Chapter 6
Information Security Standards for Health Information Systems: The Implementer's Approach

Evangelos Kotsonis
Adacom SA, Greece

Stelios Eliakis
Athens University of Economics and Business, Greece

ABSTRACT

Current developments in the field of integrated treatment show the need for IS security approaches within the healthcare domain. Health information systems are called to meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. At the same time, the data contained in health information systems are strictly confidential and, due to the ethical, judicial and social implications in case of data loss, health related data require extremely sensitive handling. The purpose of this chapter is to provide an overview of information security management standards in the context of health care information systems and focus on the most widely accepted ISO/IEC 27000 family of standards for information security management. In the end of the chapter, a guide to develop a complete and robust information security management system for a health care organization will be provided, by mentioning special implications that are met in a health care organization, as well as special considerations related to health related web applications. This guide will be based on special requirements of ISO/IEC 27799:2008 (Health informatics — Information security management in health using ISO/IEC 27002).

INTRODUCTION

While security of personal information is considered important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure confidentiality, integrity, auditability and availability of personal health information. This type of information is considered by many as the most security demanding, since confidentiality, availability and integrity is considered to be critical for such information in several contexts and environments. Protecting confidentiality is essential if the privacy of subjects of care is to be

DOI: 10.4018/978-1-61692-895-7.ch006

maintained. Integrity of health information must be protected to ensure patient safety, and an important component of this protection is ensuring that the information's entire life cycle is fully auditable. Availability of health information is also critical to effective health care delivery.

Because of this critical nature of requirements that characterizes health care information, all health organizations should examine whether they have established information systems that satisfy privacy, safety, security and availability requirements, regardless of their size, location and model of service delivery (Sunyaev, 2009).

When addressing these special information security needs of the health sector, a security approach should accordingly take into consideration the unique operating environment in health organizations (ISO 27799:2008). If the understanding of the security requirements is not the same for all involved parties and the security mechanisms that will be implemented do not comply with some globally accepted rules and practices, then the system that will be designed will not necessarily achieve the desired security level. Thus, it will be very difficult to interoperate with other systems, which, in the context of health care, could have lethal consequences.

Additionally, it is of general agreement that security issues should be considered very early in an e-health development process, in order to avoid risks and to facilitate the achievement of the overall e-health system (Sunyaev A., 2009). It is therefore clear that the role and contribution of international standards to the design and implementation of security in health care information systems is dominant. Standards-setting and professional regulatory organizations have been busy addressing the problems of medical privacy and the security of healthcare information from their own perspectives, but until recently a unified approach was not available in the form of an international standard, focused on managing information security in health organizations. This gap has been filed by ISO/IEC 27799:2008, which was issued by the International Organization for Standardization.

The purpose of this chapter is to provide an overview of information security management standards in the context of health care information systems and focus on the most widely accepted family of standards for information security management which is the ISO/IEC 27000 family of standards.

In the following section, an overview of standard organizations and standardization processes will be provided. Following, the ISO/IEC 27000 family of standards will be described and a focus on ISO 27001:2005, ISO 27002:2005 and ISO 27799:2008 will be provided. In the end of this chapter, a guide to develop a complete and robust information security management system for a health care organization will be provided by mentioning special implications, which are met in a health care organization in general, and special considerations related to health related web applications. This guide will be based on special requirements of ISO/IEC 27799:2008.

BACKGROUND ON STANDARDS AND CERTIFICATIONS

"Standardization is the process of developing and agreeing upon technical standards. A standard is a document that establishes uniform engineering or technical specifications, criteria, methods, processes, or practices" (Tsohou, 2009). Standards may fall into one of the following categories: International standard (a standard adopted by an international standards organization and made available to the general public), European standard (a standard adopted by a European standards organization and made available to the general public), and National standard (a standard adopted by a national standards organization and made available to the general public) (Guijarro, 2009).

The development of standards for software in healthcare has been an essential step for creat-