DEALING WITH THE COMPLEXITIES WHEN IMPLEMENTING INFORMATION SECURITY PRACTICES IN HEALTHCARE ORGANIZATIONS

Heitor Gottberg and Ivan Torres Pisa
Federal University of São Paulo (UNIFESP), Brazil

Keywords: Information Security Guidelines, Information Storage and Retrieval, Computer Security, Information Management.

Abstract: With the increasing use of electronic healthcare records and other medical systems, private and confidential information are electronically stored on different databases in several computers. A new set of processes and controls are necessary to assure the information system security and personal privacy. One of the approaches to meet these demands is to establish information security practices based on international standards. Due to the complexity of healthcare operations, managers must be aware that there are additional complexities on implementing those practices. This article depicts these additional efforts, highlighting four of the extra controls that shall be implemented: disposal of media, clock synchronization, backup, and network services – as well as threats as repudiation, theft, and terrorism that must be taken into consideration by healthcare CIOs in order to become compliant to the information security standards and, therefore, fostering the use of IT on medical practice.

1 INTRODUCTION

Currently, information security issues are increasingly calling the attention of system administrators, IT managers, software and IT services vendors. Organizations and public infrastructures depend on information systems and services that store and retrieve information in a digital way and might be vulnerable to information security threats (Cavalli, 2004).

There is also an increasing pressure for organizations to fulfil the requirements determined by the regulatory agents and institutions (e.g. Health Information Portability and Accountability Act – HIPAA) in order to assure trust and recognitions from customers and business partners. The corporate security policies must then be compliant on renowned standards, guidelines and best practices, e.g. ISO17799 (ISO, 2005), so that the organization certification of the information security controls can be accepted by other entities. Regulations are designed to prevent disastrous incidents and reduce security threats. By the nature of information security – that must prevent information leaks to happen – the corporation is impelled to act and implement a proactive information security enforcement strategy (Yip, 2006).

The wider use of clinical and administrative health information systems imposes a careful management of all aspects of security within the IT environment, including assets as hardware, software, data entry and storage, networking, and also processes and controls of information security. The essential objectives are to guarantee: (1) data integrity: i.e. the data must be protected from accidental or intentional alterations or losses; (2) data availability whenever needed by authorized users; and (3) data confidentiality: i.e. the data must only be accessible to authorized users - people or programs (Ravera, 2004). Due the reasons presented above, companies start focusing on implementing information security controls within an Information Security Management System (ISMS).

This article – based on the existing works of the International Standards Organization (ISO) – depicts part of the extra effort that is necessary when implementing information security controls and practices in healthcare organizations due the special business characteristics and demands of provisioning healthcare services.

Gottberg H. and Torres Pisa I. (2008).
DEALING WITH THE COMPLEXITIES WHEN IMPLEMENTING INFORMATION SECURITY PRACTICES IN HEALTHCARE ORGANIZATIONS.
In *Proceedings of the First International Conference on Health Informatics*, pages 205-208

2 INTERNATIONAL INFORMATION SECURITY STANDARDS

From the extent content of material produced by the ISO, including published standards, standard's drafts, and technical committees' debates; two documents will support this article to show some of the existing content around information security controls. These documents are the ISO 17799 and the ISO/DIS 27799 which are further explained below.

ISO/IEC 17799:2005 – ISO/IEC 17799 version 2005 is an internationally recognized standard that establishes guidelines and general principles for implementing information security controls as part of a corporation's ISMS. Within the document, the objectives are outlined to provide a general guidance and best practices for information security management that are commonly accepted. Control objectives and implementation guidelines are stated to drive the development of the organizations processes. Organizations seeking for ISO 17799's certification will typically develop and modify their organization security policy and processes to match the controls specified in the ISO document. In this task, those organizations will make use of assessment toolkits consisting of the standards itself and templates that ease the work of designing a control in according to the standard. While internationally, over 80,000 firms are said to be ISO 17799 compliant, apparently the companies use the ISO 17799 as a guideline, selecting some of the controls applicable to their environment. They usually do not seek the certification of the entire standard but to portions of the standard relevant to their operations (ISO, 2005). In this direction, healthcare organizations will also make a selection of the controls to be applied.

To support this adaptation task of healthcare organizations – to ISO 17799 and other themes – and provide additional and internationally accepted standards for healthcare informatics, the International Standards Organization established the Technical Committee "TC 215 - Health Informatics" with the main aim of contributing to the improvement and maintenance of health by producing those ISO standards, which the international community regards as necessary to enable the successful utilization of health Information and Communication Technology (ISO/TC215, 2000).

ISO/DIS 27799 - ISO/DIS 27799(ISO/TC215, 2006) is a standard under development by the ISO/TC 215, currently available in a "Draft of International Standard" status. It explores the specificities of implementing security management of the health sector and its unique operating environments.

According to the ISO 27799 all of the security control objectives described in ISO/IEC 17799 are relevant to health informatics but some controls require additional explanation in regard to how they can best be used to protect the confidentiality, integrity, and availability of health information. There are also additional health sector specific threats that must be analyzed when designing the institution's ISMS. The goal of this international standard is to provide additional guidance and controls, adjusting the format and terminologies. Making use of this standard, people responsible for health information security can understand and adopt in a faster (and possibly cheaper) way. Besides giving extra details to the ISO 17799 controls, ISO 27799 also states some threats to information security specifically to healthcare environments.

It is important to be aware that this standard is under development but still it can be used as reference to make tangible the extra complexity of implementing information security controls in health services provision. To do that we will choose some controls and some of the threats stated in it.

3 INFORMATION SECURITY CONTROLS

Information security controls are part of an ISMS, which implementation phases involves several steps as: ISMS design, risk identification and assessment, control selection, documenting security measurements, implementation, evaluation of measurements versus documentation, auditing, and improvement (Posthumus, 2004). These phases can be related to a Plan, Do, Check, and Act (PDCA) model, which guide the establishment and constant development of the ISMS (ISO/TC215, 2006). Figure 1 relates these steps to the PDCA cycle.

Based on Figure 1, we see that each organization must define the controls that will be part of its ISMS.

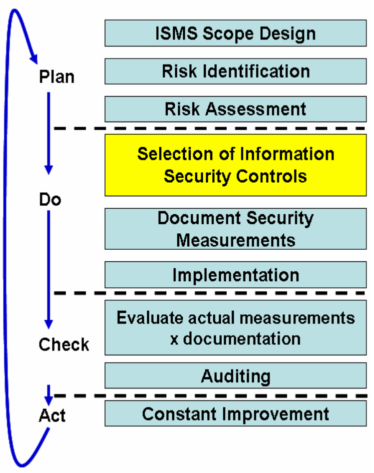
Plan
Do
Check
Act
ISMS Scope Design
Risk Identification
Risk Assessment
Selection of Information Security Controls
Document Security Measurements
Implementation
Evaluate actual measurements x documentation
Auditing
Constant Improvement

Figure 1: ISMS implementation phases.

The ISO 17799 itself states that the investments to put controls in place must be balanced to the equivalent risk that it prevents and, at the Controls Selection chapter, reinforces the idea that not all the controls of the standard must be actually implemented. In healthcare environment, this selection is equally critical and, according to ISO 27799, enhanced by the need of additional controls.

Below, four of these controls and 3 additional threats are explained, which have been selected by our comprehension that they can best exemplify the additional complexities when implementing information security practices in healthcare organizations:

Disposal of media: When disposing an information storage media or medical devices that record and report data, all personal health information must be securely overwritten or deleted, evaluating also the possibility of destroying the media. Not to pay the correct attention to this disposal continues to be a source of serious breaches of patient confidentiality. It is important to note that this control should be applied not only on disposal but also prior to the repair of any associated equipment (ISO/TC215, 2006).

An example of how critical this issue can be in healthcare is a report that focused on discarded hard drives and disk sanitization practices. It disclosed that in August 2002, the United States Veterans Administration Medical Center in Indianapolis sold or donated 139 of its old computers without removing confidential information contained on their hard drives, including the names of veterans who had AIDS and mental illnesses (Hoffman, 2006).

Clock synchronization: In healthcare operations, being able of tracing the exact timeline of happenings and activities is a must for health information systems supporting time critical care activities. The institution's IT infrastructure shall provide time synchronization services to support tracing and reconstitution of activity timelines. This information must be certified in a way that can be accepted by outside and legal entities, once the timing of events as electronically recorded in personal health information and in audit records can be relevant in processes such as coroners' inquests, investigations into medical malpractice, and other judicial proceedings (ISO/TC215, 2006).

Health information backup: In healthcare organizations, the backup of information serves not only to free storage space but attend also the regulations of future availability. If we merge this demand to the necessity of confidentiality of the stored information, we are driven to the need of a control that assure that back up of all personal health information is stored it in a physically secure environment and backed up in an encrypted format (ISO/TC215, 2006).

Security of network services: In addition the guidelines of ISO/IEC 17799, institutions dealing with personal health information should be aware of the higher impact of loosing the network service availability, e.g. impacts upon clinical practice (ISO/TC215, 2006).

These additional controls remind us that once we migrate the patient record to a digital format in an information system, the clinical practice will have this system as the fundamental tool to perform the day to day operational work. Unlike other segments, in healthcare, breaks in processes workflow due system or network crashes, are usually very near of costing lives.

4 INFORMATION SECURITY THREATS

Figure 1 above shows that to plan the ISMS it is necessary to identify and assess the risks involved at the company operations, related to digital information. Those risks relate to the threats existing on the corporate environment and processes setup.

In healthcare, there are also some additional threats that must be considered when planning an ISMS as:

Repudiation: This threat refers to users denying that they have sent or received a message. Nowadays, informatics provides us with tools to assure the preventions of this threat, such as digital signatures on prescriptions and receive/read receipts messages to emails. This assurance can become critical on flows of personal health information from one provider to the other and/or on investigations of medical practice (ISO/TC215, 2006).

Theft: Theft of data and equipment is a serious problem in hospitals. Theft may cause breaches of confidentiality, either because confidential data resides on a server or laptop computer that is subsequently stolen or, else because the data itself is the target of the theft. The threat of theft personal health information increases with the fame or notoriety of the data subject (e.g. a celebrity or head of state) and decreases with the potential severity of punitive consequences - e.g. the loss by a physician of his or her license to practice (ISO/TC215, 2006).

Terrorism: Even having no notice of wide terrorist acts to healthcare institutions, once the healthcare infrastructure is usually part of the national or regional community sustainability infrastructure, once large scale health information systems are planned, the terrorist threat must be assessed due the possible effects on increased effectiveness of bioterrorist and other attacks that cause a health-related crisis (ISO/TC215, 2006).

5 CONCLUSIONS

From the exposed above, we explain that the establishment of an information security management system, compliant to international standards, gains complexity and scope extent when we are in a healthcare organization. This statement is reinforced by the existence of a technical committee within ISO to study the specificities of the use of informatics by healthcare service providers – the ISO TC 215 – and within this group, a subgroup focusing the information security needs.

On the other hand, this additional complexity is a price to pay for the benefit of converting the patient information to an electronic form and so have the possibility of storing, retrieving, and distributing this information in an easier, faster, and cheaper way.

We must remember that provisioning healthcare services itself is one of the most complex duties in terms of managing the needs and legal regulations of integrity, confidentiality, and availability of patient information. Therefore, the additional tasks that come with the informatization of these data are a natural consequence of its nature.

This work will now continue in two steps. First we will try to identify the existing and used tools to implement the information security controls (e.g. standards toolkits and risks assessment tools). Second we will move on trying to map and score how compliant are healthcare organizations in our region to the international standards that are suggested by the Brazilian National Council of Medicine to allow the migration of hospitals to full electronic healthcare records.

ACKNOWLEDGEMENTS

We thank Mrs. Beatriz Leão (SBIS - Brazilian Association for Health Informatics) for supporting the development of this paper.

We thank also CISCO do Brasil Ltda that is supporting the participation of the main author at HealthINF 2008.

REFERENCES

Cavalli, E, et al, 2004; *Information security concepts and practices: the case of a provincial multi-specialty hospital*; International Journal of Medical Informatics (2004) 73, 297-303.

ISO, 2005; *ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management*; International Standard Organization.

Yip, F, et al, 2006; *Enforcing business rules and information security policies through compliance audits*; IEEE 1-4244-0176 - 03/2006.

Ravera, L, et al, 2004; *Security and privacy at the private multispecialty hospital istituto clinico humanitas: strategy and reality*; International Journal of Medical Informatics (2004) 73, 321—324.

ISO TC 215, 2000; *ISO/TC 215 business plan template*; International Standard Organization – Technical Committee 215 – Health Informatics (extracted from: http://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/ISO_TC_215__Health_informatics_.pdf?nodeid=1001750&vernum=0; in Feb, 24th, 2007).

ISO TC 215, 2006; *ISO/Draft of international standard 27799: health informatics — security management in health using ISO/IEC 17799, ICS 35.240.80; 2006*; International Standard Organization – Technical Committee 215 – Health Informatics.

Posthumus, L., 2004; *Use of the ISO/IEC 17799 framework in healthcare information security management*; Stud Health Technol Inform. 2004, 103:447-52 (PMID: 15747954).

Hoffman, S.; Podgurski, A., 2006, *In sickness, health, and cyberspace: protecting the security of electronic private health information*; Social Science Research Network Electronic Paper Collection (http://ssrn.com/abstract=931069).