Chapter 20
Seamless Access to Healthcare Folders with Strong Privacy Guarantees

Tristan Allard
University of Versailles & INRIA Rocquencourt, France

Nicolas Anciaux
INRIA Rocquencourt, France

Luc Bouganim
INRIA Rocquencourt, France

Philippe Pucheral
University of Versailles & INRIA Rocquencourt, France

Romuald Thion
INRIA Grenoble, France

ABSTRACT

During the past decade, many countries launched ambitious Electronic Health Record (EHR) programs with the objective to increase the quality of care while decreasing its cost. Pervasive healthcare aims itself at making healthcare information securely available anywhere and anytime, even in disconnected environments (e.g., at patient home). Current server-based EHR solutions badly tackle disconnected situations and fail in providing ultimate security guarantees for the patients. The solution proposed in this paper capitalizes on a new hardware device combining a secure microcontroller (similar to a smart card chip) with a large external Flash memory on a USB key form factor. Embedding the patient folder as well as a database system and a web server in such a device gives the opportunity to manage securely a healthcare folder in complete autonomy. This paper proposes also a new way of personalizing access control policies to meet patient's privacy concerns with minimal assistance of practitioners. While both proposals are orthogonal, their integration in the same infrastructure allows building trustworthy pervasive healthcare folders.

DOI: 10.4018/978-1-60960-183-6.ch020

1. INTRODUCTION

Driven by the need to improve the quality of care while decreasing costs, many countries around the world are setting up large scale Electronic Health Record (EHR) systems gathering the medical history of individuals. Interoperability among heterogeneous healthcare information systems and privacy preservation are two main challenges in this context. Pervasive healthcare on its side strive to remove location and time constraints to access patient's healthcare folders. Cares provided at home to elderly or disabled people illustrate well the need for pervasiveness. In this context healthcare data is often collected and consulted at home by practitioners having different privileges and acting at different time periods. Healthcare information must be safely exchanged among practitioners to improve care coordination but no connection to the Internet can be always guaranteed. Data can also be issued by institutions external to the care coordination (e.g., a medical lab) and join the patient's folder. The folder is sometimes accessed by practitioners outside patient's home (e.g., doctor's office, hospital). Finally, a large collection of folders can be targeted by epidemiological studies for a general health benefit. In this paper, we discuss how smart objects can provide a seamless access to healthcare folders without privacy breach in all these situations.

EHR systems aim at answering most of the requirements mentioned above. The objective of centralizing medical information in database systems is manifold[1]: completeness (i.e., to make the information complete and up to date), availability (to make it accessible through the internet 24h-7 days a week), usability (to organize the data and make it easily queryable and interpretable), consistency (to guarantee integrity constraints and enforce atomicity and isolation of updates) and durability (to protect the data against failure). A recent report identified more than 100 EHR running projects worldwide at the scale of a country or regions in 2007 (Door, 2008). Other reports suggest that about 25% of U.S. healthcare practices use EHR systems. Within Europe these figures vary greatly between countries, from 15% in Greece up to 90% in the Netherlands today.

Regarding pervasiveness, healthcare folders can be reached by allowing internet connections to the server(s) through mobile devices (e.g., laptop, PDA, tablet PC). This however requires that every point of the territory be connected through a secure, fast, reliable and cheap network, a situation uncommon in many countries and regions today.

In addition, and despite the unquestionable benefit of EHR systems in terms of quality of care, studies conducted in different countries show that patients are reluctant to use existing EHR systems arguing increasing threats on individual privacy (The Times, 2008; The International Council on Medical & Care Compunetics, 2009). This suspicion is fueled by computer security surveys pointing out the vulnerability of database servers against external and internal attacks (Gordon et al., 2006). Indeed, centralizing and organizing the information make it more valuable, thereby motivating attacks and facilitating abusive usages. Regardless of the legislation protecting the usage of medical data and of the security procedures put in place at the servers, the patient has the sense of losing control over her data.

Hence, implementing a trustworthy pervasive access to healthcare folders requires addressing accurately the following issues:

1. How to make patient's healthcare folder available in a disconnected mode?
2. How to make patient's healthcare folder seamlessly available in a connected area?
3. How to make the patient trust the EHR security?
4. How to get the patient consent about a pervasive use of her healthcare folder?

As discussed above, existing EHR systems answer well issue 2 but fail in answering issue 1 and issue 3. Therefore, EHR systems fail also