Chapter 17
Information Security and Privacy in Medical Application Scenario

Sigurd Eskeland
University of Agder, Norway

Vladimir Oleshchuk
University of Agder, Norway

ABSTRACT

This chapter discusses security and privacy aspects for medical application scenario. The chapter analyze what kind security and privacy enforcements would be needed and how it can be achieved by technological means. Authors reviewed cryptographic mechanisms and solutions that can be useful in this context.

INTRODUCTION

With the emergence of information technology in health care, there has been much focus on security and confidentiality issues of electronic patient records (EPR) in medical environments. Medical records contain confidential personal information which may include sensitive data about AIDS/HIV status, sexual transmittable diseases, emotional problems, psychiatric illnesses, sexual divergences, genetic predispositions to diseases, information about toxic addictions, and so on (Rindfleisch, 1997). It is therefore essential that such information is protected from disclosure except when medical practitioners require access to patient records in order to provide proper medical care to patients. An important issue here concerns proper authorization of access to EPRs. A basic criterion for this should be legitimacy, meaning that only medical personnel providing medical care to a given patient (or patients) should be granted only access to the necessary medical data of the concerning patient they are providing care to. Another significant security issue concerns secure and confidential management, handling and storage of personal medical information (Serour, 2006).

Security of medical networks and privacy of medical data have long been topics of great concern, since almost every person would have at least one patient record containing personal and confidential medical information. The manual record keeping systems of the past lacked automatic enforcement

DOI: 10.4018/978-1-60566-030-1.ch017

of access control. Medical practitioners would necessarily not be prohibited to access arbitrary patient records, meaning that the confidentiality of patients was resting considerably on the discretion of each individual medical practitioner and legal enforcement. Today, medical data is in general managed by networked computer systems which have replaced paper-based patient records and manual record keeping systems. Health organizations and hospitals are administrating large databases of such personal electronic patient records (EPR). Computerized medical databases have a number of advantages compared to paper-based systems concerning flexibility, functionality and a more effective data management due to the possibly ubiquitous accessibility of data, independently of location and time. This complies well with decentralized organizations since data can be easily transferred within and across health establishments by means of wired and wireless computer networks.

In agreement with common medical ethics and due to the confidential nature of medical data, access to medical data should rest on a "need-to-know"-basis and legitimacy. In other words, the medical data of a patient should only be disclosed to medical personnel that have a legitimate need to access the medical data of the patient, which would be due to providing medical care to that patient. Proper measures should be taken to confine the availability of the data in agreement with the "need-to know"-principle. The increased accessibility of medical data due to digitalized data management and networked computing, rise important needs and requirements concerning the security and privacy of medical data and confidentiality of patients. Threats and violations to the privacy medical data could just as well come from within the health organization than from outside, and it is essential that proper access control mechanisms and data protection should be facilitated.

In this chapter we discuss security and privacy aspects for medical application scenario. We look at what kind of security and privacy enforcements would be needed and how it can be achieved by technological means. We review relevant issues in this context such that authorization and granting of EPR access, patient consent, access acquisition, teams, hierarchy, and related cryptographic issues.

PATIENT CONFIDENTIALITY

The confidentiality of the patient is a focal point of importance. The same applies to patients' medical records that may contain very sensitive information such as AIDS/HIV status, sexual transmittable diseases, emotional problems, psychiatric illnesses, genetic predispositions to diseases, drug addictions, etc. Electronic medical databases and networking provide an efficient data management and availability but may create needs for strengthening ethical and legal requirements correspondingly.

Patients' Rights

A significant factor related to patient confidentiality is the right the patient has to decide the course of action to be undertaken by medical practitioners or others in relation to the patient. With respect of patient confidentiality and patient consent, American Medical Association (AMA) states that "the physician's duty to maintain confidentiality means that a physician may not disclose any medical information revealed by a patient or discovered by a physician in connection with the treatment of a patient. The physician generally should not reveal confidential communications or information without the patient's express consent" (American Medical Association, 2008). Patients' right for self-determination could include:

1. An informed basis for medical treatment and medical procedures to be undertaken.