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*

Towards Personalization of the Treatment: The treatment of certain diseases such as cancer, HIV, or other serious medical conditions relies on a regular administration of critical drugs that are necessary to keep those life-threatening diseases under control. Those drugs (e.g. Efavirenz, Imatinib, Tacrolimus, Tobramycin) have a narrow therapeutic range and a poorly predictable relationship between the dose and the blood drug concentration, which may 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 for targeting drug concentration in the therapeutic interval. In order to ensure a better prediction of the relationship between dose and drug concentration, the ISyPeM2 project[1] has developed a Bayesian TDM approach [GWM^{+}12] based on studies in general or special populations. This approach requires population health data (covariates, dosages, drug concentrations) to be collected and analyzed by researchers, in order to enhance the prediction models. Therefore the following question arises: **how is it possible to share and aggregate medical data for research purposes while preserving the patients' privacy?**

Challenges: Trying to answer this question we face the following challenges:

- Achieving interoperability in the distributed environment (patients data may be distributed over many medical systems, involving a range of IT systems with different interfaces, which have to follow the requirements of regulations and standards (e.g, HL7, EC Data Protection Directive 95/46/EC)
- Ensuring protection of patients' privacy (medical data is sensitive, aggregation of the distributed anonymized data about the patient still can reveal sensitive information, the patient has to be able to set up the access control policy in convenient and efficient way)

Ongoing work: We are tackling these challenges by: **(1)** Developing an interface for the TDM software compliant with HL7 and integrating it with the laboratory system MOLIS deployed at CHUV (Lausanne). **(2)** Constructing a secure and scalable architecture of an eHealth system for primary and secondary use of the health data. We propose an eHealth infrastructure that does not require the existence of a fully trusted party. Patients' data are pseudonymized (based on the scheme for multi-key searchable encryption [PZ13]) and stored in an encrypted form, such that no un-authorized party can learn neither identity of the patient, nor the content of the EHR[2]. Nevertheless, the EHR can be accessed according to the access control policy in an efficient manner. We also build an anonymized research database applying a *k, k^m-anonymization* approach proposed in [PLGD13] in a distributed setting. In addition, we employ the pseudonymization principle that is used for storing EHR. Such construction allows a caregiver to update information about a particular patient and re-contact him/her if needed, while satisfying privacy requirements.

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, which will be assisting medical doctors and, in turn, it will significantly improve patient care.

References:

[GWM+12] V. Gotta, N. Widmer, M. Montemurro, S. Leyvraz, A. Haouala, L. A. Decosterd, C. Csajka, and T. Buclin. Therapeutic drug monitoring of imatinib. Clinical Pharmacokinetics, 51(3):187{201, 2012.

[PZ13] R. A. Popa and N. 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.

[1] a continuation of the Nano-Tera project: Intelligent Integrated Systems for Personalized Medicine, ISyPeM, (http://www.nano-tera.ch/projects/368.php)

[2] Electronic Health Record