Security and Privacy Issues for enabling the Secondary use of EHRs in Clinical Research

Elif Eryilmaz[1], Gokce B. Laleci Erturkmen[1]
[1] SRDC- Software Research & Development and Consultancy Ltd., Silikon Bina 1. Kat No: 14 ODTU Teknokent 06800 Cankaya/Ankara, Turkey,
elif@srdc.com.tr , gokce@srdc.com.tr

Abstract: **Re-using Electronic Healthcare Records (EHR) for facilitating clinical research studies has a great potential. Besides interoperability, safeguarding the security and privacy of the medical data in the context of secondary use for clinical research is one of the most important challenges in this respect. In this presentation we will introduce the SALUS security architecture, including de-identification and pseudonymization mechanisms applied to the queried clinical instances as well as additional security services compatible with IHE ATNA Profile that guarantees the safe use of EHRs for the clinical research studies.**

Introduction

In the SALUS Project [1], which is co-financed by the European Commission within the 7th Framework Program (FP7), we aim to create the necessary infrastructure to enable secondary use of EHRs in an efficient and effective way for reinforcing the post market safety studies so that patient safety can be ensured through early detection of rare adverse events. We are developing functional interoperability profiles to query population based EHR data from distributed EHR systems for carrying out post market safety studies. As a result of these population based queries, a set of medical summaries of the eligible patients can be shared in standard based medical summary formats, one of which is Health Level Seven (HL7) Clinical Document Architecture (CDA) Release 2 [2] document templates. From the security and privacy point of view, we have developed novel data protection mechanisms to work directly on top of clinical data represented in CDA based templates for the post-market safety studies.

In the literature, there are several efforts [3,4,5] that describe generic frameworks enabling anonymization and pseudonymization of patient data in research networks. Among these, the Pommerening approach [3] is a pioneering work as a result of a study that was carried out by the TMF of Germany (the Telematics Platform for the Medical Research Networks of the Federal Ministry of Education and Research). It provides the basic

requirements of ensuring safety of patient data in research studies, and five different models for pseudonymization. However, in these scenarios, the purpose is creating a separate data warehouse (DWH) that is set up for the purpose of clinical research studies and the proposed pseudonymization services are used to create such a DWH. However, in SALUS project, we claim that without the need of such separate clinical research data warehouses, EHR systems can be involved in clinical research studies, by accepting population based queries from trusted parties and sharing de-identified medical summaries of the eligible patients through secure channels.

For this reason, we have applied data protection mechanisms on top of the clinical data instances shared as result sets of population based queries instead of securing all data elements in the DWH of the responsible parties. The mechanisms developed in this scope include de-identification and pseudonymization services providing that clinical information is shared securely within the interoperable parties in SALUS architecture in an effective way, complying with all necessary legal requirements designed to protect patient rights and interests. Additional mechanisms such as auditing of events and message level security compliant with the Integrating the Healthcare Enterprise (IHE) standards complement this data level security approach in our infrastructure.

In order to build a generic security infrastructure for this purpose, we have analyzed many different approaches for enabling safety of the medical data in the context of secondary use for clinical research by taking into account the available policies and regulations within EU. In conformance to the selected standards, guidelines, and well-accepted methodologies, we have tried to find a balance between the privacy concerns for the use of personal data and the requirements of clinical research environments that aim to serve to the public good. In this respect, we have created a flexible security architecture, where some thresholds for the uncommon cases can be configured with the Data Protection Offices of EHR sources according to their preferences.

In this paper, we present the overview of the extensible security framework that is compliant with legal and ethical requirements analyzed at the European level. At the end of the SALUS project, we will provide a fully functional open source toolset that will enable the developers to self-enhance this security infrastructure for their research purposes according to the rules and regulations valid in their sites.

Materials and Methods

In order to explain the security infrastructure that we have developed in the SALUS project in a more systematic way, we have separated the data protection mechanisms, where we have a novel approach to deal with the privacy of clinical data represented in CDA templates, from the additional security mechanisms supporting this approach.

In the composition diagram below, SALUS security and privacy services with these two separate sides are shown:

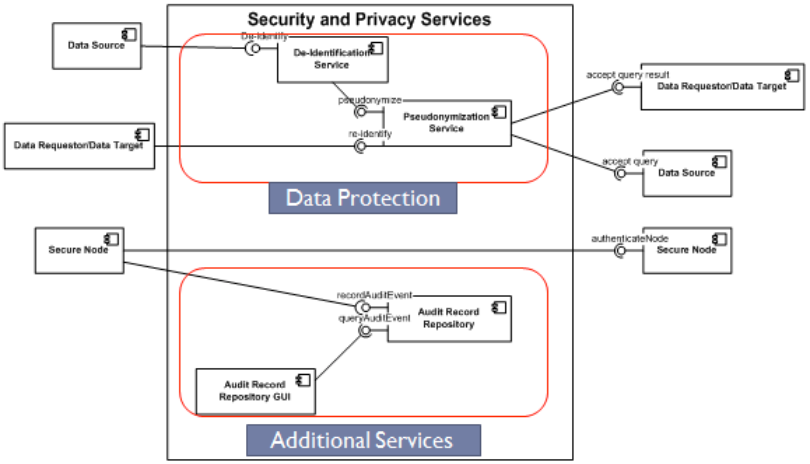

Figure 1 – Composition diagram for SALUS Security and Privacy Services

As pointed out in Figure 1, regarding the data level protection, De-Identification Service is called at the Data Source side, after collecting the queried clinical data instances from the underlying Data Source throughout the SALUS interoperability services. The Data Requester is hosted outside the Care Zone in our architecture. The De-identification Service is configured for each selected element in the SALUS content models. After de-identifying the clinical data set based on the configuration, this data set is passed to the Pseudonymization Service for the selected data items to be pseudonymized.

As additional mechanisms to support the data level protection, SALUS security architecture includes the implementation of IHE Audit Trail and Node Authentication (ATNA) Profile [6] for the secure exchange of

healthcare information and the auditing of events related to the access, production or modification of healthcare information. These mechanisms ensure the secure exchange of clinical data at the message level and provide the audit records in conformance to existing interoperability standards.

Acknowledgment

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no ICT-287800, SALUS Project (Scalable, Standard based Interoperability Framework for Sustainable Proactive Post Market Safety Studies).

References

[1] SALUS Project- Scalable, Standard based Interoperability Framework for Sustainable Proactive Post Market Safety Studies, http://www.salusproject.eu/
[2] Clinical Document Architecture (CDA) http://www.cdc.gov/nhsn/cda_esurveillance.html
[3] Klaus Pommerening, Michael Reng. Secondary use of the Electronic Health Record via pseudonymisation. In: L. Bos, S. Laxminarayan, A. Marsh (eds.): Medical Care Compunetics 1, IOS Press, Amsterdam 2004; pp. 441–446
[4] Thielscher, C., Gottfried,M., Umbreit, S., Boegner, F., Haack, J., Schroeders, N. Patent: Data processing system for patient data. Int. Patent, WO 03/034294 A2 (2005).
[5] Noumeir R, Lemay A, Lina JM. Pseudonymization of ra-diology data for research purposes. J Digit Imaging. 2007 Sep;20(3):284-95.
[6] IHE Audit Trail and Node Authentication (ATNA) Profile, http://wiki.ihe.net/index.php?title=Audit_Trail_and_Node_Authentication