Chapter 2
Modeling Access Control in Healthcare Organizations

Efstratia Mourtou
St. Andrew General Hospital, Greece

ABSTRACT

Since Hospital Information Systems (HIS) are designed to support doctors and healthcare professionals in their daily activities, information security plays a vital role in managing access control. Efficiency and effectiveness of information security policy is crucial, especially when dealing with situations that affect the status and life-history of the patient. In addition, the rules and procedures to follow, in order to provide confidentiality of sensitive information, have to focus on management of events on any table of the HIS. On the other hand, control and statement constraints, as well as events and security auditing techniques, play also an important role, due to the heterogeneity of healthcare professionals' roles, actions and physical locations, as well as to the specific characteristics and needs of the healthcare organizations. This chapter will first explore issues in managing access control and security of healthcare information by reviewing the possible threats and vulnerabilities as well as the basic attributes of the hospital's security plan. The authors will then present a hierarchical access model that, from a security policy perspective, refers to data ownership and access control issues. The authors conclude the chapter with discussions of upcoming security issues.

INTRODUCTION

This chapter considers perhaps the most important topic in the acceptance of Information and Communication Technology (ICT) systems in healthcare. This topic covers the security from unauthorized access, the secure availability, the trust and the privacy protection of the HIS. The issues are discussed and a model access system – implemented in a Greek hospital – is presented. By understanding the key challenges and adopting strategies to improve security control policy between the user and the data of the HIS, hospi-

DOI: 10.4018/978-1-61692-895-7.ch002

talists could significantly improve the quality of healthcare. First we present the context.

In today's world there is high demand for improving both the quality of healthcare and the overall health status of individuals. National healthcare systems are facing a number of challenges in the coming years and pose great opportunities to IT professionals. Although the preservation of human life and the improvement of its quality are the subject areas of utmost importance to healthcare professionals, the provision of IT applications from research to practice, from medical procedures to palliative care and from health restoration to health preservation are some of the greatest challenges.

Health care providers are looking to IT not only to improve quality, but also to reduce costs, with efforts well under way to integrate it into the healthcare systems. For example, the Information Society in Greece (2005) reports that the West Greece sanitary district has spent € 2.570.000, 00 to implement an integrated HIS for 11 amenable hospitals and healthcare centers. However, there are many gaps in hospitals' use of IT that vary by institutional size and accreditation status. Almost 90 percent of Greek hospitals, for example, reported that they use HIS for administration transactions across a number of departments, but not in the area of clinical process and activity-based analysis. Nearly 4.87 percent of hospitals use electronic medical records and a 46,34 percent partly uses electronic lab results (Mourtou, 2007). Electronic medical records lag behind other types of hospital IT, not only because of implementation, cost, and integration difficulties, but also due to the absence of acceptance and trust by the healthcare workers.

Users' acceptance is one of the key components for success of an HIS from various perspectives. Among others, some of them are: (a) the system must become a help, not a hindrance, to all the healthcare workers (b) the system must allow fast and easy data retrieval and analysis and (c) the system must assure data quality, since clinical decisions are based on them. On the other hand a number of considerations are raised in healthcare environment, like confidentiality, privacy and ethical issues that must be properly faced. Since the patient-physician relationship depends on very high levels of trust, without proper organizational, ethical, and technological safeguards, patient information would be easily accessible to unauthorized users with intent on stealing, altering, or destroying the information contained in the HIS. In addition, important ethical questions surround the use of Electronic Medical Record (EMR) and thus, the security of HIS should be provided and used in such a manner that the rights and legitimate interests of patients are respected. Mediated access puts control policy between the user and the data and, thus, illustrates a general point that all healthcare managers should bear in mind: sound health information privacy and security access include a range of controls (Wiederhold & Bilello, 1998). Some of the security controls include:

1. Users' actions that specify what is to be done, if a situation of interest occurs
2. Roles that assign specified permissions to users to perform specific actions and rules that comprise specific conditions for actions. As Blobel & Roger-France, 2001) pointed out, "to handle any kind of user-related issues, the management of users including their specification of their possible roles and the rules applied to fulfill a security policy is needed as basis for all other application and communication security services".
3. Access levels that determine what kind of data any user can view, register and edit.

However, "access levels vary from access to the entire health record of a patient, to fine grained access definitions at the level of medical concepts" (Linden et al., 2009). Concepts in the medical domain spans levels of precision, complexity, and breadth of participation that makes the access problem more challenging than that in any other domain. The levels of access