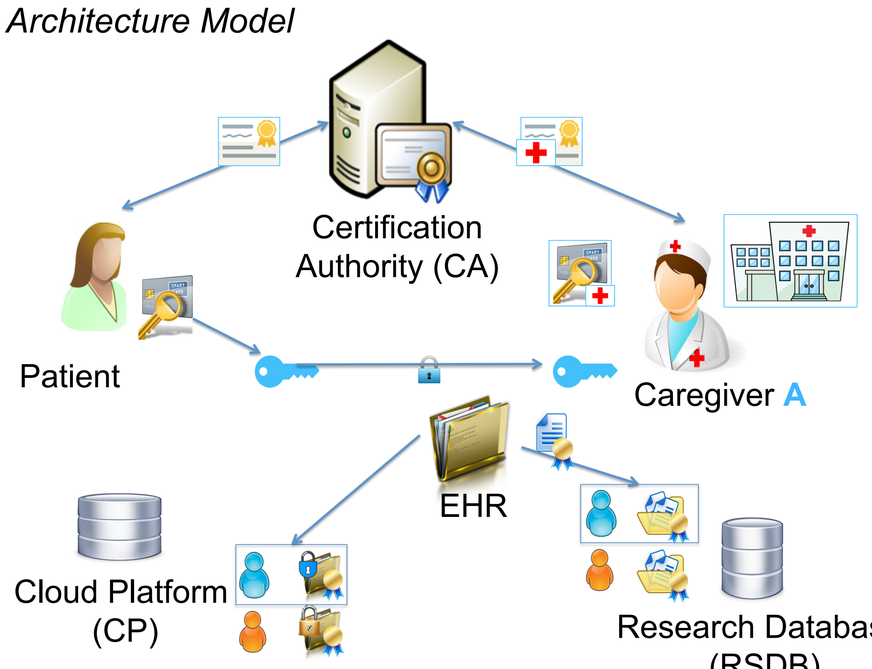
Challenges

- *Achieving interoperability in the distributed environment*
  - Dynamicity of the data
  - Regulations and standards
  - Different interfaces
- *Protection of patients' privacy*
  - Sensitivity of medical data
  - Aggregation of the distributed data about the patient (can reveal sensitive information!)
  - Consent management
  - Access control policy requirements

Ongoing Work

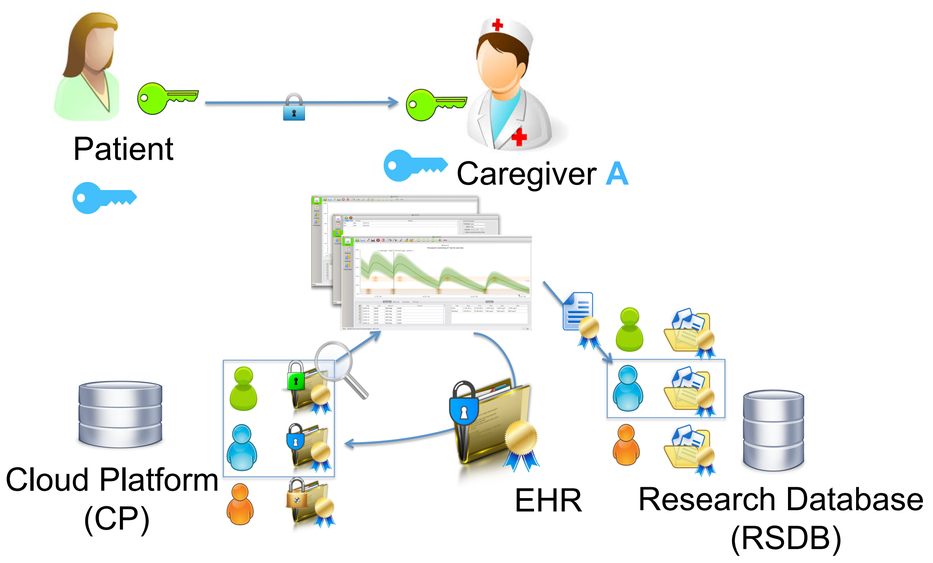
- Developing an interface for the TDM software compliant with HL7 and integrating it with the laboratory system in CHUV (Lausanne)
- Constructing a secure and scalable architecture of an eHealth system for primary and secondary use of the health data:

Architecture Model



- Caregivers and Patients have their secret keys and corresponding public keys certified by CA
- Patient generates from her secret key a shared key with each caregiver she visits
- The sensitive data are encrypted with the shared key and signed with the public key of a caregiver
- De-identified data are signed and sent to RSDB

Access control management



- Caregiver can search for all entries associated with Patient (,) iff he has corresponding keys (,) in an efficient way without revealing identity of the patient or a content of the medical record

RSDB:

- Pseudonymization based on the scheme for multi-key searchable encryption [PZ13]
- k, k^m−anonymization [PLGS13] in a distributed environment

Conclusion

- We address the problem of achieving interoperability and data integration while ensuring users' privacy in the context of a new approach for TDM
- Sharing health data for research will help to put into practice TDM, that will be assisting medical doctors and will significantly improve patient care

References

- [PZ13] Raluca Ada Popa and Nickolai Zeldovich. Multi-key searchable encryption. Cryptology ePrint Archive, Report 2013/508, 2013
- [PLGS13] G. Poulis, G. Loukides, A. Gkoulalas-Divanis, and S. Skiadopoulos, "Anonymizing Data with Relational and Transaction Attributes", in European Conference, ECML PKDD 2013