Chapter 14
Privacy Enhancing Technologies in Electronic Health Records

Christian Stingl
Carinthia University of Applied Sciences, Austria

Daniel Slamanig
Carinthia University of Applied Sciences, Austria

ABSTRACT

In recent years, demographic change and increasing treatment costs in North American and European countries demand the adoption of more cost efficient, highly qualitative and integrated health care processes. The rapid growth and availability of the Internet facilitate the development of eHealth services and especially of electronic health records (EHRs) which are promising solutions to meet the aforementioned requirements. The EHR integrates all relevant medical information of a person and represents a lifelong documentation of the medical history. Considering implementations of EHRs, one of the most critical factors of success is the protection of the patient's privacy, which is clearly reflected in surveys concerning such systems. This chapter will provide a security analysis of EHR systems, discuss basic and enhanced security methods and finally introduce levels of security to classify EHR systems.

INTRODUCTION

An electronic health record (EHR) is the integration of relevant medical information of a person and represents a lifelong documentation of the medical history of this person. EHRs improve the availability of medical data and consequently help to improve the quality and efficiency of medical treatment processes. One interesting aspect of EHRs is the moderation of health data. This can either be realized by authorized medical staff and/or the patients. The second group is especially of high importance in context of Personal Health Records (PHRs). Moderation comprises not only the management of medical data but also the task of granting access to medical data to other parties. Moreover, it is also possible to nominate trustworthy delegates for the moderation of the medical data, e.g. a general practitioner or a relative.

The focus of this chapter is a discussion of security issues regarding EHR systems, where we assume that these systems provide a time and loca-

DOI: 10.4018/978-1-61520-777-0.ch014

tion independent access via the Internet. This is, of course, a central aspect in most of the currently available and deployed systems.

As mentioned above, one important aspect of EHR systems is the management of highly sensitive medical data. It must be emphasized that medical data are much more sensitive than data from the banking or telecommunication sectors. Consequently, a high level of security and especially the protection of the patient's privacy are essential for EHR systems. Hence, we claim that this is a critical success factor for the public acceptance of these systems.

The two main issues that will be discussed in this chapter are the security analysis of EHR systems and security concepts that can be applied to encounter the identified threats and thus to achieve a very high level of security.

The security analysis firstly classifies potential attackers, namely external adversaries, internal adversaries and so called curious persons. Secondly, we are focusing on components of an EHR system that can be attacked, i.e. the EHR system itself, the communication channel and the user's client. Thirdly, we will identify data that are vulnerable to attacks and consequences which result from attacks against these data. We want to point out, that the analysis primarily focuses on aspects regarding the patients in order to enhance their privacy.

After this analysis we will introduce methods to realize a security concept for EHR systems. These methods are divided into basic and enhanced ones, whereas the enhanced methods can be used to significantly improve the patient's privacy. Furthermore, we define five security levels which consist of subsets of the above mentioned methods. These levels can be applied for the implementation of security concepts for EHR systems to prevent security threats discussed in the security analysis. Moreover, we will give some characteristic real-world examples as well as some virtual scenarios of attacks against medical data that are in our opinion highly realistic and analyze them with respect to the security levels.

Before we start with the security analysis we will give some background information on electronic health records, health data, legal requirements and cryptography.

BACKGROUND

Health Records

In this section we are going to discuss the basic terminology und characteristics regarding digital health records. In context of these records two main classifications can be found in the literature. The first classification uses the terms electronic medical records (EMRs) and electronic health records (EHRs). Thereby, an EMR includes medical records of patients which are managed by clinicians as well as health care institutions. An EHR additionally includes health information of individuals and furthermore can be managed by individuals themselves (NAHIT, 2008). The second classification uses the terms EMR, EHR and personal health records (PHRs) whereas PHRs are intended to be moderated by the Patients (Tang et al., 2006). Throughout the remainder of this chapter we are using the term EHR to address EHRs and PHRs and patients are able to access their medical data (see Figure 1).

Figure 1 shows the actors involved in a EHR which are relevant to the content of this chapter. However, it must be noted that EHRs may additionally integrate other parties like insurances, pharmacies and other healthcare providers like laboratories, general practitioners, etc.

First of all it must be stated, that EHR applications are ranging from stand-alone applications, e.g. USB-tokens (Wright and Sittig, 2007), to web-based applications (Eichelberg et al., 2005). The latter approach usually integrates different EMRs and consequently holds all relevant medical information regarding individuals. Moreover, individuals are able to access and manage their health information via the Internet. Additionally,