Chapter 2
Privacy and Security in e-Health Applications

Milan Petković
Philips Research Europe & Eindhoven University of Technology, The Netherlands

Luan Ibraimi
University of Twente, The Netherlands

ABSTRACT

The introduction of e-Health and extramural applications in the personal healthcare domain has raised serious concerns about security and privacy of health data. Novel digital technologies require other security approaches in addition to the traditional "purely physical" approach. Furthermore, privacy is becoming an increasing concern in domains that deal with sensitive information such as healthcare, which cannot absorb the costs of security abuses in the system. Once sensitive information about an individual's health is uncovered and social damage is done, there is no way to revoke the information or to restitute the individual. Therefore, in addition to legal means, it is very important to provide and enforce privacy and security in healthcare by technological means. In this chapter, the authors analyze privacy and security requirements in healthcare, explain their importance and review both classical and novel security technologies that could fulfill these requirements.

INTRODUCTION

Recently, many e-Health applications are proposed worldwide. They include initiatives on creation of national/regional electronic health record (EHR) infrastructures such as RHIO's in the US, the NHS Spine project in the United Kingdom and NICTIZ in the Netherlands, as well as efforts on creating commercial Web-based personal health record (PHR) systems such as Microsoft HealthVault and Google Health. These applications process, store and exchange patient's medical information. Next to that, there is an increasing number of extramural telemedicine applications in the personal healthcare domain such as remote patient monitoring. On the one hand these technologies

DOI: 10.4018/978-1-60960-469-1.ch002

improve the quality of health care by providing faster and cheaper health care services, on the other hand they are exposed to different security threats as it becomes simpler to collect, store, and search electronic health data, thereby endangering people's privacy. Therefore, they pose new security and privacy challenges towards the protection of medical data.

In contrast to other domains, such as financial, which can absorb the cost of the abuse of the system (e.g. credit card fraud), healthcare cannot. Once sensitive information about an individual's health problems is uncovered and social damage is done, there is no way to revoke the information or to restitute the individual. Therefore e-Health applications must implement safeguards in place to protect the privacy of patients' health data.

This is recognized by legislation. There are a number of laws around the world designed to protect the electronic health data that the healthcare institutions maintain about their patients, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US, which specifies rules and standards to achieve security and privacy of health data, or directive 95/46/EC in the EU for protecting personal data processed by information systems. Furthermore, there are a number of sophisticated security mechanisms, such as access control mechanisms, encryption techniques and auditing tools which are applicable for e-Health applications.

In this chapter, we address the issues of security and privacy in e-Health applications. Firstly, we survey different types of digital health records and describe examples of human-centered e-Health applications which use them. Next we overview their privacy and security requirements such as data availability, data confidentiality, data integrity, accountability, anonymity and user awareness and discuss the state-of-the-art technologies which address these requirements. The focus is put on the technologies centered around the patient.

DIGITAL HEALTH RECORDS: CURRENT SITUATION AND TRENDS

To reduce cost and improve accuracy there is a pressure on healthcare providers to start managing and sharing patient information in digital form. This implies a revolution in the way health information is managed. Paper-based records are becoming obsolete as with the increasing complexity of the healthcare system the paper systems cannot fulfill the complicated requirements and ensure that the right information is available at the point of care when needed. Therefore, digital records are increasingly used within hospitals in departmental information systems (DIS) as well as at the hospital level in hospital information systems (HIS). However, the use of digital records will go beyond the walls of the hospital. General practitioners (GP), pharmacies, remote patient monitoring systems and other home e-Health services are increasingly using them.

In this section, we give an overview of digital health records and describe two main purposes they have: (i) to serve healthcare providers and (ii) to empower the patient/consumer. To make the differences clear, we describe the architecture of a national/regional EHR system, as well as an example of a PHR system. However, there are a number of dedicated services such as remote patient monitoring systems that collect and use some types of health data, such as blood pressure, pulse, weight, etc. These systems share a number of security and privacy concerns with EHR and PHR systems, but we do not describe them in this chapter as their architectures are in most cases related to the EHR and PHR architectures. For a good example, the interested reader can check the architecture of the Philips Motiva system (Simons, 2006).

Electronic Health Records (EHR)

Digital health records are used at different levels in healthcare. First, they are used in hospitals at