Security And Privacy Of Medical Data

Challenges For Next-Generation Patient-Centric Healthcare Systems

Vladimir Janjic
Juliana Bowles
vj32@st-andrews.ac.uk
jkfb@st-andrews.ac.uk
School of Computer Science, University of St Andrews
United Kingdom

Marios Belk
Andreas Pitsillides
belk@cs.ucy.ac.cy
andreas.pitsillides@ucy.ac.cy
Department of Computer Science, University of Cyprus
Cyprus

ABSTRACT

We describe the recently-started EU H2020 *Serums: Securing Medical Data in Smart Patient-Centric Healthcare Systems* project that aims to develop novel techniques for safe and secure collection, storage, exchange and analysis of medical data, allowing the patients of the next-generation smart healthcare centers to get the best possible treatment while respecting privacy and ownership of their sensitive personal data. Our goal is to significantly enhance trust in the new medical systems. We outline the techniques that will be extended/developed over the course of the project and describe the use cases that will be used to verify the effectiveness of these technologies in practice.

KEYWORDS

Medical data, Smart Healthcare, Data Sharing, Privacy, Security, Personalised Medicine

ACM Reference Format:
Vladimir Janjic, Juliana Bowles, Marios Belk, and Andreas Pitsillides. 2019. Security And Privacy Of Medical Data: Challenges For Next-Generation Patient-Centric Healthcare Systems. In *27th Conference on User Modeling, Adaptation and Personalization Adjunct (UMAP'19 Adjunct), June 9–12, 2019, Larnaca, Cyprus.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3314183.3326364

1 INTRODUCTION

In order to achieve the highest quality of healthcare provision, it is increasingly important to collect highly confidential and personal medical data that has been obtained from a variety of sources, including personal medical devices, and to share this through a variety of means. Integrating home-based healthcare into a holistic treatment plan is more cost effective, reduces travel-associated risks and costs, and increases the quality of healthcare provision. Consequently, the medical centres of the future will be *highly decentralised*, with individual patient data residing on a number of different devices, some of which will be outside of the trusted networks of the medical organisation. In some cases, cooperation between health institutions from different countries might be required to ensure that patients get the best possible treatment. All this raises a number of issues related to preserving security and privacy of the patient data, together with complying to a combination of different national and international legislations (such as GDPR) that regulate ownership and sharing of that data.

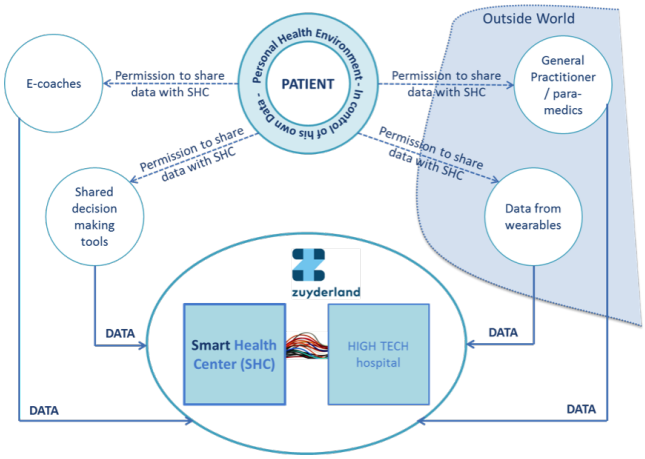

Figure 1: Example of Data Sharing in Smart Health Center

The goal of the recently-started *Serums: Securing Medical Data in Smart Patient-Centric Healthcare Systems* EU H2020 project is to develop novel mechanisms for safe and secure collection, storage, communication and analysis of medical data. We aim to put patients in the centre of future healthcare provision, enhance their personal care, maximise the quality of their treatments while ensuring trust in the security and privacy of their confidential medical data. Figure 1 shows an example of data sharing in the future-generation smart healthcare centres, where different entities (different classes of users and parts of the healthcare center system) need to exchange data. The main objectives of the *Serums* project are:

- to develop new techniques that will ensure the *security and protection of personal medical data* that is shared between patients, hospitals and medical practitioners in smart healthcare systems;
- to integrate personal medical data from multiple sources (e.g. personal monitoring devices, hospital diagnostics systems, specialists and general practicioners) into a single coherent *smart patient record*;

UMAP'19 Adjunct, June 9–12, 2019, Larnaca, Cyprus

ACM ISBN 978-1-4503-6711-0/19/06…$15.00
https://doi.org/10.1145/3314183.3326364

- to develop *new data analytic techniques* that will be able to take advantage of advances in the availability of heterogeneous real-time personal healthcare information, as part of a holistic smart healthcare system, while respecting privacy and security concerns;
- to develop/enhance *authentication and trust mechanisms* that ensure that only properly authorised agents have access to the required parts of medical records;
- to demonstrate world-leading levels of compliance with emerging legal and ethical requirements for the protection of personal and medical data across national boundaries, including transnational requirements such as GDPR;
- to *demonstrate the effectiveness of the Serums techniques against a variety of real-world medical use cases*, including both ongoing and emergency medical care scenarios.

2 THE *SERUMS* TECHNOLOGIES

As a part of the *Serums* project, we will extend or develop the following novel techniques for handling medical data:

- *Smart Patient Record Format*, that will standardise representation of the patient medical data across different use cases. Our aim is to develop a unified way of structuring medical records that will allow for easier and more generic data analysis, as well as automatic generation of synthetic medical data for development and testing of systems.
- *Blockchain technology* that will be used to control storage and access to the sensitive medical data and to record all transactions on the data.
- *Deep-learning based metadata extraction mechanisms* that will be used to pre-process possibly unstructured medical data (e.g. data coming from personal monitoring devices) and extract the useful metadata from it that is required for the appropriate storage and data analytics on it.
- *Distributed Privacy-Preserving Learning Technology* for analysing medical data, that will be tailored to the distributed smart medical centres of the future, and will allow processing of the data without leakage of any sensitive information.
- *Authentication and Authorisation Techniques* that will go beyond the traditional "one-size-fits-all" authentication and authorisation schemes, will be bootstrapped to different classes of users by considering their preferences and interaction context, and will make sure that only the appropriate entities can view the (appropriate parts of) smart patient records.
- *Data Cloaking* for masking the data to allow safe transmission over possibly untrusted networks.
- *Data Fabrication* that will allow the generation of synthetic but realistic medical data, based on strict rules and relationships between individual data items. This will allow rapid development and training of authentication, storage, access, cloaking and analytic models without risks of exposing sensitive personal data.

3 USE CASES

The *Serums* technologies will be evaluated on several large-scale use cases, demonstrating their effectiveness when applied to real-world scenarios.

Zuyderland Medisch Centrum Healthcare Centre will be a new system that will combine data collected outside of the hospital walls with data generated inside the hospital. This data is currently collected and analysed by several institutions, like for example wearable developers (e.g. Fitbit), e-health applications (e.g. e- coaches from Sananet), shared decision making tools, etc. Data from these organisations are currently scattered around on different servers and are not analysed as a whole. We want to combine this data in order to be able to provide patients with personalise advice, based on their own health situation.

Hospital Clinic of Barcelona Smart Platform will integrate data from the whole patient healthcare ecosystem, combining data gathered from different sources inside the hospital and outside of it and considering different levels of communication. The data sources will include the Catalonian Healthcare Platform, which is a regional healthcare data repository that will share the data it contains with the Hospital Clinic of Barcelona, taking into account GDPR and different local regulations. We want to integrate this data into the coherent system, taking into account the appropriate permissions of the patients and data exchange security standards.

Edinburgh Cancer Data Gateway aims to improve the quality and capability of reporting outcomes within South East Scotland Oncology databases in real time using routinely captured and integrated electronic healthcare data, as well as patient reported outcome measures (PROMS). We will use the National Health Service Lothian (NHS Lothian) cancer patient data from multiple resources, scattered across different system and platforms. There is currently a lack of proxy between the different (sub)systems or mechanisms to join the information automatically. This data has to be integrated to make it possible to accurately predict toxicity levels from a treatment regime, taking into account patient information (PROMS) in between treatments, comorbidities and further medications.

Transnational Data Exchange will focus on scenarios where information from individual use cases needs to be exchanged, transmitting data across national borders, complying with a combination of different regulations.

4 CONCLUSIONS

The *Serums* project will tackle the main challenges (such as establishing trust, allowing patients to have full control of their data, providing high level of security and anonimity of the data and providing high level of transparency in operation) for implementing fully distributed next-generation smart healthcare centers that will allow patients to get the best possible healthcare while at the same time conforming to all relevant legislations about the privacy and ownership of their data. By developing novel pre-processing, storing, authentication, data cloaking and data analythics method, supported by data fabrication techniques for generating synthetic but realistic data, the project will allow major advances to be made in handling sensitive and confidential medical data.

ACKNOWLEDGMENTS

This work has been supported by the EU H2020 grant *Serums: Securing Medical Data in Smart Patient-Centric Healthcare Systems* (code 826278).