

**The ISO/IEC 27002 and ISO/IEC 27799  
Information Security Management Standards:  
A Comparative Analysis from a Healthcare Perspective**

by

**Tembisa G. Ngqondi**

**Dissertation**

submitted in fulfillment of the requirements for the degree

**Magister Technologiae**

in

**Information Technology**

at the

**School of Information and Communication Technology**

in the

**Faculty of Engineering, the Built Environment and  
Information Technology**

of the

**Nelson Mandela Metropolitan University**

**Supervisor: Prof. Dalenca Pottas**

**April, 2009**

## Dedication

My sincerest gratitude and appreciation are extended to:

- **God, Almighty** for all the blessings he gave me;
- My Supervisor, **Professor Dalenca Pottas** for her trustworthiness, support; advice and patience. Prof. you are exceptional, thank you for your tireless support;
- My daughter **Lithemba** and my sister **Zanele** for their understanding and continuous support;
- My employer **WSU** and colleagues in my department for their support;
- My **Family** and **Friends** for their support.
- Finally, to **Debbie** for all the time she spent proofreading this dissertation.

DEPARTMENT OF ACADEMIC ADMINISTRATION

EXAMINATION SECTION

SUMMERSTRAND NORTH CAMPUS

PO Box 77000  
Nelson Mandela Metropolitan University  
Port Elizabeth  
6013



**Nelson Mandela  
Metropolitan  
University**

*for tomorrow*

Enquiries: Postgraduate Examination Officer

**DECLARATION BY CANDIDATE**

**NAME:** Tembisa Ngqondi

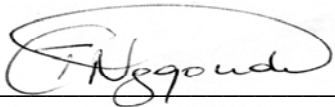
**STUDENT NUMBER:** 20008669

**QUALIFICATION:** Magister Technologiae: Information Technology

**TITLE OF PROJECT:** The ISO/IEC 27002 and ISO/IEC 27799  
Information Security Management Standards:  
A Comparative Analysis from a Healthcare Perspective

**DECLARATION:**

In accordance with Rule G4.6.3, I hereby declare that the above-mentioned treatise/  
dissertation/ thesis is my own work and that it has not previously been submitted for  
assessment to another University or for another qualification.

**SIGNATURE:** \_\_\_\_\_  


**DATE:** \_\_\_\_\_ 2009, January, 23

## Table of Contents

---

List of Figures .....	iv
List of Tables .....	v
Abstract .....	vi
<b>Chapter 1: Introduction.....</b>	<b>1</b>
1.1. Background .....	1
1.2. Problem Statement.....	6
1.3. Research Objectives .....	7
1.4. Research Methodology.....	7
1.5. Structure of the Dissertation .....	8
1.6. Conclusion.....	10
<b>Chapter 2: The Healthcare Sector.....</b>	<b>11</b>
2.1. Background .....	11
2.2. Technological Advancements in the Healthcare Sector .....	14
2.2.1. Challenges of Technological Advancements in the Healthcare Sector .....	16
2.2.2. Benefits of Technological Advancements in the Healthcare Sector .....	19
2.2.2.1. Changes in the Practitioner/Patient Relationship .....	20
2.2.2.2. Secondary Uses of Health Data .....	20
2.3. The Unique Security Needs of the Health Sector .....	21
2.4. Conclusion.....	24
<b>Chapter 3: Information Security Management Standards .....</b>	<b>26</b>
3.1. Introduction.....	26
3.1.1. Information Security .....	27
3.1.1.1. Confidentiality .....	27
3.1.1.2. Integrity .....	28
3.1.1.3. Availability .....	28

3.1.2.	Risk Management .....	28
3.1.2.1.	Risk Identification .....	29
3.1.2.2.	Risk Assessment .....	29
3.1.2.3.	Risk Treatment.....	30
3.1.3.	Information Security Management .....	30
3.2.	ISO 27002:2005 - Information Technology Security Techniques: Code of Practice for Information Security Management.....	31
3.2.1.	Introduction .....	31
3.2.2.	Terminology Used in the ISO 27002 .....	32
3.2.3.	The Difference between ISO 17799:2000 and ISO 27002:2005 .....	33
3.2.4.	The Content of the ISO/IEC 27002 .....	34
3.2.5.	The Eleven Security Clauses of the ISO/IEC 27002 .....	35
3.3.	ISO 27001:2005 - Information Technology Security Techniques: Information Security Management Systems Requirements.....	37
3.4	ISO 27799: 2008 - Health Informatics: Information Security Management in Health Using ISO/IEC 27002.....	40
3.4.1.	Introduction.....	40
3.4.2.	The content of the ISO 27799.....	41
3.5	Conclusion.....	41

**Chapter 4: A Comparative Analysis of the ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards ..... 43**

4.1.	Background .....	44
4.2.	High Level Comparison of ISO 27002 and ISO 27799 .....	44
4.3.	ISO 27002 (Sections 0 - 4) versus ISO 27799 (Introduction and Sections 1 - 6) .....	47
4.3.1.	Part I: Findings of the Comparison.....	51
4.4.	Part II: ISO 27002 (Sections 5 - 15) versus ISO 27799 (Section 7).....	52
4.4.1.	Structural Comparison .....	53
4.4.2.	Part II: Findings of the Structural Comparison .....	56
4.4.3.	Part II: Detailed Comparison .....	57
4.4.4.	Part II: Findings of the Detailed Comparison .....	58

4.5.	Part III: Comparison of Attachments Included in the Standards .....	61
4.5.1.	Part III: Findings of the Comparison of Appendices.....	64
4.6.	Critique: Contribution of ISO 27799 to Security Needs of Health Sector .....	64
4.7.	Conclusion.....	66
 <b>Chapter 5: Conclusion .....</b>		<b>68</b>
5.1.	Background .....	68
5.2.	Re-examining the Sub-Objectives of the Research .....	69
5.3.	Chapter Overview .....	71
5.3.1.	Chapter 1 - Introduction .....	71
5.3.2.	Chapter 2 - Healthcare Sector Structure.....	71
5.3.3.	Chapter 3 - Information Security Management Standards .....	72
5.3.4.	Chapter 4 - Comparison: ISO 27002 versus ISO 27799 .....	73
5.3.5.	Chapter 5 - Conclusion .....	74
5.4.	Benefits and Limitations of the Research .....	74
5.5.	Future Research.....	75
5.6.	Conclusion.....	76
 <b>References.....</b>		<b>78</b>
<b>Appendix A1.....</b>		<b>88</b>
<b>Appendix A2.....</b>		<b>124</b>

## List of Figures

---

Figure 1.1: Layout of Dissertation .....	9
Figure 2.2: Patient Support Systems in the Healthcare Sector .....	22
Figure 3.1: ISO 17799:2000 Edition and ISO 27002:2005 Updated Edition Control Objectives and Controls .....	34
Figure 3.2: Plan-Do-Check-Act Model Applied to ISMS Processes .....	39
Figure 4.1: High Level Comparison of the ISO 27002 and ISO 27799 Standards....	45

*Note that Figure 4.1 is also included as Appendix A2 (p. 124) in a fold-out format to facilitate viewing of the diagram while reading Chapter 4.*

## List of Tables

---

Table 3.1: ISO 17799:2000 Edition vs ISO 27002:2005 Updated Edition Security Clauses .....	33
Table 4.1: ISO 27002 (Sections 0 – 4) versus ISO 27799 (Introduction and Sections 1 – 6) .....	47-51
Table 4.2: ISO 27002 (Sections 5 – 15) versus ISO 27799 (Section 7) .....	54-55
Table 4.3: ISO 27002 versus ISO 27799 (Total Number of Clauses, MSCs and Controls) .....	56
Table 4.4: ISO 27002 versus ISO 27799 (Appendices) .....	62-64
Table 4.5: Summary of New Clauses, MSCs and Controls in ISO 27799 .....	65



## Abstract

---

Technological shift has become significant and an area of concern in the health sector with regard to securing health information assets. Health information systems hosting personal health information expose these information assets to ever-evolving threats. This information includes aspects of an extremely sensitive nature, for example, a particular patient may have a history of drug abuse, which would be reflected in the patient's medical record. The private nature of patient information places a higher demand on the need to ensure privacy. Ensuring that the security and privacy of health information remain intact is therefore vital in the healthcare environment.

In order to protect information appropriately and effectively, good information security management practices should be followed. To this end, the International Organization for Standardization (ISO) published a code of practice for information security management, namely the ISO 27002 (2005). This standard is widely used in industry but is a generic standard aimed at all industries. Therefore it does not consider the unique security needs of a particular environment. Because of the unique nature of personal health information and its security and privacy requirements, the need to introduce a healthcare sector-specific standard for information security management was identified. The ISO 27799 was therefore published as an industry-specific variant of the ISO 27002 which is geared towards addressing security requirements in health informatics. It serves as an implementation guide for the ISO 27002 when implemented in the health sector.

The publication of the ISO 27799 is considered as a positive development in the quest to improve health information security. However, the question arises whether the ISO 27799 addresses the security needs of the healthcare domain sufficiently. The extensive use of the ISO 27002 implies that many proponents of this standard (in healthcare), now have to ensure that they meet the (assumed) increased requirements of the ISO 27799. The purpose of this research is therefore to conduct a comprehensive comparison of the ISO 27002 and ISO 27799 standards to determine whether the ISO 27799 serves the specific needs of the health sector from an information security management point of view.

---

# Chapter 1

---

## 1 Introduction

The aim of **Chapter 1** is to provide an overview of the dissertation. This includes presenting the problem statement, research questions, objectives and the research methodology of the research project. The chapter layout of the dissertation is presented in graphical format together with a brief overview of each chapter.

### 1.1 Background

Events where individuals have had their privacy rights breached are not new in the healthcare domain (Maseti, 2008). Various incidents can be cited, viz.:

- In a report released by the Government Accounting Office in the United States (as cited in Maseti, 2008), over 40% of federal health insurance contractors and medical aid agencies reported experiencing a privacy breach involving personal health information over the past two years.
- In a recent special investigation by *The Times* newspaper, it was reported that the medical record of Dr. Manto Tshabalala-Msimang, who was Minister of Health at the time, was stolen from the private clinic where she was admitted. It was then passed on illegally to a news reporter, who used it to write an article that exposed the minister's behavior when she was admitted to the clinic (Maker & Power, 2007).
- More than a decade ago a report by the U.S. Congress (U.S. Congress, 1993) suggested that information brokering was a widespread problem and provided the example of a Medical Information Bureau, where information was gathered and banked solely for the purpose of assisting the insurance industry in making coverage exclusions in their policies.

The afore-mentioned reports and events clearly highlight the challenges of handling sensitive patient information in the health sector. Dube, Mtenzi & Shoniregun (2008) indicate that the domain of healthcare has become a challenging testing ground for information security due to the complex nature of healthcare information and individual privacy. Electronic health records stored at individual organizations are vulnerable to internal and external agents that seek to violate the security and confidentiality policies of the specific organization (National Academies Press, 1997). The vulnerability of health records raises concerns regarding the privacy and security of health information.

The National Academies Press (1997) states that privacy and security of health information concerns are classified into two categories namely:

- Concerns about the inappropriate release of information from individual organizations, whereby this can originate either from authorized users who intentionally or unintentionally access or disseminate information in violation of organizational policy, or from outsiders who break into an organization's storage system; and
- Concerns about the systemic flows of information throughout the healthcare and related industries whereby this concern refers to the open disclosure of patient-identifiable health information to parties that may act against the interests of the specific patient or may otherwise be perceived as invading a patient's privacy.

These concerns give emphasis to the reference by Dube et al. (2008) to the complex nature of healthcare information and individual privacy. In a report distributed by the U.S. Congress (U.S. Congress, 1993), the American Health Information Management Association is cited as defining *health information* or *healthcare information* as any data or information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient or other recorded subject; and 1) relates to a patient's health care; or 2) is obtained in the course of a patient receiving treatment from a health care provider, from the patient, from a member of the patient's family or an individual with whom the patient

has a close personal relationship, or from the patient's legal representative. The report further recognizes that parties who are not directly involved in patient care also gather and maintain healthcare information, for example educational institutions, the civil and criminal justice systems, pharmacies, life and health insurers, rehabilitation and social welfare programs, credit agencies and banking centres, public health agencies, and medical and social researchers.

The ISO 27799 standard defines personal health information (which excludes anonymized information) as information about an identifiable person which relates to the physical or mental health of the individual, or to provision of health services to the individual, and which may include (ISO 27799, 2008):

- a) information about the registration of the individual for the provision of health services;
- b) information about payments or eligibility for healthcare with respect to the individual;
- c) a number, or particular symbol assigned to an individual to uniquely identify the individual for health purposes;
- d) any information about the individual collected in the course of the provision of health services to the individual;
- e) information derived from the testing or examination of a body part or bodily substance; and
- f) identification of a person (e.g. a health professional) as provider of healthcare to the individual.

While it is not the intention at this stage to argue the appropriateness of or differences in the afore-mentioned definitions, the fact remains that in order to protect health information, it must be understood what precisely is constituted by the term. From the two definitions listed the complex nature of health information can be confirmed. It must be understood that the full range of health information must be protected in order to ensure that privacy and security concerns are addressed appropriately.

Nemasisi (2007) cautions that the improper use or disclosure of health information could have disastrous consequences and that there are various laws that regulate the use and disclosure of information in the health sector. The legal liability to ensure that health information is protected, cannot be ignored. Locally, notable laws include the South African National Health Act (SANHA), the Electronic Communication and Transactions Act (ECTA), and the Traditional Health Bill (Tuyikeze & Pottas, 2005). Further afield the Health Insurance Portability and Accountability Act (HIPAA) from the United States is well-known.

In order to comply with legal requirements and show that due care was applied regarding the protection of health information, healthcare organizations implement comprehensive information security programmes. Von Solms & Von Solms (2006) argue that due care can be applied by implementing some form of best practices in the protection of critically important company information assets. This can be achieved by using information security management (ISM) standards or guidelines. Widely known examples of ISM standards, include:

- ISO/IEC 27002: 2005 *Information Technology Security Techniques Code of Practice for Information Security Management*, which sets out guidance and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It contains best practices regarding control objectives and controls in information security management (ISO 27002, 2005).
- ISO/IEC 27001: 2005 *Information Technology Security Techniques Information Security Management Systems Requirements*, which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof (ISO 27001, 2005).

It should be noted that for the sake of brevity, this dissertation generally refers to the afore-mentioned standards as ISO 27001 and ISO 27002, rather than ISO/IEC 27001 and ISO/IEC 27002. This applies to other standards such as the ISO 27799 as well.

Box (2008) notes that the *Code of Practice for ISM* is well-accepted and widely adopted within industry, is used globally and is well-advocated within the security practitioner community. Siponen (2002) comments that although it is widely used, it is broadly-written, thereby failing to consider that organizations and their security needs differ. It therefore does not address unique security needs but instead, prescribes universal procedures advocated by security practitioners (Siponen, 2003). This is supported in the ISO 27002 (2005), which states that:

*“Controls can be selected from this standard or from control sets, or new controls can be designed to meet the specific needs of the organization. It is necessary to recognize that some controls may not be applicable to every information system or environment and might not be practicable for all organizations.”*

The ISO 27799 (2008) standard indicates that:

*“ISO 27002 is a broad and complex standard and its advice is not tailored specifically to healthcare.”*

For this reason, the ISO 27799 standard was released in 2008 to address the special information security management needs of the health sector and its unique operating environments (ISO 27799, 2008). The ISO 27799: 2008 (*Health Informatics - Information Security Management in Health using ISO/IEC 27002*) provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002 (ISO 27799, 2008).

Although the title of the ISO 27799 refers to the ISO 27002 only, the standard states in its *Introduction* that:

*“It is not intended to supplant ISO/IEC 27002 or ISO/IEC 27001. Rather, it is a complement to these more generic standards.”*

The standard therefore attempts to address the implementation of an information security management system (ISMS) as well, rather than addressing the ISMS in a separate standard as was done in the ISO 27001.

From the discussion it is clear that a new standard, viz. the ISO 27799 has been published to address the unique needs of the health sector in terms of information security management. This leads to an introduction of the problem statement that is addressed in this research.

## **1.2 Problem Statement**

The health sector is a vast and complex environment that handles critical health information. Health-sector-specific security requirements are encapsulated in the ISO 27799 standard. The main problem addressed in this research is whether the ISO 27799 standard serves the needs of the health sector from an information security management point of view. In order to investigate this properly the following research questions must be answered:

- How is the health sector constituted and what are the unique security needs of the health sector?
- How can these needs be addressed through proper information security management practices?
- How does the overall structure of the ISO 27002 and ISO 27799 standards differ?
- How do the eleven security control clauses and 39 main security control categories described in ISO 27002, differ in ISO 27799?
- Will the application of the ISO 27799 ensure that privacy and security of health information concerns are addressed adequately and continuously through establishing a robust information security management system?

Addressing the afore-mentioned research questions support the achievement of the main and secondary research objectives that are subsequently discussed.

### **1.3 Research Objectives**

The main objective of this research is to determine whether the ISO 27799 standard serves the needs of the health sector from an information security management point of view. This is achieved by addressing the following list of secondary objectives that support the primary objective:

- Investigate the health sector and the special needs of health information security.
- Examine information security management practices in general as well as in the health sector.
- Perform a high level comparison of the ISO 27002 and ISO 27799 standards.
- Execute and document the results of a detailed comparative analysis of the security control clauses in both standards.
- Determine the approach of the ISO 27799 in regard to the establishment of an information security management system.
- Based on the afore-mentioned actions, critique the contribution of the ISO 27799 to serving the security needs of the health sector.

In order to achieve these objectives, the following research methods were applied.

### **1.4 Research Methodology**

Two research methods were used to achieve the objectives of this study, viz. literature review and comparative analysis. The literature study was conducted to review secondary literature about the topics relevant to this research. This includes:

- The health sector and its special security needs;
- Information security management standards and best practices;
- Establishing an information security management system; and
- Information security management as pertaining to the health sector.



The sources used to do the literature review were selected based on availability and trustworthiness.

After a clear understanding of the health sector, its security needs and information security management practices were established, a comprehensive comparative analysis of the ISO 27002 and ISO 27799 standards was executed and documented. According to Hofstee (2006), when doing a comparative analysis, the researcher investigates in a focused and systematic manner two, sometimes three items in depth and compares them to each other to find differences or similarities. This approach suits the objective of this research. The case for comparing the two standards as a means of serving the objective of the research is based on:

- The fact that the ISO 27002 standard is a recognized and widely used international standard for information security management.
- The fact that the ISO 27799 is based on the ISO 27002.

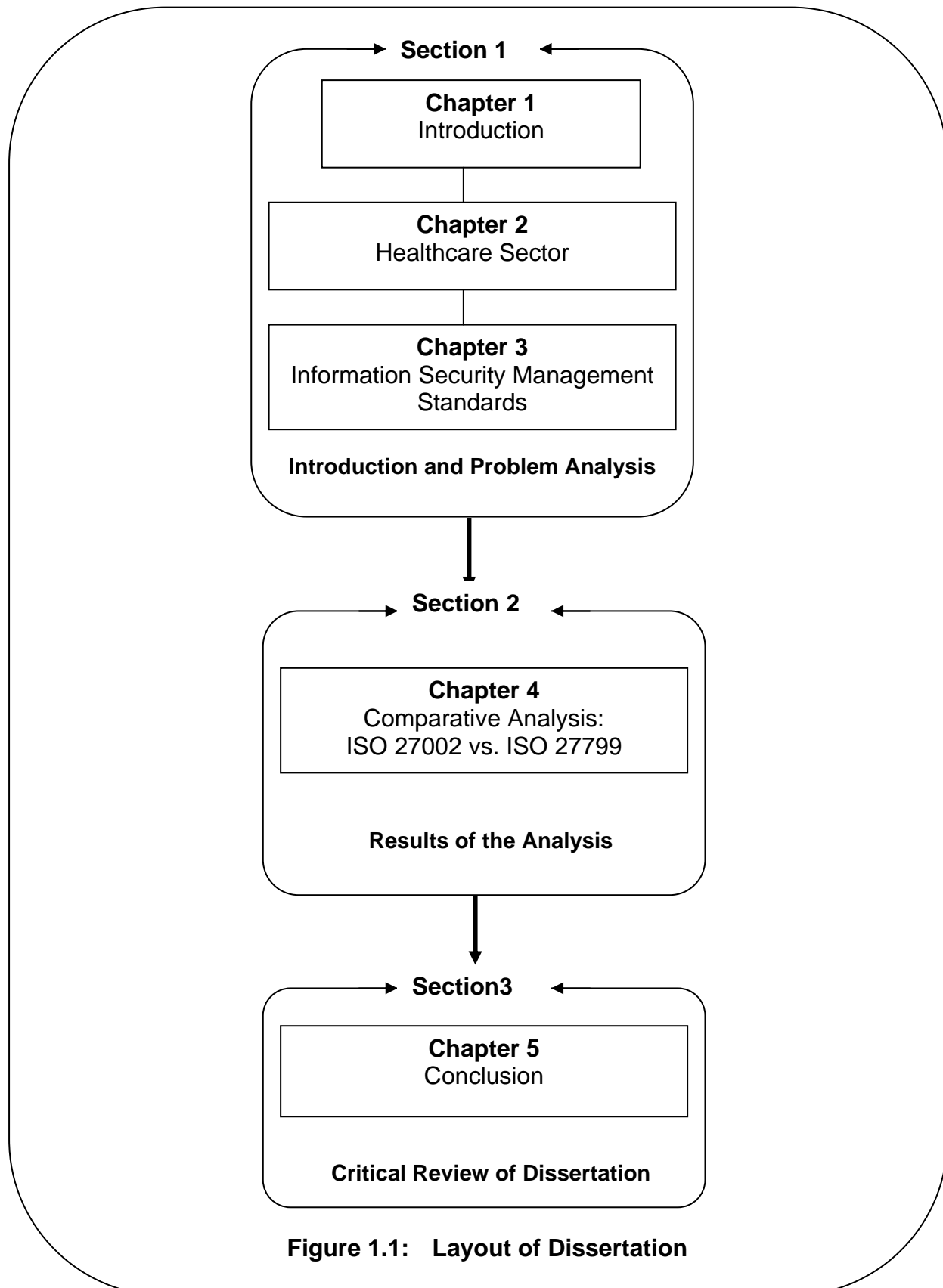
The comparison of the standards identifies aspects that were added (through modification or addition) to provide guidance to healthcare organizations. This allows the researcher to critique the contribution of the ISO 27799 in regards to serving the information security management needs of the health sector.

## **1.5 Structure of the Dissertation**

The layout of the dissertation is divided into three sections and five chapters and is depicted in Figure 1.1.

Section 1 is comprised of the first three chapters of the dissertation and covers the background of the research area. Chapter 1 provides a brief introduction of the dissertation and expounds the problem statement, objectives, and methodology of the research. Chapter 2 discusses the nature of the health sector, investigates technological advancements in this sector and the challenges and benefits of the changes brought about by these advancements. The importance of protecting personal health information is confirmed. Chapter 3 introduces risk management and information security management and provides an overview of the relevant

standards. It also explicates the advancement of the standards through various editions.



**Figure 1.1: Layout of Dissertation**

Section 2; Chapter 4, constitutes the solution of this dissertation and reports on a comprehensive comparative analysis of the ISO 27002 and ISO 27799 standards.

Section 3, Chapter 5 constitutes the conclusion of the dissertation. This chapter summarises what has been covered in the dissertation and shows how the objectives itemised in Chapter 1, were achieved. It presents a critical review of the dissertation. The chapter further considers proposals for future and continued research in this area.

### **1.6 Conclusion**

The purpose of this Chapter was to introduce the reader to the broader research area of this project and then narrow it down to the problem statement. This was achieved in Sections 1.1 and 1.2. Section 1.3 indicated the main objective and sub-objectives of this research. The research methods that are applied towards reaching the intended outcome of the research were discussed in Section 1.4. In Section 1.5 a high-level outline of the dissertation was provided. In the next chapter this groundwork is further expanded by reporting on the literature study conducted about the health sector and its security needs.

# Chapter 2

---

## 2. The Healthcare Sector

The aim of **Chapter 2** is to investigate the nature of the health sector, highlight technological advancements in this sector and the challenges and benefits related to these advancements. The importance of security and the unique security needs in the health environment are explored.

### 2.1 Background

The healthcare sector is seen as one of the most complex business areas with diverse types of interactions (Gomes & Lapão, 2008). Langabeer (2008) highlights that the healthcare sector is a business because:

- It manages the same set of business resources as other types of organizations, including financial resources, personnel, equipment, supplies, technology and facilities;
- It employs a large complement of staff and has a large payroll;
- It serves as a marketplace and supplies valuable services to hundreds of customers daily;
- It procures a vast array of supplies, both pharmaceutical and technological;
- Time, people, money and business processes are managed to function efficiently;
- It is an economic engine that generates significant cash flows and provides economic value.

The healthcare sector resembles a jigsaw consisting of a large number of pieces and it is difficult to see the whole healthcare picture without fitting all the pieces together (Solanas & Castellà-Roca, 2008).

Health systems and the healthcare sector are defined by a set of activities whose intent it is to improve or maintain health, enhance responsiveness and assure fairness of financial contribution (Murray & Frenk, 2000). Murray et al. (2000) expound these components as follows:

- The improvement of health involves both increasing the average health status and reducing health inequalities;
- Responsiveness includes respect for persons and comprises dignity, confidentiality, the autonomy of individuals and families to decide about their own health, and client orientation which comprises prompt attention, access to social support during care, quality of basic amenities and the choice of a provider;
- Fairness of financial contribution means that every household pays a fair share of the total health bill for a country and this means that poor households may pay nothing. This implies that everyone is protected from financial risk due to healthcare costs.

According to Dr Margaret Chan, Director-General of the World Health Organization, there is a growing appetite among policymakers for knowledge related to how health systems can become more equitable, inclusive and fair, which reflects a fundamental shift towards the need for more comprehensive thinking about the performance of the health system as a whole (World Health Organization [WHO], 2008).

The World Health Report (WHO, 2008) stresses the benefits of using information and communication technologies to improve access, quality and efficiency in primary care. Like any other organization, healthcare organizations need information to make informed decisions.

The healthcare sector is not limited to the electronic record - both electronic and manual or paper-based records are used (Australian General Practice Network, 2007). Both electronic and manual records may serve as input to decisions in healthcare. A decision taken in one unit or entity will at some stage, be informed by information from other entities. Each entity may access healthcare information in different available formats. For example, a doctor in a hospital (using an electronic

health record) may use paper-based information from a clinic to attend to a patient referred by a primary healthcare worker who works at the clinic. This illustrates how the decisions taken in one entity of the healthcare sector may serve as input to another entity and that information about the patient informs the decision-making process. The Canadian Institute for Health Information [CIHI] (1996) maintains that effective decision making in the health organisation is dependent upon relevant, timely, accurate, accessible and comprehensive information.

The reality is that throughout a patient's lifetime, healthcare services may typically be provided by a number of healthcare providers. In the case of a lack of integrated healthcare systems, this may mean that a patient has various medical records owned by different healthcare providers. These records could also be in different formats. Each time that patients visit a new healthcare provider, they may have to give an account of their prior medical history. This may lead to a number of problems, for example (Sprague, 2004; Tessier, 2004; Waegemann, 2007):

- The physician may be “practicing medicine blindly”. Care is provided to the patient without knowledge of what has been done previously and by whom; this results in both wasteful duplication and clinical decisions that do not take into account critical data related to the health of the patient;
- Tests may be repeated because there is no record of them having been done. This is a waste of time and money;
- The paper-based systems that are still in use create redundancy issues, data inconsistencies, inaccurate and incorrect patient information, security issues, lost records and storage issues.

Nations globally are reforming their healthcare systems with the intention of developing automated systems which are more outcome focused, integrated, and promote accountability (CIHI, 1996). A healthcare system must provide the right services to the right people in the most cost effective manner.

Automated systems can be effective only if organisations, including the healthcare sector, use new Information Technology (IT) advancements (Gomes & Lapão, 2008).

It is not sufficient to improve the efficiency of the current processes. These new technologies, including various pioneering means of communication, can provide opportunities to develop and expand IT support for the care process (Perjons, Wangler, Wäyrynen, & Ahlfeldt, 2005). Technological advancements in the healthcare sector are subsequently discussed in Section 2.2.

## **2.2 Technological Advancements in the Healthcare Sector**

Technological advancement in the healthcare sector was initially introduced to improve healthcare administrative processes. Information systems in the healthcare sector, from the business perspective, were initially built to be used at a secondary level for administrative and organisational processes. They were not built to be used at a primary level to support patient care (Hübner & Elmhorst, 2008). Medical informatics dates back to the 1960s when computers were first introduced into hospitals to support healthcare administrative tasks (Wagner, 1999). Langabeer (2008) notes that technology should be considered wherever quality and efficiency is low and further points out that it is important to replace all viable and repetitive processes by less expensive or cost effective automation technology.

Many healthcare administrative and medical duties are repetitive and can be improved by using the relevant automated technology to improve quality and service delivery. Health informatics helps doctors with their decision-making and actions, and improves patient outcomes by making better use of information and by making efficient the way patient data and medical knowledge is captured, processed, communicated, and applied (Sullivan & Wyatt, 2006). Solanas et al. (2008) state that many new technologies are continuously being incorporated into the health sector with the aim of making it better. Some of these technologies are mainly devoted to improve the exactness of the diagnosis while others are mainly devoted to the management of medical records.

Various authors agree that there is a need for technological advancements in the healthcare sector, but the question is, how will this technological advancement improve the quality of service in the various units in the healthcare sector? Hübner &

Elmhorst (2008) maintain that technological advancements will be implemented through information technology tools that are relevant to the healthcare sector. These tools include the following (Hübner et al., 2008):

- **Electronic Health Record**

The concept of the Electronic Health Record (EHR) forms a core element of Information and Communication Technology (ICT) developments in the healthcare sector. It is sometimes referred to as an Electronic Patient Record (EPR). The EHR assumes the role of a data repository that allows different applications to access all the patient-related records in an integrated manner. The importance of the EPR is underlined by the fact that a growing number of countries are setting up national plans for EPR systems to both aid the flow of information supporting the complete care process within a healthcare organisation and facilitate shared care across organisational borders.

- **Networking and Telemedicine**

A network system in the form of intra- and extranets together with the Internet facilitates interdisciplinary cooperation. The hospital intranet system can be used, for example, to send radiological images simultaneously to the treating clinicians, so that while the radiologist is working on a diagnosis, the clinician can have an independent view of the image and converse with the radiologist.

- **Electronic Health Card**

The Electronic Health Card comprises a chip card containing the administrative and/ or medical data of the patient. This card can exist either as a practitioner-held card, which the practitioner keeps and uses as the EPR, or as a patient-held card, which creates the possibility of a portable health record, through which the patient may give access to her/his complete or partial medical record to any practitioner.

- **Decision Support Technologies**

The development of software and ICT tools for the medical specialist allows for the development of decision support systems, which strengthen the diagnostic



capacity of individual practitioners. Such technologies can, for example, suggest diagnoses, provide reminders for checkups and preventative measures, or alert practitioners to side-effects.

- **Medical Databases**

The establishment of large medical databases that have been extracted and aggregated from individual clinical and administrative data can enhance healthcare evaluation, public health observation and epidemiology. These databases may be used, for example, to trace the long-term effects of certain drugs, the courses of particular diseases, the outcomes of particular medical interventions, and plot disease incidence.

- **The Internet**

The Internet has made access to health information easier for patients and practitioners regardless of their location. Citizens use it for their own health education and participation in healthcare. It helps the practitioner to provide advice to their patients without a long waiting period for the results to be received.

These information technology tools have brought changes that are both positive and negative to the healthcare sector. Nevertheless, they help stakeholders in the healthcare sector to interact more efficiently. They improve this sector's reliability, efficiency and quality (Solanas et al., 2008). While it cannot be negated that there is an improvement in the healthcare systems, there are also challenges that have been brought about by these changes.

### **2.2.1 Challenges of Technological Advancements in the Healthcare Sector**

There are several roles in the healthcare sector that technological advancements have served according to Langabeer (2008). These include automating manual processes, to improve transaction processing capabilities and to improve the quality of analysis, reports, and decision-making. It is to be expected that such advancements (e.g. improved transaction processing capabilities) brought about changes in the healthcare sector, which in turn gave rise to a number of challenges.

The following challenges are examples of those that are introduced by technological advancements:

- Resistance to change

It seems to be part of the human makeup to be most comfortable with the status quo unless that status quo inflicts discomfort (O'Carroll, Yasnoff, Ward, Ripp, & Martin, 2002). The technological advancements in the healthcare sector, introduced a new means of operation to support business activities. This change required all people who operate the system to acquire additional computer skills which is currently a problem in the healthcare sector. O'Carroll et al. (2002) indicate that the different attitudes which cause resistance to occur are due to various assumptions by the users and these include that:

- The new system will cause a reduction in their authority;
- It will change the management reporting structure;
- It will cause the work to become more difficult;
- It will force users to learn new skills; and finally
- The current system appears sufficient.

- Financial Challenges

The introduction of ICT tools to the healthcare sector has brought a shift to their business processes. The reform in the healthcare sector in many countries has brought a substantial cost increase in health sector resources (Blas, 2002). Healthcare resources are not limited to the institution that finances or provides services, but include a diverse group of organisations that provide input to those services, particularly human resources, physical resources such as facilities and equipment, and knowledge (Murray et al., 2000). The financial impact on these resources includes the following:

- Human resources – the healthcare sector must secure funds for the ongoing training of staff because technology is constantly changing.
- Equipment and facilities need to be frequently maintained and upgraded to comply with new hardware and software needs which originate from third

parties and from the internal organizational perspective. This is costly because the third party and the healthcare systems are integrated for some business processes and should the third party change its equipment this has an effect on the healthcare systems.

- Information costs are particularly high for data that is captured by health professionals using the structured coded representation that is often required by a computerised record system. The cost of this information is expensive because it takes more time to capture coded data and it may cause difficulties in interpretation for secondary use of the data.
- Erroneous information in regard to the health supply chain can be costly to the organization. A patient may be given an incorrect prescription because the patient data is error-prone or incomplete. This refers to patient data which was previously captured and may cost the organisation the life of the patient.

- **Security and Privacy Challenges**

The intersection of ethics and health informatics introduces issues of privacy and confidentiality. These issues concern people, scientists and laypeople (O'Carroll et al., 2002). Healthcare, by its nature, requires that privacy and confidentiality are considered in different ways from those accustomed to. O'Carroll et al. (2002) maintain that the core problem with confidentiality and the electronic health media comprises the dilemma between simultaneously making information easily accessible to the appropriate users and inaccessible to the inappropriate ones. This is problematic because the means for accomplishing the one are in conflict with the means for accomplishing the other.

The list of challenges relating to technological advancements in the healthcare sector varies between countries. Developed countries that have enough financial support may, for example, not experience the same financial and other challenges that are experienced by developing countries. However, it applies to all healthcare institutions that they have a large amount of information that needs to be handled to perform their tasks and that technological advancement is their common solution to this challenge (Perjons et al., 2005).

Despite the challenges; there are a number of benefits that technological advancement has brought to the healthcare sector. A variety of these benefits is discussed.

### **2.2.2 Benefits of Technological Advancements in the Healthcare Sector**

Data stored in paper-based repositories was fragmented, unstructured, used incompatible terminologies, separated clinical and administrative data and caused a break-up of patient data over time and space (Rodrigues, 2000). The arrangement of these non-automated repositories prevented optimal use of the wealth of data it contained. Technological advancement has improved the storage structure of the records of patients by collecting automated patient data which is accurate, comprehensive, standardised, timely and accessible (AGPN, 2007).

According to the Australian General Practice Network, data must have the following characteristics to be useful (AGPN, 2007):

- Accurate when it is both valid and reliable, and can be validated by both patient and medical professional;
- Comprehensive when it provides a complete record or summary of medical history and treatment of the patient and is ready for use in the next domain;
- Standardised when it is collected using common terminologies which enables it to be directly compared with other data;
- Timely when it is available to the healthcare providers at the appropriate time and is ready for use;
- Accessible regardless of the ownership, and with due consideration to patient privacy. It must be available to support all healthcare units that need it for their decision making including administration, research, policy and strategy, clinical interventions and similar.

Wagner (1999) states that automated tools introduced an integrated filing system which provides improved access, retrieval and storage of patient records. The electronic recording of data facilitates its transmission and sharing between

practitioners and relevant third parties, for clinical, administrative, statistical, and for research purposes. Tools, such as electronic health records, computerized prescribing systems and clinical decision aids, support practitioners in providing safer care in a range of settings; for example, in a village in western Kenya, electronic health records integrated with laboratory, drug procurement and reporting systems have drastically reduced clerical labour and errors, and have improved follow-up care (WHO, 2008).

Integrated systems have also brought changes to the governance of the healthcare sector, where the integration of rural and urban hospital systems has provided opportunity for alliances (Savage, Taylor, Rotarius, & Buesseler, 1997). The integration of systems has contributed to rural hospitals being able to survive. Fujitsu (2006) and Wagner (1999) agree that technological advancements in the healthcare sector have championed a variety of benefits. Changes (for the better) in the practitioner / patient relationship and improved secondary uses of personal health data are further benefits which are subsequently discussed.

### **2.2.2.1 Changes in the Practitioner/ Patient Relationship**

Computers have become an integral feature of the interactions between practitioners and their patients through the development of the EHR and other software to support the daily administrative work of medical practitioners (Wagner, 1999). Sullivan et al. (2006) and Savage et al. (1997) maintain that people with health concerns do not have to become patients by consulting a health professional, because electronic health tools provide access to many of the resources that can satisfy their needs. New applications, services and access to information have permanently altered the relationships between consumers and health professionals, putting knowledge directly into people's own hands (WHO, 2008).

### **2.2.2.2 Secondary Uses of Health Data**

The secondary uses of health data include health administration, cost containment, reimbursement, health policy, quality care auditing, epidemiological and other

studies. ICT tools support the secondary use of health data to achieve the following benefits (Aydin, Harmsen, Slooten, & Stegwee, 2004):

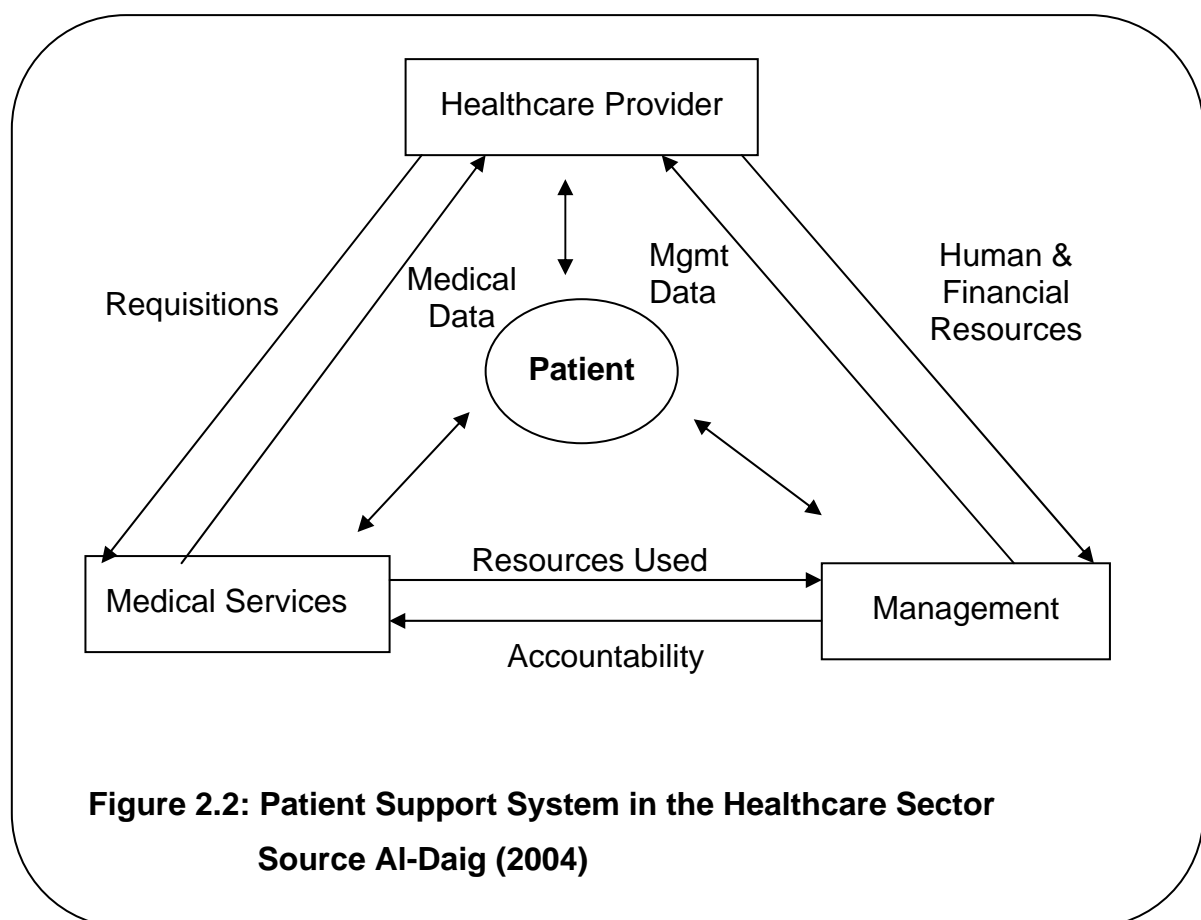
- Improved efficiency at both clinical and managerial level, by allowing greater visibility of work and avoiding duplication;
- Improved quality assurance activities and programs which control the performance and practice of healthcare professionals;
- The use of patient profiles as a basis for health policy decision-making;
- Faster access, retrieval and distribution of patient information;
- Improved privacy of patient information through controlling and tracking access to this data which produces accurate audit trails that demonstrate regulatory compliance;
- Reduced physical storage requirements for patient health information;
- Reduced costs associated with photocopying, faxing or using courier services to transport patient information.

Even though technological advancements in the health sector have led to major benefits in a number of areas, it also exposes personal health information to various threats. The prospect of storing health information in electronic form raises concerns about patient privacy and data security (Smith & Eloff, 1999). Section 2.2.1 identified security and privacy as a challenge of technological advancements in the health sector. Section 2.2.1 further indicated that healthcare, by its nature, requires that security and privacy be considered in ways different from those accustomed to. This statement is subsequently expounded in terms of the unique security needs of the health sector.

### **2.3 The Unique Security Needs of the Health Sector**

Ever since healthcare information systems have been implemented, their security has been considered as an important issue, especially in the light of the fact that their data are deemed to comprise extremely sensitive information (Smith & Eloff, 1999). Al-Daig (2004) maintains that the patient is a focal point of the healthcare sector and that health information must receive priority when it comes to privacy and

security. Al-Daig (2004) further indicates that the unique security needs of healthcare should be investigated by looking at the diverse structures that support healthcare activities as illustrated in Figure 2.2. Section 2.1 of this chapter indicated that decisions taken in one unit are informed by information from other entities. Figure 2.2 illustrates that patient information is handled by different units in the healthcare sector. These include healthcare providers, medical services and management units. Each of these units may include other units, entities and individuals.



Healthcare providers may include internal and external healthcare suppliers, medical services may include doctors, nurses, therapists and all of the same, and management may include administrators, personnel, finance and all the entities dealing with different administration duties including the management of the organisation. In Figure 2.2 the arrows between the patient and the different units demonstrate the flow of patient information, hence it is indicated that the starting

point of protecting the security and privacy of patient information should be by understanding all the contributing factors to the patient information. Understanding contributing factors to patient information implies that there is a need for a holistic view of handling information security in the healthcare sector.

The nature of the healthcare environment is one component that influences the unique security and privacy needs of the healthcare sector. The other important aspect is the sensitivity of patient information.

According to Ahlfeldt (2006) there are two aims concerning information security in healthcare, which are to:

- Reach a high level of security, i.e. to give patients opportunities for the best care with right information available at the right time; and
- Reach a high level of patient privacy; i.e. to protect patients from sensitive information being distributed to unauthorized persons.

Janczewski & Xinli Shi (2002) confirm that the healthcare sector has some unique characteristics in terms of information security, which include:

- Sensitivity of electronic medical records;
- Large number of small organisations;
- Multiple providers and multiple locations;
- Relaying health information;
- Data-dependent access;
- Status of privacy legislation; etc.

The third component which influences the unique security and privacy needs of the healthcare sector is the ever-evolving legal compliance requirements posed by laws and guidelines. Internationally, legislators have recognised the problems in terms of data protection and transmission of health data and have taken action by issuing various data protection acts (Smith & Eloff, 1999), for example, the American Health Insurance Portability and Accountability Act (HIPAA). HIPAA came into law on



August, 21, 1996. Its primary focus is to mandate that healthcare information becomes portable and available (but protected) by legislating the use of uniform electronic transactions and other protective and administrative measures.

In Australia, concern about the detail of laws to protect patient privacy has resulted in an overlap of state and federal government privacy jurisdictions, creating complexity and confusion in the health privacy legislative environment (Fernando, 2004). Laws for the protection of citizens in healthcare differ from country to country, since they reflect the diversity in long-standing cultural traditions, of medical secrecy, ownership of medical data, patient autonomy, professional liability, etc. (Wagner, 1999).

It can be concluded that the security needs of the health sector requires appropriate guidelines and principles to be applied to ensure that the security and privacy of personal health information is protected.

## **2.4 Conclusion**

The purpose of Chapter 2 was to investigate the health sector and the special needs of health information security. It was shown that technological advancements in the sector have culminated in major benefits for the sector, but also uprooted some challenges. One of these challenges, namely protecting the security and privacy of personal health information, is the focus of this research. The sharing of information among different units of the healthcare sector is a growing area of concern in terms of information security. Shared patient information must be protected from any threat that can lead to violation of the dignity of the patient. The Tshabalala-Msimang incident referred to in Chapter 1, Section 1.1, serves as a case in point.

As mentioned in Chapter 1, healthcare organizations implement comprehensive information security programmes based on information security management standards, best practices and guidelines in order to comply with legal requirements and to show due care in the protection of health information. Based on the discussion of the unique security needs of the health sector in Section 2.3, it is clear that information security management (ISM) and the implementation of an

information security management system (ISMS), are indispensable for health organizations to satisfy their security needs. Chapter 3 further investigates the concepts of ISM and ISMS and in particular, international standards of relevance to these topics.

---

# Chapter 3

---

## 3. Information Security Management Standards

The aim of **Chapter 3** is to discuss information security management and to provide an overview of the relevant ISO standards namely; ISO/IEC 27002: 2005 (*Information Technology Security Techniques - Code of Practice for Information Security Management*), ISO/IEC 27001: 2005 (*Information Technology Security Techniques - Information Security Management Systems Requirements*) and ISO 27799: 2008 (*Health informatics - Information Security Management in Health using ISO/IEC 27002*).

### 3.1. Introduction

Gerber, von Solms & Overbeek (2001) define information security as the process of controlling and securing information from unplanned or malicious changes and deletions or unauthorised disclosures. Information security is further defined as all the aspects that relate to achieving and maintaining confidentiality, integrity, and availability (ISO 13335-1, 2004). These aspects of information security can be achieved successfully if the effort aimed at minimizing the chances of a security breach and its potentially adverse effects (i.e. *risk management*), are well managed (Taylor, n.d.). Risk management forms an integral part of Information Security Management (ISM).

It should be noted that in this study, risk management is considered in the context of ISM. While risk management is a subject of numerous security standards, this dissertation only considers the ISO27k standards that have been listed (viz. ISO 27002, ISO 27001 and ISO 27799). Risk management standards are not

included in the study, but risk management is discussed to explicate its relationship with ISM.

Information security management comprises controls that organisations need to employ to ensure that they are sensibly managing risks (Schlarman, 2002). It is a business issue and an integral part of managing risk, and establishing, implementing and operating an Information Security Management System (ISMS) (NSW Department of Commerce, 2007). The NSW Department of Commerce further emphasizes that the information assets of an organization cannot be appropriately safeguarded if the organization does not recognise that information security management is a business issue. This implies that the organization is vulnerable to attacks should it not employ some form of information security management.

It is important to elaborate on the concepts of information security, risk management and information security management, to show how they relate to each other and to show how they apply in the healthcare context.

### **3.1.1 Information Security**

The term information security is often divided into the three components of confidentiality, integrity and availability. A brief definition of each of these terms follows.

#### **3.1.1.1 Confidentiality**

Confidentiality relates to information not being accessible or revealed to unauthorised people (Wallin & Xu, 2008). According to Buckovich, Rippen & Rozen (1999), confidentiality is a status afforded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or both, and must be disseminated only to authorised individuals or organisations.

In the healthcare context information must be available strictly on a need-to-know basis and therefore its confidentiality must be protected as a fundamental requirement.

### **3.1.1.2 Integrity**

Integrity is the safeguarding of the accuracy and completeness of information (Carlson, 2008) and its processing methods. According to Wallin & Xu (2008), integrity concerns protection against undesired changes. The integrity of information is imperative in healthcare as information guides healthcare staff members with decision-making. Incorrect healthcare information can result in hazardous events like death of patients, or patients being prescribed the wrong medication.

### **3.1.1.3 Availability**

Availability is ensuring that authorised users have access to information and the associated assets when required (Carlson, 2008). According to Wallin & Xu (2008), availability concerns the expected use of resources within the desired time frame. For healthcare organisations to function properly, healthcare information needs to be accessed by authorised stakeholders whenever the need arises. Healthcare organisations, therefore, must ensure that the availability of information is not compromised.

It is impossible for an organisation to deal with information security without considering risk management. The concept is briefly described before expanding on the activities it comprises in Sections 3.1.2.1 – 3.1.2.3.

## **3.1.2 Risk Management**

Risk management comprises coordinated activities which direct and control an organisation with regard to risk. The Nonprofit Risk Management Center (2008) defines risk management as a discipline for dealing with the possibility that some future events will cause harm. Risk management as defined by major risk management organisations in the UK, clearly indicates that it gathers an

understanding of the potential benefits and disadvantages of the factors which can affect an organisation (Association of Insurance and Risk Managers [AIRMIC], National Forum for Risk Management in the Public Sector in the UK [ALARM], & Institute of Risk Management [IRM], 2002). Information security risk management ensures that the correct assets are being identified and risks are quantified accurately to ensure their appropriate mitigation or acceptance (Wallin & Xu, 2008).

The basic risk management activities typically include risk identification, risk assessment and risk treatment. These are discussed.

### **3.1.2.1 Risk Identification**

The risk identification process uses real-time data to identify vulnerabilities and threats related to security technology, people, and processes (VeriSign, 2008). AIRMIC, ALARM and IRM (2002) indicate that risk management should be approached in a methodical way to ensure that all important activities within the organisation have been identified and all risks flowing from these activities are defined. Once the risks have been identified, they must then be assessed as to the potential severity of loss and the probability of their occurrence.

### **3.1.2.2 Risk Assessment**

Risk assessment assesses the severity of loss and the probability of occurrence after the risk has been identified (Wikipedia<sup>a</sup>, 2008). ISO 27002 (2005) highlights that risk assessment should:

- Include a systematic approach to estimate the magnitude of risks (risk analysis);
- Include comparison of the estimated risks against risk criteria to determine the significance of the risks (risk evaluation);
- Be performed periodically to address changes in the security requirements and in the risk situation;
- Be undertaken in a methodical manner capable of producing comparable and reproducible results.

Once the risks have been identified and assessed, the organisation must seek potential treatment for the risks.

### 3.1.2.3 Risk Treatment

Risk treatment is the process of selecting and implementing measures to modify the risk (AIRMIC, ALARM, & IRM, 2002). Wikipedia<sup>a</sup> (2008) indicates that risk treatment includes several techniques to manage risk to the organization and that these techniques fall into one or more of the following categories:

- Risk avoidance which includes not performing an activity that could carry risk;
- Risk reduction which involves the methods that reduce the severity of the loss or the likelihood of the loss from occurring;
- Risk retention which involves accepting the loss when it occurs. It is a valuable strategy for small risks where the cost of insuring against the risk would be greater than the total losses sustained; and
- Risk transference which involves the transference of the risk to another party.

Implementation of these techniques to manage risks to the organization can reduce the likelihood of a wide range of threats and consequently lessen the adverse impact on the information systems of the organization.

One of the key deliverables of the risk management process is a register of risks. This clearly identifies major risks that need to be addressed and underscores how risk management relates to information security management. Information security management cannot identify the best information security management controls without identifying the relevant risks.

### 3.1.3 Information Security Management

Information security management is informed or guided by various recognized ISO standards that help the organization to identify the best information security practices for their business activities. The International Standards Organisation (ISO) is a network of national standards bodies for over 150 countries. The central secretariat,

which coordinates the network, is based in Geneva, Switzerland. It is a non-governmental organization, with the letters “ISO” representing 'International Organization for Standardization'. The letters are derived from the Greek word, 'isos', which means equal. The forerunner of ISO, the International Electrotechnical Commission (IEC), was established in 1906. The ISO was officially founded in 1947.

The ISM standards published by the ISO that are of relevance to this research and constitute the rest of the discussion in this Chapter are:

- ISO 27002: 2005 - *Information Technology Security Techniques: Code of Practice for Information Security Management;*
- ISO 27001: 2005 - *Information Technology Security Techniques: Information Security Management Systems Requirements;*
- ISO 27799: 2008 - *Health Informatics: Information Security Management in Health using ISO/IEC 27002.*

These standards are introduced in Sections 3.2, 3.3 and 3.4 respectively as a precursor to the detailed comparative analysis of the ISO 27002 and the ISO 27799 standards that is reported on in Chapter 4.

## **3.2 ISO 27002: 2005 - Information Technology Security Techniques: Code of Practice for Information Security Management**

### **3.2.1 Introduction**

The ISO/IEC 17799: 2005 was renumbered as the ISO/IEC 27002: 2005 in the middle of 2007 to bring it into the ISO/IEC 27000 family of standards. The text remains identical to the ISO/IEC 17799: 2005 and in fact, the exact ISO/IEC 17799 standard is sold together with a cover sheet noting the change of number.

The ISO 17799 Information and Resource Portal describes the ISO 17799 security standard as the most widely recognized security standard (Kokolakis, Demopoulos, & Kiountouzis, 2000). It is based upon the British Standard Institution's BS 7799 standard which was last published in May 1999 as an edition which, itself, included



many enhancements and improvements on its previous versions (Frangopoulos, & Eloff, 2004). The ISO 17799 was initially published in December 2000. The most recent updated version was published in June 2005 as the ISO/IEC 17799: 2005. As mentioned above, this version was renumbered during 2007 and is now known as the ISO/IEC 27002: 2005.

### 3.2.2 Terminology Used in the ISO 27002: 2005

The ISO 27002 uses a number of terms which denote and comprise the structure of the standard. These terms are carried forward to the ISO 27799 and are used throughout the rest of this dissertation. It is therefore important to provide an explication of these terms as per the ISO 27002 (2005).

#### Security Clause

A security clause defines a key area to consider when implementing IT controls, for example, *Access Control* is one of the security clauses of the ISO 27002. Security clauses are sometimes referred to as security domains. The ISO 27002 standard lists eleven (11) security clauses or security domains. For each security clause, a comprehensive set of information security best practices are provided in the form of *Main Security Categories (MSC)*.

#### Main Security Category

Main security categories are sometimes referred to as sub-domains of security clauses or domains. Each main security category contains:

- a) a control objective stating what is to be achieved; and
- b) one or more controls that can be applied to achieve the control objective.

The control objectives in effect comprise a generic functional requirements specification for an organization's information security management controls architecture. In the ISO 27002, the *Access Control* security clause has seven *MSCs*, one of which is *User Access Management*. The *User Access Management* *MSC* has four controls addressing *User Registration*, *Privilege Management*, *User Password Management* and *Review of User Access Rights*.

### Control

A control defines the specific control statement to satisfy the control objective. Each control further provides implementation guidance to support the implementation of the control in meeting the control objective. Some organizations may decide to implement a control using ways other than provided due to suitability to their specific environment.

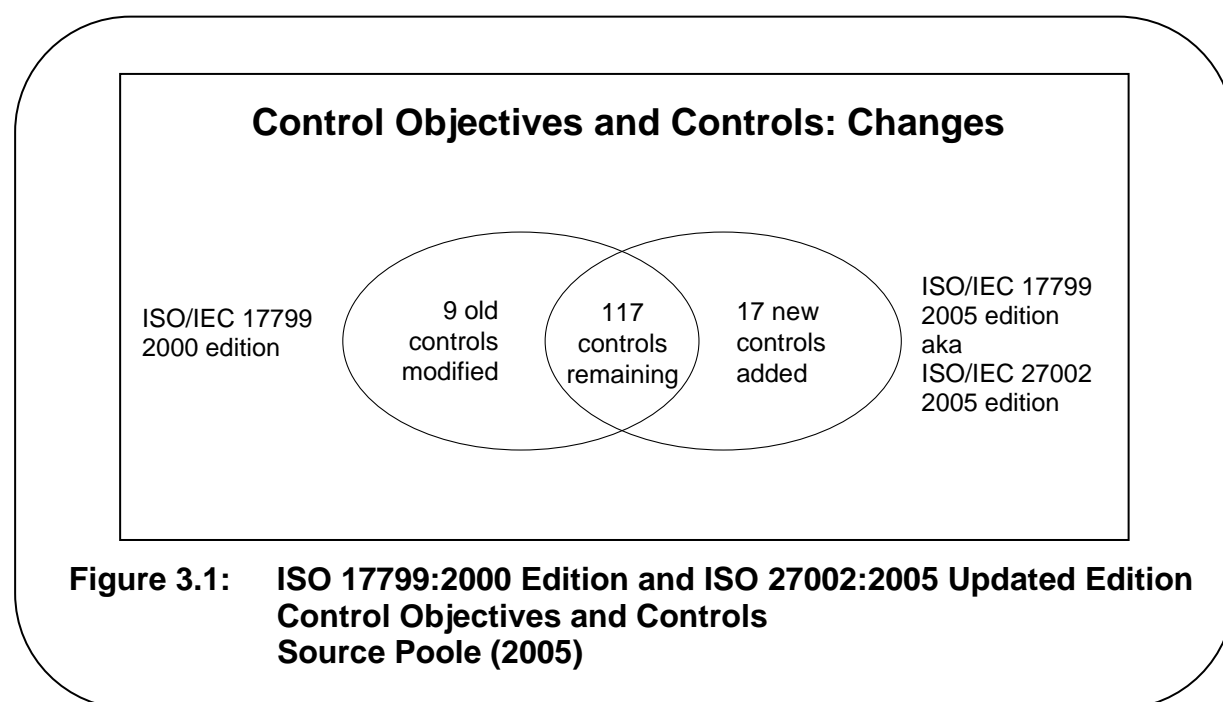
### 3.2.3 The Difference between ISO 17799:2000 and ISO 27002:2005

Much of the difference between ISO 17799:2000 and ISO 27002:2005 is renaming and category reshuffling. The new standard starts with the first security clause as *5.0 Information Security Policy*, with its sub-clauses as 5.1, 5.2 etc. The previous 2000 standard began with *Information Security Policy* as section 3.0. This creates a numbering difference that cascades into the various topics of the standard. There are a number of naming changes as illustrated in Table 3.1.

ISO 17799:2000 Edition (10 Clauses)	ISO 27002:2005 Edition (11 Clauses)
Security Policy	Security Policy
Security Organization	Organizing Information Security
Asset Classification & Control	Asset Management
Personnel Security	Human Resources Security
Physical & Environmental Security	Physical & Environmental Security
Communications & Operations Management	Communications & Operations Management
Access Control	Access Control
Systems Development & Maintenance	Information Systems Acquisition, Development and Maintenance
	Information Security Incident Management
Business Continuity Management	Business Continuity Management
Compliance	Compliance

**Table 3.1: ISO 17799:2000 Edition vs ISO 27002:2005 Updated Edition Security Clauses**  
Source Poole (2005)

The ISO/IEC 27002:2005 consists of eleven security clauses that specify 39 control objectives to protect information assets and provides 133 best practice controls that can be adopted based on a risk assessment process. It leaves an organization free to select controls not listed in the standard which gives great flexibility to its implementation (Lineman, 2008). The differences between the ISO 17799:2000 and ISO 27002:2005 at the level of controls and control objectives are summarized and illustrated in Figure 3.1.



### 3.2.4 The Content of the ISO/IEC 27002

ISO 27002 is comprised by a foreword (not numbered) and a further sixteen sections numbered 0 – 15. Sections 0 to 4 address introductory and informative aspects such as an introduction to information security, the scope of the standard, important terms and definitions, the structure of the standard and a brief coverage of risk assessment and treatment. The bulk of the standard is set out in Sections 5 – 15 which cover the security clauses, sub-clauses, control objectives and controls. The last part of the standard comprises a bibliography and an index.

### 3.2.5 The Eleven Security Clauses of the ISO/IEC 27002

The security clauses of the ISO/IEC 27002 are briefly discussed to provide insight into the main areas addressed by the standard. The discussion is sourced primarily from Edmead (2006), except where indicated otherwise.

#### i. Security policy

The *Security Policy* clause demonstrates management commitment to security and provides high-level rules for protecting assets (Yhan, n.d.). The clause states that it aims to achieve management direction and support for information security in line with business requirements and legal obligations (ISO 27002, 2005).

#### ii. Organization of information security

This clause addresses the establishment and organizational structure of the security program which includes an appropriate management framework for information security. It provides guidelines on addressing security when dealing with external parties.

#### iii. Asset management

This clause further assists the organization to be in a position of understanding what information assets it holds, and to manage their security appropriately.

#### iv. Human resources security

The *Human Resources Security* clause describes best practices for personnel management and includes hiring practices, termination procedures, employee training on security controls, dissemination of security policies, and use of incident response procedures.

#### v. Physical and environmental security

This clause addresses the different physical and environmental aspects of security and includes the best practices an organization can use to mitigate service interruptions, prevent unauthorized physical access, or minimize the theft of corporate resources.

**vi. Communications and operations management**

This clause discusses the requirements pertaining to the management and operation of systems, networks and electronic information. Examples of the controls include change management, third party service delivery, system planning and acceptance, capacity management, backups, network controls and e-commerce services.

**vii. Access control**

This security clause describes how access to corporate assets should be managed and includes access to digital and non-digital information and network resources.

**viii. Information systems acquisition, development and maintenance**

This clause discusses the development of IT systems and includes applications created by third-parties, and how security should be incorporated during the development phase.

**ix. Information security incident management**

This clause identifies the best practices for communicating information security events and weaknesses, such as reporting and escalation procedures. The clause further requires that organizations learn from information security incidents and implement measures towards improvement.

**x. Business continuity management**

The controls of the *Business Continuity Management* clause are designed to minimize the impact of security incidents that happen despite the preventive controls that are implemented (ISO 27001 Security, n.d.). It covers the development, implementation, testing, maintenance and re-assessment of business continuity plans.

**xi. Compliance**

The final clause provides valuable information for auditors to use when identifying the compliance level of systems and controls with internal security policies, industry-specific regulations, and government legislation. It covers compliance with legal requirements, security policies, standards and technical compliance as well as audit considerations.

The ISO 27002 advises that not all the controls contained in the security clauses are applicable and that organizations should implement applicable clauses according to their needs, which must be identified through a proper risk assessment (ISO 27002, 2005).

Organizations that implement an ISMS in accordance with the best practice advice in the ISO 27002 are likely to simultaneously meet the requirements of ISO 27001, but proved conformance (i.e. certification) with ISO 27001, is entirely optional. An outline of the ISO 27001 follows.

### **3.3 ISO 27001: 2005 - *Information Technology Security Techniques: Information Security Management Systems Requirements***

In October 2005, the ISO 27001 replaced the ISO 17799-2, which was based on the BS 7799-2, as the specification for an ISMS. BS7799-2 was first published by the British Standards Institution in 1999. BS7799-2 explains how to apply and implement the ISO 17799 (aka ISO 27002) and, critically, how to implement and maintain an ISMS (ISO 17799 FAQ, n.d.).

The ISO 27001 was developed by a variety of diverse organizations who had the common interest of protecting their information assets which they view as the 'life-blood' of all business (Humphreys, 2006). They developed the Information Security Management System (ISMS) standard to enable them to achieve cost effective information security solutions to protect their businesses (Humphreys, 2006). ISMSs must, as with all management processes, remain effective and efficient in the long term, by adapting to changes in the internal organization and external environment (Wikipedia<sup>b</sup>, 2008).

An ISMS is a system for establishing, operating and continuously ensuring the appropriateness of the installed safeguards against the identified security threats (Broderick, 2006). The ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS (ISO27001, 2005). The ISO 27001 (2005) states that the design and implementation of the ISMS

are influenced by an organization's needs and objectives, security requirements, the processes employed and its size and structure.

It cannot be overstressed that an ISMS does not merely comprise technology and documentation. While both technology and documents are necessary, Commerce Report No. 07006 states that the crucial elements of an ISMS are its managed planning and operation of processes which must be in accordance with documented procedures and properly recorded decisions and actions (NSW Department of Commerce, 2007).

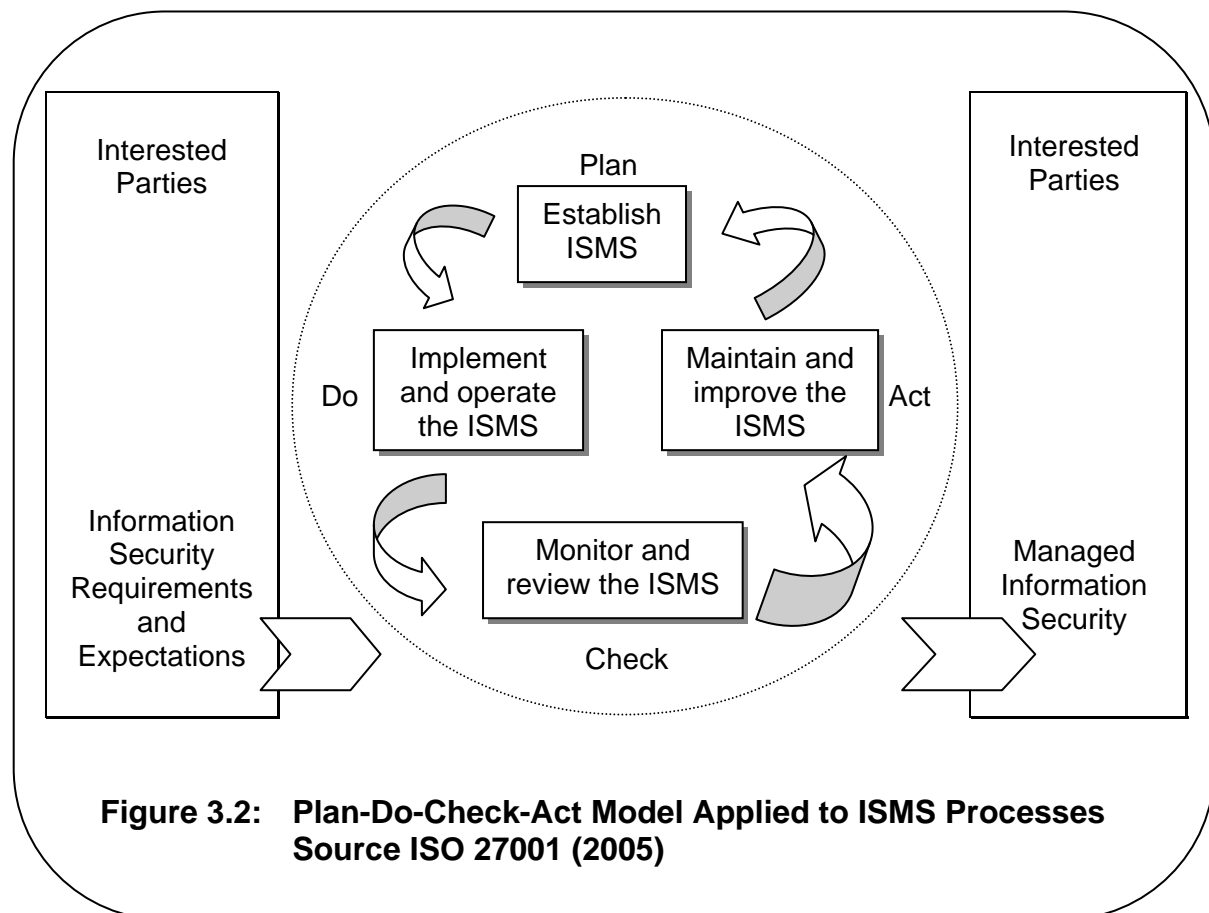
An ISMS uses a cyclic model that aims to ensure that the best practices of an organization are documented, reinforced and improved over time (Eloff, & Eloff, 2005). However, an ISMS will not be effective unless there is proper training and awareness of all the stakeholders involved. The NSW Department of Commerce (2007) emphasizes that an ISMS depends on people together with appropriate training and awareness.

The ISO 27001 standard adopts the Plan-Do-Check-Act (PDCA) process cycle model which is applied to structure all the ISMS processes and requirements for continual improvement (ISO 27001:2005). Figure 3.2 illustrates the PDCA model as applied to ISMS processes.

The PDCA model is used to implement a virtuous circle of continual improvement within the ISMS. It reflects the constant evolution of an ISMS to meet ever-changing threats, vulnerabilities and business needs (Humphreys, 2006). The activities of the PDCA cycle in an ISMS are summarized as follows:

- The **Plan** phase deals with designing the ISMS, assessing the information security risks and selecting the appropriate controls;
- The **Do** phase involves the implementation and operation of the selected controls;

- The **Check** phase reviews and evaluates the performance, the efficiency and effectiveness, of the ISMS; and
- The **Act** phase comprises making the necessary changes to bring the ISMS back to peak performance.



The ISO 27001 is a companion guide to the ISO 27002, explaining how to apply and implement the ISO 27002 standard and the ISMS which is required to ensure a continuous cycle of activities. The ISO 27001 and ISO 27002 standards are more generic and therefore guidance is required as to their application in the health domain. This motivated the consideration and publication of the ISO 27799 which is subsequently discussed.



### 3.4 ISO 27799: 2008 - *Health Informatics: Information Security Management in Health using ISO/IEC 27002*

#### 3.4.1 Introduction

The ISO 27799: 2008 was published in June 2008. It was developed by ISO technical committee TC215 responsible for health informatics, rather than JTC1/SC27, the joint ISO and IEC committee responsible for ISO27k. The Report on ISO TC215 Health Informatics standards development meetings in Montreal (Rowlands, 2007) indicates that it was resolved that ISO/TC215 should approve the Working Group 4 (WG4) recommendation that ISO 27799 “*Health Informatics – Security Management in Health using ISO/IEC 17799*” be renamed to ISO 27799 “*Health Informatics – Information Security Management in Health using ISO/IEC 17799*”. This was subsequently changed to “... *using ISO/IEC 27002*” to be in line with the 27000 et seq. numbering scheme used for information security management standards.

The ISO 27799 addresses the area of personal health information and how to protect its confidentiality and integrity while ensuring its availability for healthcare delivery (International Organization for Standardization [ISO], 2008). The standard specifies a set of controls for managing health information security and provides best practice guidelines. The implementation of this standard, according to ISO, will enable healthcare organizations and other custodians of health information to ensure a minimum requisite level of security that is appropriate to their size and circumstances (ISO 27799, 2008).

It is envisaged that adoption of ISO 27999 will assist interoperation, and better enable the adoption of new collaborative technologies in healthcare delivery (The ISO 27000 Directory, n.d.). This occurred because healthcare professionals contributed their expertise during the definition of the guidelines to specifically support the interpretation and implementation of ISO 27002 in health informatics (ISO, 2008). The International Organization for Standardization states that an important consideration was the adaptability of the guidelines, bearing in mind that many health professionals work as solo health providers or in small clinics that lack

IT resources to manage information security (as cited in Poremba, 2008). This international standard, therefore, provides additional guidance in a format that persons responsible for health information can readily understand and adopt. It contains a practical action plan for implementing ISO 27002 in the health environment.

### **3.4.2 The Content of the ISO 27799**

Although based on the ISO 27002, the structure of the ISO 27799 differs. It commences with a foreword and introduction (not numbered) and has a further seven sections numbered 1 – 7. Similar to the ISO 27002, the Introduction and Sections 1 to 6 address introductory and informative aspects such as an introduction to health information security, the scope of the standard, normative references, health and information security terms and definitions and an extensive discussion of a practical action plan to implement ISO 27002. The bulk of the standard is set out in Section 7 which covers the security clauses, sub-clauses, control objectives and controls of the standard. The last part of the standard comprises three Annexes and a bibliography.

It is important to note that ISO 27799 incorporates aspects of the ISO 27001 in its Section 6, which discusses an action plan to implement the ISO 27002.

An in-depth comparison of the ISO 27799 and the ISO 27002 standards is reported on in Chapter 4 and therefore the content of the ISO 27799 is not discussed further at this stage.

## **3.5 Conclusion**

The purpose of this chapter was to provide an overview of the concepts of information security, risk management and information security management and thereafter, to investigate the ISM-related standards that were identified in Chapter 1 as relevant to this research. The purpose and development of the ISO 27002 and ISO 27799 standards were discussed and an overview provided of their structure

and content. The development and approach of the ISO 27001 standard as a directive to establish an ISMS, were discussed.

Chapter 3 concludes Section 1 of this dissertation as explicated in Chapter 1 (Figure 1.1). The next section of the dissertation, comprised by Chapter 4, reports on a comparative analysis of the ISO 27002 and ISO 27799 standards from a healthcare point of view.

# Chapter 4

## 4. A Comparative Analysis of the ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards

The aim of **Chapter 4** relates directly to the main objective of this research, namely to assess whether the ISO 27799 serves the information security management needs of the health sector. This is done through conducting a comparative analysis of the generic ISO 27002 ISM standard and the healthcare specific ISO 27799 ISM standard.

Section 4.1 commences by providing background information about the standards. A high level comparison of the standards that demonstrates the overall structure of the standards is discussed and illustrated diagrammatically in Section 4.2. The results of the high-level comparison are used as a point of departure for the detailed comparison reported on in Sections 4.3 – 4.5.

The detailed comparison is divided into three parts namely Parts I, II and III. Part I is addressed in Section 4.3 and investigates the introductory and informative sections of the standards. Part II is addressed in Section 4.4 and provides a detailed analysis of the security control clauses of the standards. New and amended security categories and controls that have been included in the ISO 27799 are identified. Part III is addressed in Section 4.5 and reports on the differences between the attachments or appendices included in the two standards. Section 4.6 uses the aforementioned three sections as input to compile a final critique of the contribution of the ISO 27799 to the ISM needs of the health sector.

## 4.1 Background

As established in Chapter 3 and confirmed by Arnason & Willett (2007), the ISO 27001 represents a management system for information security, whereas ISO 27002 presents guidelines for security controls which are generic to all companies who have considered implementing information security management for their activities. Fraser (2007) indicates that the ISO 27002 is an internationally recognized generic information security standard which is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry. The ISO 27799 is described as a complement to the generic ISO 27001 and ISO 27002 standards and provides guidelines in dealing with the security of personal health information (ISO 27799, 2008).

This Chapter intends to determine what value the ISO 27799 standard adds over and above the ISO 27002 standard, to satisfying the information security management needs of the health sector. In order to achieve this, the ISO 27002 and ISO 27799 standards are compared. The comparison commences with a simple explication of the structural differences between the standards in Section 4.2.

## 4.2 High level comparison of ISO 27002 and ISO 27799

As a point of departure, this study investigated the ISO 27002 and ISO 27799 standards from the perspective of understanding, at a high level, how the sections contained in the standards map to each other. The result of this investigation is illustrated diagrammatically in Figure 4.1. The figure is repeated in Appendix A2 in a fold-out format to enable the reader to view the structural composition of the standards while reading the rest of Chapter 4.

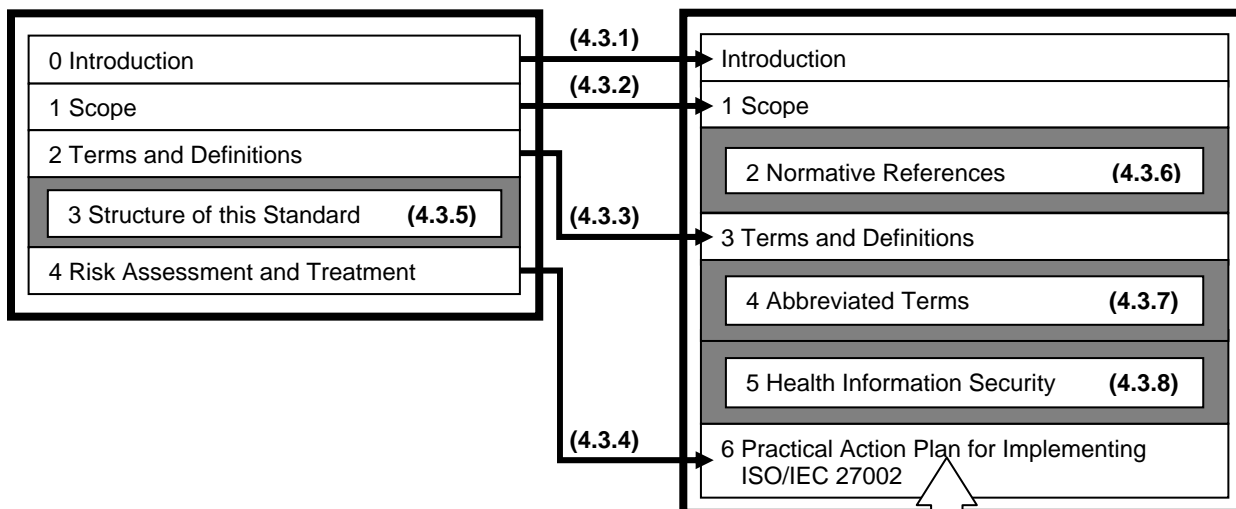
The layout of and legend used in Figure 4.1 are as follows:

- The ISO 27002 standard and the sections it contains, are depicted on the left of Figure 4.1. Each section heading of the standard is represented by a rectangle which shows the section number allocated in the standard as well as the name of the section.

ISO 27002

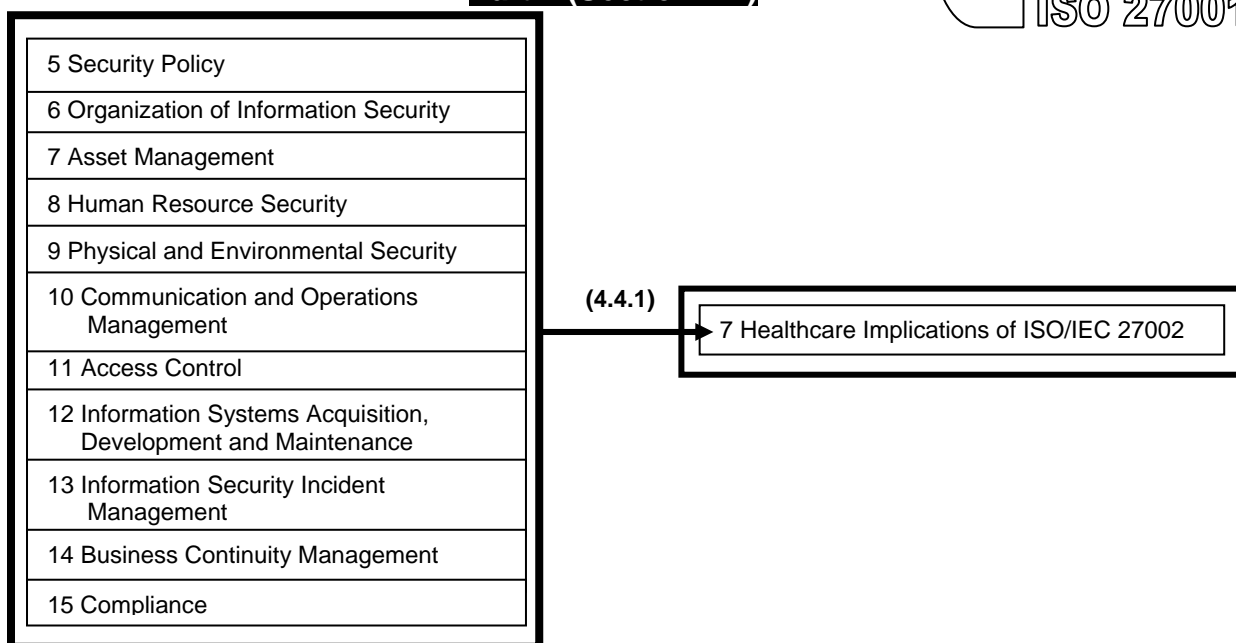
Part I (Section 4.3)

ISO 27799



Part II (Section 4.4)

ISO 27001



Part III (Section 4.5)

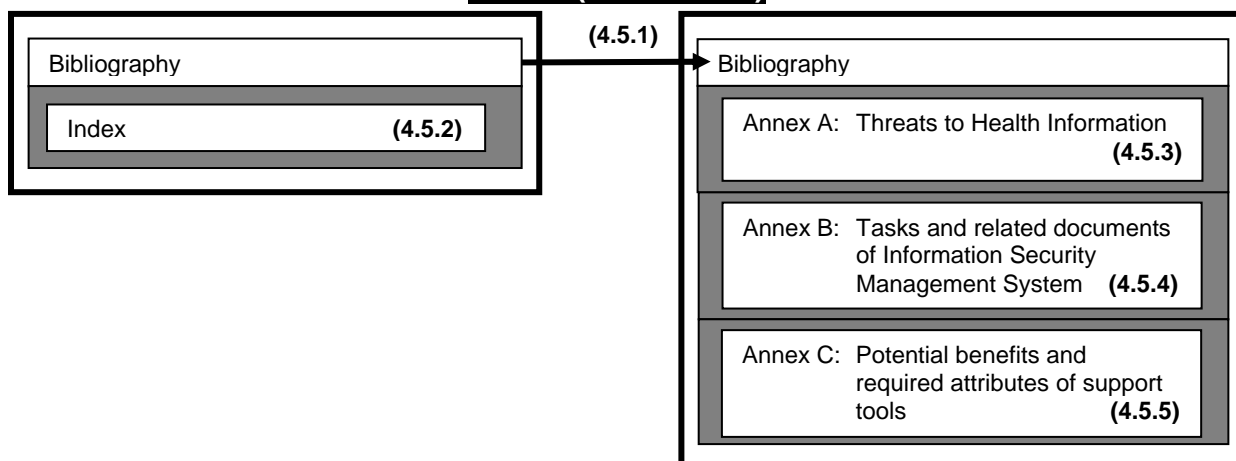


Figure 4.1 High Level Comparison of the ISO 27002 and ISO 27799 Standards

- Similarly the ISO 27799 standard and its sections are depicted on the right of Figure 4.1 using rectangles to represent the section numbers and headings used in the standard.
- Sections contained in the ISO 27002 standard that are included in the ISO 27799 standard for a similar purpose, are shown with an arrow pointing towards the section contained in the ISO 27799 standard. These arrows represent the mapping between the sections in the standards and each mapping is shown with a number in brackets (above the arrow) which corresponds with the section in this dissertation, where the particular mapping is discussed.
- There are a number of sections which, based on content covered, can be classified as “unique sections”; i.e. these sections are covered primarily in one of the standards and not the other. These unique sections are highlighted with shaded rectangles in Figure 4.1. Each unique section shows a number in brackets next to the name of the section, which corresponds with the section in this dissertation where it is discussed.

Figure 4.1 demonstrates the following:

- The initial sections of both standards (ISO 27002 Sections 0 – 4 and ISO 27799 Introduction and Sections 1 – 5) tend to address preparatory aspects and set the context, scope and structure of the standards respectively.
- Section 4 of the ISO 27002 maps to Section 6 of the ISO 27799, but the ISO 27799 includes aspects from the ISO 27001 (Information Security Management Systems Requirements) standard in its Section 6.
- Sections 5 – 15 of the ISO 27002 standard map to Section 7 of the ISO 27799 standard. These sections discuss the security control clauses of the standards.
- Both standards contain appendices or attachments.

Based on these preliminary findings, it was decided to approach and structure further comparison and discussion of findings in three main parts, depicted as Parts I, II and III respectively in Figure 4.1. Figure 4.1 additionally shows that Part I is discussed in Section 4.3, Part II in Section 4.4 and Part III in Section 4.5 of this dissertation.

### 4.3 Part I: ISO 27002 (Sections 0 – 4) versus ISO 27799 (Introduction and Sections 1 – 6)

Figure 4.1 (Part I) illustrates that the informative sections of the ISO 27002 and ISO 27799 standards contain 3 sections each that address similar aspects (i.e. *Introduction*, *Scope* and *Terms and Definitions*). This does not imply that the content of the sections is the same, only that the sections are included in the standards for the same purpose, for example, to introduce the scope of each standard or to define the terms and definitions applicable in the relevant standard. Section 3 of the ISO 27002 and Sections 2, 4 and 5 of the ISO 27799 are unique sections in the respective standards.

In order to facilitate the comparison, the sections of the standards depicted in Part I of Figure 4.1, are now compared in table format (refer to Table 4.1). For ease of reference, the table lists and discusses the sections as follows:

- Column 1: Sections of the ISO 27002;
- Column 2: The mapping number shown in Figure 4.1 above the arrows that depict the mapping between the sections and in some cases, in brackets after the section headings; and
- Column 3: Sections of the ISO 27799.

ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
<p>Section 0: <u>Introduction</u></p> <p>Information security is defined in general and the important organisational issues of information security are introduced. The following are briefly discussed:</p> <ul style="list-style-type: none"> <li>• Definition of information security;</li> </ul>	<p>4.3.1</p>	<p><u>Introduction</u></p> <p>(Section not numbered)</p> <p>The standard is introduced by:</p> <ul style="list-style-type: none"> <li>• Defining its relevance to and for healthcare specific activities;</li> <li>• Defining the need to have a standard which addresses aspects specific to the</li> </ul>



ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
<ul style="list-style-type: none"> <li>• Importance of information security in the organisation;</li> <li>• Methods of establishing security requirements;</li> <li>• Assessing security risks;</li> <li>• The selection of controls;</li> <li>• Critical success factors of implementing information security within an organisation.</li> </ul>		<p>healthcare sector;</p> <ul style="list-style-type: none"> <li>• Explaining its relationship with the ISO 27002 standard; and</li> <li>• Outlining the benefits of its use together with guidance on how it can be used.</li> </ul>
<p><u>Section 1: Scope</u> →</p> <p>This section defines the scope of the standard in terms of information security management practices.</p>	<p>4.3.2 →</p>	<p><u>Section 1: Scope</u></p> <p>The role of the standard in the healthcare sector is outlined. The fact that it is technology-neutral is emphasized. Its applicability to health information in all its aspects and forms is confirmed. It notes the relationship between itself and the ISO 27002 standard. The areas of information security which do not form part of ISO 27799 are identified and listed, e.g. network quality of service and data quality (as distinct from data integrity).</p>
<p><u>Section 2: Terms and Definitions</u> →</p> <p>General information security management terminology is defined.</p>	<p>4.3.3 →</p>	<p><u>Section 3: Terms and Definitions</u></p> <p>Healthcare specific terms and some generic information security management terminology are defined.</p>

ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
<p data-bbox="188 353 603 427"><u>Section 4: Risk Assessment and Treatment</u></p> <p data-bbox="188 521 699 831">The assessment of security risks and possible treatment options are briefly discussed. These topics comprise one and a half pages of the standard and are not discussed extensively.</p>	<p data-bbox="762 353 836 387">4.3.4</p>	<p data-bbox="895 353 1342 501"><u>Section 6: Treatment/Practical Action Plan for Implementing ISO/IEC 27002</u></p> <p data-bbox="895 521 1406 1384">This section provides a brief taxonomy of the ISO 27001 and ISO 27002 standards. It is explained that compliance with the ISO 27002 is not a simple matter and requires an operational ISMS in which there are appropriate compliance auditing processes. The section defines the importance of introducing an ISMS where there is a requirement for formal accreditation or certification. It is stated that healthcare organizations need evident support from management when attempting compliance.</p> <p data-bbox="895 1458 1398 1711">The rest of the section provides detailed discussion of establishing, operating, maintaining and improving an ISMS in a healthcare environment.</p>
<p data-bbox="188 1758 571 1832"><u>Section 3: Structure of this Standard</u></p> <p data-bbox="188 1852 667 1944">This section is unique. It explains the structure of the standard in</p>	<p data-bbox="762 1758 836 1792">4.3.5</p>	

ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
terms of the number of clauses and main security categories it contains. It further explains that the composition of main security categories comprises of a control objective and one or more controls.		
	<b>4.3.6</b>	<u>Section 2: Normative References</u> This section is unique. It lists the ISO 27002: 2005 as a normative reference in the use of the ISO 27799.
	<b>4.3.7</b>	<u>Section 4: Abbreviated Terms</u> Section 4 is unique. It provides a list of acronyms used in the ISO 27799. It is a brief list containing <i>five</i> terms only.
	<b>4.3.8</b>	<u>Section 5: Health Information Security</u> Section 5 is unique. A concerted effort is made to contextualize health information security. The main topics of interest in this section include: <ul style="list-style-type: none"> <li>• Health information security goals;</li> <li>• Information security within information governance;</li> <li>• Information governance within</li> </ul>

ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
		corporate and clinical governance; <ul style="list-style-type: none"> <li>• Health information to be protected; and</li> <li>• Threats and vulnerabilities in health information security.</li> </ul>

**Table 4.1: ISO 27002 (Sections 0 – 4) versus ISO 27799 (Introduction and Sections 1 – 6)**

#### 4.3.1 Part I: Findings of the Comparison

The comparative analysis of ISO 27002 Sections 0 – 4 versus ISO 27799 Introduction and Sections 1 – 6 demonstrated the following:

- a. The *Introduction*, *Scope* and *Terms and Definitions* sections of both standards address aspects that are required to contextualize the standards, i.e. for the ISO 27002 these sections contextualize the standard in terms of information security and information security management, while for the ISO 27799 these sections contextualize the standard in terms of the ISO 27002, health information security and health information security management.
- b. The content of the unique sections contained in the ISO 27799 (i.e. Sections 2, 4 and 5) satisfy a basic objective, namely to provide sufficient information about issues of relevance (and examples) in the healthcare context. This contributes to the nature of the ISO 27799 as an industry-specific version of the ISO 27002.
- c. While Section 3 of the ISO27002 is a unique section which is not covered in the ISO 27799, the information it contains is of direct relevance to the ISO 27799. It therefore makes sense that it is not repeated in the ISO 27799 as the standard

has been compiled using the same structural entities (e.g. security clauses, main security categories, control objectives, etc.).

- d. The ISO 27002 (2005) states that its control objectives and controls are intended to be implemented to meet requirements identified by a risk assessment. This explains the inclusion of Section 4 in the standard, which provides a brief overview of the topics of risk assessment and treatment. These topics are covered in Section 6 of the ISO 27799, hence the mapping between the sections as indicated in Figure 4.1. However, upon cursory inspection of the ISO 27001 as compared to Section 6 of the ISO 27799, it became clear that the purpose of this section was not to expound on the topics of risk assessment and risk treatment only. It was included to guide healthcare organizations in implementing the ISO 27002. The question therefore arose as to why healthcare organizations were not simply referred to the ISO 27001 for this purpose? Further inspection of Section 6 of the ISO 27799 revealed that the section does include information relating to the healthcare context, which is not covered in the ISO 27001. For example, the “*reactions of subjects of care*” is listed as a factor to be taken into account by health organizations when considering risk acceptance criteria. It is concluded therefore that Section 6 of the ISO 27799 addresses the implementation of the ISO 27002 and provides additional information in this regard, related to the healthcare context. Note that the scope of this research project precluded a detailed comparison of the ISO 27799 with the ISO 27001.

#### 4.4 Part II: ISO 27002 (Sections 5 - 15) versus ISO 27799 (Section 7)

The ISO 27799 (2008) states that all of the security control objectives described in ISO/IEC 27002 are relevant to health informatics, but some controls require additional explanation about their use in the protection of the security of health information. It is also made clear that the guidance given is in addition to, but not a replacement for, the guidance found in ISO/IEC 27002.

Figure 4.1 (Part II) shows that Sections 5 – 15 of the ISO 27002 maps to Section 7 of the ISO 27799. These sections of the standards, which comprise the bulk of the standards, are now compared. The comparison commences by looking at the

number of security clauses, main security categories and controls contained in each standard. Table 4.2 summarises the results of this comparison. Thereafter, the detailed comparison of the security control clauses (attached as Annexure A1) is discussed.

#### 4.4.1 Part II: Structural Comparison

Table 4.2 presents an overview of the differences and similarities in the structure of the security clauses in the standards. The layout of the table is explained as follows:

- The first three columns show the section numbers and names of the security clauses in each standard. In cases where the section names differ, the two names are listed below each other, with the alignment of the section number providing an indication of the relevant standard.
- The next three columns represent information relating to the ISO 27002 standard in terms of:
  - The section number of each Main Security Category (MSC) contained in a security clause;
  - The total number of MSCs (# MSC) contained in a security clause;
  - The total number of controls (# Ctrl) contained in each main security category.

For example, security clause 6 of the ISO 27002 is comprised by two MSCs numbered 6.1 and 6.2. These MSCs contain 8 and 3 controls respectively.

- The last three columns show the same information as relating to the ISO 27799 standard.
- Shaded blocks in the columns used for the ISO 27002, indicate that there is a security clause or a main security category that has been included in the ISO 27799, but not the ISO 27002. For example, MSC 7.12.1 of the ISO 27799 is not included in the ISO 27002.
- Shaded blocks in the columns used for the ISO 27799 mean that this standard does not provide additional guidance over and above the information contained in the ISO 27002 and that as a result; a section (MSC or Ctrl) number was not assigned. For example, MSC 14.1 of the ISO 27002 is adopted “as is” in the

ISO 27799 and therefore Sections 14.1 and 14.1.1 – 14.1.5 of the ISO 27002 do not have corresponding Section numbers in the ISO 27799.

ISO 27002	ISO 27799	Security Clause	ISO 27002			ISO 27799		
			MSC Nr	# MSC	# Ctrl	MSC Nr	# MSC	# Ctrl
	7.1	General				0	0	0
5	7.2	Security Policy <i>Information Security Policy</i>	5.1	1	2		0	2
6	7.3	Organization of Information Security <i>Organizing Information Security</i>				7.3.1	3	0
			6.1	2	8	7.3.2		4
			6.2		3	7.3.3		3
7	7.4	Asset Management	7.1	2	3	7.4.1	2	0
			7.2		2	7.4.2		2
8	7.5	Human Resources Security	8.1	3	3	7.5.1	3	3
			8.2		3	7.5.2		3
			8.3		3	7.5.3		2
9	7.6	Physical and Environmental Security	9.1	2	6	7.6.1	2	3
			9.2		7	7.6.2		5
10	7.7	Communications and Operations Management	10.1	10	4	7.7.1	10	4
			10.2		3	7.7.2		0
			10.3		2	7.7.3		2
			10.4		2	7.7.4		2
			10.5		1	7.7.5		0
			10.6		2	7.7.6		2
			10.7		4	7.7.7		4
			10.8		5	7.7.8		4
			10.9		3	7.7.9		2
			10.10		6	7.7.10		7

ISO 27002	ISO 27799	Security Clause	ISO 27002			ISO 27799			
			MSC Nr	# MSC	# Ctrl	MSC Nr	# MSC	# Ctrl	
11	7.8	Access Control	11.1	7	1	7.8.1	6	2	
			11.2		4			7.8.2	4
			11.3		3			7.8.3	0
			11.4		7			7.8.4	0
			11.5		6				
			11.6		2			7.8.5	2
			11.7		2			7.8.6	2
12	7.9	Information Systems Acquisition, Development and Maintenance	12.1	6	1	7.9.1	5	0	
			12.2		4			7.9.2	5
			12.3		2			7.9.3	2
			12.4		3			7.9.4	3
			12.5		5			7.9.5	0
			12.6		1				
13	7.10	Information Security Incident Management	13.1	2	2	7.10.1	2	0	
			13.2		3			7.10.2	3
14	7.11	Business Continuity Management <i>Information Security Aspects of Business Continuity Management</i>	14.1	1	5		0	0	
15	7.12	Compliance		3	0	7.12.1	4	0	
			15.1		6			7.12.2	3
			15.2		2			7.12.3	0
			15.3		2			7.12.4	0

Table 4.2 ISO 27002 (Sections 5 - 15) versus ISO 27799 (Section 7)



#### 4.4.2 Part II: Findings of the Structural Comparison

The following should be noted. Table 4.2 takes shaded blocks (in the columns used for the ISO 27799) to mean that additional guidance over and above the information contained in the ISO 27002 is not provided. Generally this leads to a section number not being assigned to the particular MSC or control. However, the standard has an inconsistent approach in this regard as it does sometimes allocate section numbers and names to MSCs and controls that do not provide guidance in addition to the ISO 27002. Refer to Appendix A1, Sections 13.2.1 (ISO 27002) and 7.10.2.1 (ISO 27799) for an example.

From the information provided in Table 4.2, the following can be deduced:

- a. Most of the ISO 27002 and ISO 27799 clauses share the same clause names but three clause names are slightly different.
- b. The ISO 27799 contains a new security clause (7.1) and two new MSCs (7.3.1 and 7.12.1) that are not included in the ISO 27002.
- c. The ISO 27799 contains three new controls (in MSCs 7.7.10, 7.8.1 and 7.9.2). This can be deduced from the fact that the number of controls (# Ctrl) is one more for the ISO 27799 than for the ISO 27002 for each of afore-mentioned MSCs.
- d. The total number of clauses, main security categories and controls contained in the standards can be summarized as follows:

	<b>ISO 27002</b>	<b>ISO 27799</b>
Number of Security clause	11	12
Number of MSCs	39	41
Number of Controls	133	136

**Table 4.3 ISO 27002 versus ISO 27799  
(Total Number of Clauses, MSCs and Controls)**

It should be noted that the totals computed for the ISO 27799 are based on the totals for the ISO 27002 plus the number of new clauses, MSCs and controls.

This is based on the ISO 27799's directive that it provides guidance in addition to and not as a replacement for the guidance found in ISO 27002 (ISO 27799, 2008). The total number of MSCs and controls of the ISO 27799 is debatable since the ISO 27799 does not include the 39 MSCs and 133 controls of the ISO 27002 in its structure as evident from Table 4.2 and mentioned in the discussion thereafter. This is confirmed in the detailed comparison conducted hereafter (refer to Section 4.4.4 points (e) and (f)).

#### 4.4.3 Part II: Detailed Comparison

The detailed comparison of the security clauses, main security categories and controls of the ISO 27002 and ISO 27799 standards has been summarized and attached as Appendix A1 to this dissertation. The layout of the table in Appendix A1 is explained as follows:

- The column headings of Appendix A comprises of the following heading names: ISO 27002, ISO 27799, FLAG and ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799.
- The first and second columns list the clauses, main security categories and controls contained in the respective standards.
- The FLAG column classifies the clauses, main security categories and controls by indicating whether the detail provided in the ISO 27799 is NEW or greater than (>) or equal (=) to what is provided in the ISO 27002.
- A FLAG which is classified as NEW indicates whether it is a new clause, main security category or control that is contained in the ISO 27799.
- A FLAG which is classified as greater than (>) indicates that the ISO 27799 provides additional directives (optional or compulsory) in the form of expanding on the control statements or the implementation guidance provided in the ISO 27002.
- A FLAG which is classified as equal (=) indicates that the ISO 27799 provides no additional guidance and that the content provided in the ISO 27002 must be implemented "as is".
- The last column in Appendix A1 summarises the additional requirements and/or

implementation guidance provided in the ISO 27799. Occasionally, the word SHALL is included in this column in white text and highlighted in black (right-aligned). This shows control statements or implementation guidance aspects, the application of which is mandatory in healthcare.

- Shading is used as follows in Appendix A1:
  - In the first column, a rectangle with grid shading indicates that the particular clause and/or main security category and/or control contained in the ISO 27799, is not included in the ISO 27002.
  - In the second column, a rectangle with grid shading indicates that the particular clause and/or main security category and/or control contained in the ISO 27002, is not included in the ISO 27799.
  - Rectangles with plain grey shading used in the last column, corresponds with the FLAG column where the value of the flag shows equal. This means that the ISO 27799 does not provide additional guidance or does not have additional requirements.
  - A rectangle with black shading is used to facilitate reading of the Appendix and simply highlights the start of a security clause or main security category.

#### 4.4.4 Part II: Findings of the Detailed Comparison

The comparative analysis of ISO 27002 Section 5 – 15 versus ISO 27799 Section 7 contained in Appendix A1, demonstrates that four types of changes have been made to the ISO 27799. These are discussed in (a) – (d) below. Other comments about the detailed comparison are discussed in (e) and (f).

##### a. Addition of new clauses, main security categories and controls in the ISO 27799

- New clauses
  - Clause 7.1: “General”

This clause contains specific advice about the clauses and security categories described in ISO 27002. It basically motivates the need for the ISO 27799 and explicitly states that the guidance given in the ISO 27799 is in addition to, but not a replacement for that found in the ISO 27002.

- New Main Security Categories

- Main Security Category 7.3.1: “General”

This main security category stresses the need for an explicit and robust information security management infrastructure, especially where organizations rely upon managed services provided by third parties. This category is critical for the healthcare sector because the effectiveness of their practice is based on the support provided by various third parties.

- Main Security Category 7.12.1: “General”

The main focus of this category is on a compliance auditing programme that addresses the full cycle of operations which must be put in place. The auditing programme must not only identify problem areas but also review outcomes and updates to the ISMS. For health organisations a 12 month to 18 month cycle of audit programmes is suggested. It is recommended for the Information Security Management Framework (ISMF) to establish a graduated compliance auditing framework with self-audit by the process operators and managers at the bottom layer and audits at subsequent layers drawing confidence from layers below it.

- New Controls

- Control 7.7.10.1: “General”

This control emphasizes the importance of security requirements relating to audit and logging. It highlights the importance of ensuring accountability and states that audit and logging can help organizations and subjects of care to obtain redress against users abusing their access privileges.

- Control 7.8.1.1: “General”

This control focuses on access to personal health information. It emphasizes that users of health information systems should only access personal health information if there is a relationship between the user and the subject of care (data subject), when the user is carrying out an activity on behalf of the data subject and when there is a need for data to support this activity.

- Control 7.9.2.1: “ Uniquely Identifying Subjects of Care”

This control indicates that it is compulsory that health information systems

ensure that subjects of care can be uniquely identified in the system and also be capable of merging duplicated or multiplied records if such records were created intentionally or during a medical emergency.

#### **b. Modified control statements**

Some control statements in the ISO 27799 are expanded to address issues of importance in health information security. Generally these control statements list more stringent requirements or more specific requirements than the ISO 27002. An example of a modified control statement is found in the *Information Security Policy (7.2)* clause of the ISO 27799, control 7.2.2 *Review of the information security policy document*. The control statement requires staged reviews such that the totality of the policy is addressed at least annually. It further requires the policy to be reviewed after the occurrence of a serious security incident. These requirements are not included as part of the control statement in the ISO 27002, which requires that the policy be reviewed at planned intervals or if significant changes occur.

#### **c. Additional implementation guidance**

Some of the controls in the ISO 27799 are provided with additional implementation guidance to support the implementation of the control in the healthcare environment. An example of additional implementation guidance is found in the *Organizing Information Security (7.3)* clause of the ISO 27799, MSC 7.3.3 *Third parties*, control 7.3.3.1 *Identification of risks related to external parties*. The implementation guidance stresses the importance of protecting the rights of subjects of care where external parties are involved. It is mentioned that the jurisdiction governing the subject of care shall apply even if the external party is governed by a different jurisdiction.

#### **d. Inclusion of normative control statements**

The ISO 27799 contains 25 normative control statements and 2 normative statements related to implementation guidance, which make the application of the relevant security control / implementation guidance aspect, mandatory. This is

indicated using “shall” in the control / implementation statement instead of “should”. The reason for this is explained in the introduction of the standard namely that the application of certain ISO 27002 control objectives is essential if personal health information is to be adequately protected (ISO 27799, 2008).

- e. Section 4.4.2, Part II: Findings of the Structural Comparison, mentioned that some of the MSCs and controls in the ISO 27002 have not been assigned a section number in the ISO 27799. This is illustrated in the detailed comparison contained in Appendix A1, for example, MSC 14.1 and controls 14.1.1 – 14.1.5 have not been assigned section numbers in the ISO 27799. This confirms that the ISO 27799 cannot be used in isolation as it will lead to an incomplete implementation of the ISO 27002.
- f. The detailed comparison further shows that some MSCs in the ISO 27002 have been consolidated. For example, MSCs 11.4 *Network Access Control* and 11.5 *Operating System Access Control* have been consolidated in the ISO 27799 as MSC 7.8.4 *Network Access Control and Operating System Access Control*. Similarly some controls are consolidated in the ISO 27799. For example, controls 6.1.1 – 6.1.8 (eight controls) in the ISO 27002 have been consolidated as controls 7.3.2.1 – 7.3.2.4 (four controls) in the ISO 27799.

#### 4.5 Part III: Comparison of Appendices Included in the Standards

Part III of the comparison addresses the appendices (including bibliography, index and annexes) of the standards. In order to facilitate the comparison, it is presented in table format (refer to Table 4.4). As in Table 4.1, the table lists and discusses the sections as follows:

- Column 1: Sections of the ISO 27002;
- Column 2: The mapping number shown in Figure 4.1 above the arrows that depict the mapping between the sections and in some cases, in brackets after the section headings; and
- Column 3: Sections of the ISO 27799.

ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
<p><u>Bibliography</u> →</p> <p>Lists related standards in information security.</p>	4.5.1 →	<p><u>Bibliography</u></p> <p>Lists related standards in health information security.</p>
<p><u>Index</u></p> <p>This section cross-references an alphabetical list of terms against the clauses, MSCs and controls of the ISO 27002 using the allocated section numbers. E.g. the term “authentication” is cross-referenced as follows:</p> <p><i>authentication</i></p> <ul style="list-style-type: none"> <li>of users 11.5.2</li> <li>of users for external connections 11.4.3</li> </ul>	4.5.2	
	4.5.3	<p><u>Annex A: Threats to Health Information Security</u></p> <p>Annex A contains an informative list of the types of threats that need to be considered by health organizations when they assess risks to the confidentiality, integrity and availability of health assets. The discussion is contextualized for the healthcare sector, for example, users degrading the availability of health information systems by using network bandwidth for personal use.</p>

ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
	4.5.4	<p data-bbox="898 353 1331 501"><u>Annex B:</u> <u>Tasks and Related Documents of the Information Security Management System</u></p> <p data-bbox="898 521 1398 1435">Annex B briefly describes tasks and related documents of operating an ISMS in a health environment. It supplements the ISMS process overview and discussion provided in Section 6 of the standard by giving informative examples of the steps typically involved in each phase of the ISMS life cycle, together with examples of the types of documents related to each phase. It relates documents to the various steps in establishing or enhancing an ISMS by providing a diagrammatic representation of the tasks and related documents for:</p> <ul data-bbox="898 1458 1398 1883" style="list-style-type: none"> <li>• B.1 - Establishing the ISMS (Plan);</li> <li>• B.2 - Implementing and operating the ISMS (Do);</li> <li>• B.3 - Monitoring and reviewing the ISMS (Check); and</li> <li>• B.4 - Maintaining and improving the ISMS (Act).</li> </ul>



ISO 27002 (2005)	Section Mapping number in Figure 4.1	ISO 27799 (2008)
	4.5.5	<p data-bbox="898 353 1276 499"><u>Annex C: Potential Benefits and Required Attributes of Support Tools</u></p> <p data-bbox="898 517 1406 992">Annex C discusses the advantages of support tools as an aid to implementing information security management. It discusses the potential benefits and required attributes of support tools. It further lists requirements for such tools to adequately support the ISO 27002 and risk analysis processes.</p>

**Table 4.4 ISO 27002 versus ISO 27799 (Appendices)**

#### 4.5.1 Part III: Findings of the Comparison of Appendices

The unique annexes included in the ISO 27799 (A, B and C) serve the purpose of further contextualizing the standard in terms of the health sector. The importance of the ISMS is emphasized through expanding the discussion already provided in Section 6 of the standard. The inclusion of an *Index* in the ISO 27799, as was provided for the ISO 27002, would be beneficial in terms of cross-referencing.

#### 4.6 Critique: Contribution of ISO 27799 to Security Needs of Health Sector

Based on the comparison of the ISO 27002 and the ISO 27799 reported on in Sections 4.3 – 4.5 of the dissertation, the following concluding remarks can be made:

- As mentioned previously, the ISO 27799 incorporates aspects from both the ISO 27002 (Information Security Management) and ISO 27001 (Information Security Management System) standards. The inclusion of the discussion of the

ISMS in Section 6 and Annex B of the standard emphasizes the perceived importance in healthcare, of implementing the standard together with a robust management system.

- As noted in the standard, a concerted effort has been made to focus on security requirements necessitated by the unique challenges of delivering electronic health information that supports the provision of care (ISO 27799, 2008). This is achieved by:
  - Contextualizing the *Introduction, Scope and Terms and Definitions* of the standard to the health sector;
  - Including three unique introductory sections (Sections 2, 4 and especially Section 5);
  - Providing new and modified security requirements and additional implementation guidance customized for the needs of health information in Section 7 (in terms of the security control clauses); and
  - Providing additional Annexes as discussed in Section 4.5.
- The following topics can be deduced as being of particular importance for information security management in the health sector by virtue of them being included as new clauses, MSCs or controls in the ISO 27799.

Type	Section Number	Name	Keywords
Clause	7.1	General	A directive that guidance given is in addition to the ISO 27002
MSC	7.3.1	General	Managed services provided by third parties
MSC	7.12.1	General	Compliance auditing
Control	7.7.10.1	General	Audit and logging
Control	7.8.1.1	General	Access control
Control	7.9.2.1	Uniquely Identifying Subjects of Care	Redundancy

**Table 4.5 Summary of new Clauses, MSCs and Controls in ISO 27799**

- The following aspects detract from the ISO 27799's utility as an implementation guide for the ISO 27002:
  - The clauses, main security categories and controls of the ISO 27799 are numbered differently than in the ISO 27002 for various reasons. Firstly, the structure of the standards differs in terms of the number of sections it contains prior to the security clauses. Secondly, the ISO 27002 addresses each security clause in its own section (i.e. Sections 5 – 15) whilst the ISO 27799 addresses all the security clauses in one section, Section 7. Thirdly, the ISO 27799 did not include all MSCs and controls explicitly if additional guidance was not required and some MSCs and controls were consolidated. This impacts on the structure and numbering of the various clauses, MSCs and controls and could be confusing when implementing the standard.
  - Some of the clauses, MSCs and controls have modified names in the ISO 27799. The changes are not major, but could be experienced as confusing. It could be asked why this was necessary as the perceived result is to cause confusion rather than add value to the standard as an implementation guide for the ISO 27002.
  - The lack of a summary which shows the mapping between the two standards can also detract from its ease of use.

Overall, it can be concluded that the ISO 27799 achieves the objective of addressing the unique security needs of the health sector in terms of information security management, but that aspects like numbering and name differences may cause confusion in its use as an implementation guide, especially by users who are not familiar with the ISO 27002.

#### **4.7 Conclusion**

Chapter 4 reported on an assessment of whether the ISO 27799 standard serves the information security management needs of the health sector. The assessment comprised a comparative analysis of the ISO 27002 and ISO 27799 standards, to determine the differences between the standards. The comparison was conducted at

two levels. Section 4.2 commenced with a high-level comparison which considered the structure of the two standards in terms of the sections contained in each standard and the perceived mapping between the sections of a similar nature. The results of the high-level comparison led to the structuring of further detail-level comparisons in three parts.

Part I (discussed in Section 4.3) compared the ISO 27002 (Sections 0 – 4) versus ISO 27799 (Introduction and Sections 1 – 6). Part II (discussed in Section 4.4) compared the security clauses of the ISO 27002 (Sections 5- 15) and ISO 27799 (Section 7). Part III (discussed in Section 4.5) compared the attachments or appendices included in the standards.

The results of the comparison were summarized in Section 4.6 which critiqued the contribution of the ISO 27799 to serving the security needs of the health sector.

In Chapter 5, a critical review of the dissertation is presented and proposals for further research in this area are considered.

---

# Chapter 5

---

## 5 Conclusion

The aim of Chapter 5 is to conclude the research presented in this dissertation by providing a critical review of the dissertation. The problem statement and objectives of the research are reiterated in order to show how they were met throughout the dissertation. Lastly, it considers the benefits and limitations of the research and suggests how the research can be extended in the future.

### 5.1 Background

In today's information age healthcare informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks (ISO, 2008). Information in its various forms is a necessity for healthcare work and security in this case is an obvious requirement (Wallin & Xu, 2008). It is crucial that the data stored in healthcare informatics systems be protected. Because of these critical requirements, all healthcare organizations must protect the health information entrusted to them appropriately and diligently.

In 2008, the ISO 27799 was introduced as the healthcare-specific standard for information security management. The standard applies ISO 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information (ISO 27799, 2008).

In this research the ISO 27002 and ISO 27799 information security management standards were analyzed and compared. Additionally the ISO 27001 standard

emerged as relevant to consider in the comparison although the title of the ISO 27799 refers to the ISO 27002 standard only.

The knowledge gained from the initial high-level investigation led to a better understanding of the differences between the ISO 27002 and the ISO 27799 standards. The detailed comparison was conducted in three main parts, viz.:

- Part I, which addressed the introductory sections of both standards.
- Part II, which compared the security control clauses. The content of these sections of the standards comprises the bulk of the standards, viz. pages 7 – 106 of the ISO 27002 and pages 20 – 56 of the ISO 27799, where the last page mentioned is the last page of each standard respectively, excluding attachments like appendices, bibliographies and the index provided in ISO 27002.
- Part III which considered the attachments to the standards.

The results of the comparative analyses were reported on according to the three parts mentioned above and summarized thereafter in a section which critiqued the ISO 27799's contribution to serving the health sector's needs from an information security management point of view.

This then addresses the primary objective of the research as laid out in Chapter 1, namely:

*“The main objective of this research is to determine whether the ISO 27799 standard serves the needs of the health sector from an information security management point of view”.*

## **5.2 Re-examining the Sub-Objectives of the Research**

In order to achieve the main objective of this research, a number of sub-objectives were identified and addressed. Each sub-objective is subsequently discussed.

**a. Investigate the health sector and the special needs of health information security.**

This sub-objective was introduced to ensure an understanding of the nature and activities of the healthcare sector and the challenges of protecting the confidentiality, integrity and availability of personal health information.

**b. Examine information security management practices in general as well as in the health sector.**

In order to address the security challenges of the healthcare sector, proper information security management practices must be applied. The purpose of this sub-objective was therefore to ensure comprehension of the concept of information security management and its application in the healthcare sector.

**c. Perform a high level comparison of the ISO 27002 and ISO 27799 standards.**

This sub-objective ensured that the high level structures of the two standards were investigated to identify how to proceed with further comparison of the standards.

**d. Execute and document the results of the detailed comparative analysis of the security control clauses in both standards.**

This sub-objective required a detailed comparative analysis of the security control clauses in both standards in order to determine the differences between the standards.

**e. Determine the approach of ISO 27799 in regard to the establishment of an information security management system.**

Proper information security management practices require the establishment, implementation, operation, monitoring, review, maintenance and continued improvement of an information security management system. The intention of this

sub-objective was to determine whether the ISO 27799 standard addresses this aspect.

**f. Critique the contribution of the ISO 27799 to serving the security needs of the health sector.**

This sub-objective required the results of the prior sub-objectives to determine the differences between the ISO 27002 and the ISO 27799. This allowed an appraisal of the contribution of the ISO 27799 to information security management in the healthcare context.

Meeting sub-objectives (a) – (f) ensured that the main objective of the research was met. Section 5.3 shows how the research questions of the research were addressed and the sub-objectives achieved on a per Chapter basis.

## **5.3 Chapter Overview**

### **5.3.1 Chapter 1 – Introduction**

Chapter 1 highlighted the need for security and privacy of patient information. This was done by providing examples of breach of patient privacy due to an assumed lack of security in a particular healthcare setting. The concept of personal health information was defined to understand the full range of health information that requires protection. The Chapter further introduced the ISM(S) standards of relevance to this research. This led to the formulation of the problem statement, objectives and the methods used in meeting the objectives of the project.

### **5.3.2 Chapter 2 – The Healthcare Sector**

#### Sub-Objective

- Investigate the health sector and the special needs of health information security.



### Research Question

- How is the health sector constituted and what are the unique security needs of the health sector?

This chapter presented the nature and activities of the health sector, considered technological advancements in the sector and the challenges and benefits that have been brought about by these advancements. One of the challenges brought about by technological advancements in the health sector relates to the security and privacy of health information. Chapter 2 showed that it is important to protect health information and that there are unique requirements inherent to securing health information. It was concluded that information security management best practices must be followed in order to address security requirements comprehensively.

### **5.3.3 Chapter 3 - Information Security Management Standards**

#### Sub-Objective

- Examine information security management practices in general as well as in the health sector.

#### Research Question

- How can the unique security needs of the health sector be addressed through proper information security management practices?

Chapter 3 commenced with an investigation of the concepts of information security, risk management and information security management. The chapter further highlighted the relevance of these concepts in the healthcare context. It was shown how risk management relates to information security management. The ISO standards relevant to information security management were introduced and the evolution of each of the standards discussed. This discussion familiarized the reader with the high-level structure and content of the standards. This set the stage for the comparative analyses required to be done in Chapter 4.

### 5.3.4 A Comparative Analysis of the ISO/IEC 27002 and ISO/IEC 27799 Information Security Management Standards

#### Sub-Objectives

- Perform a high level comparison of the ISO 27002 and ISO 27799 standards.
- Execute and document the results of a detailed comparative analysis of the security control clauses in both standards.
- Determine the approach of the ISO 27799 in regard to the establishment of an information security management system.
- Based on the afore-mentioned actions, critique the contribution of the ISO 27799 to serving the security needs of the health sector.

#### Research Questions

- How does the overall structure of the ISO 27002 and ISO 27799 standards differ?
- How do the eleven security control clauses and 39 main security control categories described in ISO 27002, differ in ISO 27799?
- Will the application of the ISO 27799 ensure that privacy and security of health information concerns are addressed adequately and continuously through establishing a robust information security management system?

Chapter 4 presented the results of the comparison of the ISO 27002 and ISO 27799 standards. The structural differences between the standards were addressed first.

The detailed comparison was presented in three parts according to the structural similarities of the standards, namely the introductory, main body and auxiliary parts of the standards. A summary of the findings of the comparison of each of these parts was presented and used to compile a final critique of the contribution of the ISO 27799 to information security management in the health sector. The Chapter showed that the ISO 27799 includes aspects relating to the establishment of an ISMS, which are not included in the ISO 27002, but rather in the ISO 27001.

### 5.3.5 Chapter 5 – Conclusion

The research project is concluded in this chapter. The achievement of the research objectives are discussed together with the benefits and limitations of the research and proposed future research directions.

## 5.4 Benefits and Limitations of the Research

The benefits of this research are summarized as follows:

- The explicit identification of aspects of the ISO 27799 which are not addressed in the ISO 27002, for example, new (additional) controls or controls that are compulsory in the ISO 27799 and not in the ISO 27002, enable the establishment of the security requirements which are of particular importance in the health sector.
- The results of the comparison of the standards can be used by organizations in the health sector to guide their adoption of this new standard. It will be particularly useful where the ISO 27002 has been used previously to facilitate an expedited understanding of the requirements over and above the ISO 27002.

The main limitation of the research is that the critique of the contribution of the ISO 27799 to the security needs of the health sector, was based on literature only. The scope of the project precluded the inclusion of a case study. Secondly, it is acknowledged that the research would benefit from gaining the perspectives of security practitioners in the health sector.

## 5.5 Future Research

A valuable follow-up on the research reported on in this dissertation, will be to do a case study in the health sector to determine whether the new information security management standard (ISO 27799) will assist in achieving the following benefits touted by the standard (ISO 27799, 2008):

- Maintained confidentiality and integrity of data in the care of healthcare organizations;
- Continuous availability of health information systems;
- Upheld accountability for health information;
- Improved interoperability; and
- Safe adoption of new collaborative technologies in the delivery of healthcare.

Such a study could measure the effectiveness of the information security programme in a healthcare setting that has adopted the ISO 27002 as a guideline for security. Similarly, the effectiveness of the programme can be measure after such an establishment adopts the ISO 27799. This will indicate whether the ISO 27799 contributed to improved security in the particular healthcare setting. The study can further obtain feedback about the relevance of the standard's unique security requirements (as compared to the ISO 27002) and the guidance it provides in the healthcare context.

Another avenue is for the study to be expanded to include additional information security management standards and best practices, for example, the *Information Security Management: National Health Service (NHS) Code of Practice* used in the United Kingdom. The results of such a comparative analysis will then serve as a guideline to organizations already using these other standards or best practices as to what the requirements of the ISO 27799 are that are not included in their environments.

## 5.6 Conclusion

At the conclusion of this research project, it is appropriate to reflect on various authors' input referenced in this dissertation. It was established that technology advancements have brought changes and improvements in the healthcare information systems that execute, access, store and retrieve patient and other important healthcare information. However these changes introduced significant information security and privacy challenges, including threats which could compromise the security and privacy of patients' information and other sensitive healthcare assets. The investigation further indicated that these challenges can be minimized through the adoption and implementation of information security management standards. Hence the study conducted an extensive investigation to compare the ISO 27002 and ISO 27799 information security management standards.

In this chapter, it was illustrated that the objectives which were established at the beginning of the research project, were accomplished. The information covered in different chapters of the dissertation was reviewed and ideas for future research were suggested.

The increasing use of wireless and Internet technologies in healthcare delivery, and the consequent growth of the electronic exchange of personal health information between health professionals, not only makes the need for effective IT security management in healthcare all the more urgent, but also implies a clear benefit to adopting a common reference for information security management in healthcare (ISO, 2008). It therefore becomes important for healthcare organizations to adopt standards that enable them to implement proper information security controls to protect the data in their care.

The ISO 27799 standard provides guidance for information security management requirements in the healthcare sector. From this perspective, the ISO 27799 standard satisfies an important need, namely to guide healthcare organizations in the implementation of security measures to achieve health information security

goals. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information (ISO 27799, 2008).

---

# References

---

- Ahlfeldt, R-M. (2006). Information security in distributed healthcare domain: Exploring the problems and needs of different healthcare providers. In *Licentiate Thesis No. 06-003, Stockholm University. Sweden.*
- Al-Daig, H. (2004). *National Information Technology Strategy in Healthcare Sector in Kingdom of Saudi Arabia* [PowerPoint slides]. Retrieved January 04, 2009, from [http://ehealthinitiativelight.org/assets/documents/GenevaHamad\\_Presentation.ppt](http://ehealthinitiativelight.org/assets/documents/GenevaHamad_Presentation.ppt)
- Arnason, S.T., & Willett, K.D. (2007). Introduction to International Standards Organization Security Standards. In *How to Achieve 27001 Certification: An Example of Applied Compliance Management* (Chapter 1). Retrieved November 15, 2008, from <http://www.infosectoday.com/Articles/27001.htm>
- Association of Insurance and Risk Managers [AIRMIC], National Forum for Risk Management in the Public Sector in the UK [ALARM], & Institute of Risk Management [IRM]. (2002). *A Risk Management Standard*. Retrieved March 28, 2008, from <http://www.airmic.com/download.cfm/docid/285D292B-C593-4CA2-8D605B2A79D7744E>
- Australian General Practice Network [AGPN]. (2007). *Information Management Policy for the Australian General Practice Network V1.1*. Retrieved October 23, 2008, from [http://www.agpn.com.au/\\_\\_data/assets/pdf\\_file/0016/1186/136800.pdf](http://www.agpn.com.au/__data/assets/pdf_file/0016/1186/136800.pdf)

- Aydin, M.N., Harmsen, F., Slooten, K., & Stegwee, R.A. (2004). An Agile Information Systems Development Method in Use. *Turkish Journal of Electrical Engineering and Computer Sciences*, 12(2), 127-138. Retrieved March 21, 2008, from <http://journals.tubitak.gov.tr/elektrik/issues/elk-04-12-2/elk-12-2-5-0404-6.pdf>
- Blas, E. (2002). Impact Evaluation of Health Systems Reform in Different Countries. *Health Sector Reform (Final Report Series), No. 55*. Retrieved July 13, 2008, from <http://www.who.int/tdrold/research/finalreps/no55.htm>
- Box, D. (2008). Business Process Security Maturity - A Paradigm Convergence. In *Academic Dissertation, Nelson Mandela Metropolitan University*. South Africa.
- Broderick, J.S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, 11(1), 26-31. Available from ScienceDirect full-text scientific online database.
- Buckovich, S.A., Rippen, H.E., & Rozen, M.J. (1999). Driving toward guiding principles: A goal for privacy, confidentiality, and security of health information. *Journal of the American Medical Informatics Association*, 6(2), 122-33. Retrieved February 14, 2008, from <http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=61351&blobtype=pdf>
- Canadian Institute for Health Information [CIHI]. (1996). *Working Group 1: Health Information Model – Background Document*. Retrieved November 16, 2008, from [http://secure.cihi.ca/cihiweb/en/downloads/partner\\_docs\\_e\\_hlthmod.pdf](http://secure.cihi.ca/cihiweb/en/downloads/partner_docs_e_hlthmod.pdf)
- Carlson, T. (2008). *Understanding ISMS*. Available from <http://www.orangeparachute.com/whitepaper-request.asp>



- Dube, K., Mtenzi, F., Shoniregun, C.A. (2009). *Electronic Healthcare Information Security* [Abstract]. Retrieved December 11, 2008, from <http://www.springer.com/computer/security+and+cryptology/book/978-0-387-84817-4>
- Edmead, M.T. (2006). Are You Familiar With the Most Recent ISO/IEC 17799 Changes? *ITAudit*, 9. Retrieved October 19, 2007, from <http://www.theiia.org/ITAuditArchive/index.cfm?act=ITAudit.printi&iid=467&aid=2209>
- Eloff, J.H.P., & Eloff, M.M. (2005). Information security architecture. *Computer Fraud & Security*, 2005(11), 10-16. Available from ScienceDirect full-text scientific online database.
- Fernando, J. (2004). Factors that have Contributed to a Lack of Integration in Health Information System Security. *The Journal on Information Technology in Healthcare*, 2(5), 313-328. Retrieved May 16, 2008, from [cui.unige.ch/~wac/publications/Wac\\_JITH\\_vol2,\\_issue5\\_MobiHealth\\_p.365-373\\_2004.pdf](http://cui.unige.ch/~wac/publications/Wac_JITH_vol2,_issue5_MobiHealth_p.365-373_2004.pdf)
- Frangopoulos, E.D., & Eloff, M.M. (2004). A Comparative Study of Standards and Practices related to Information Security Management. In: *Peer-reviewed Proceedings of the ISSA 2004 Enabling Tomorrow Conference*. 30 June – 2 July 2004, Midrand, South Africa: ISSA. Retrieved May 21, 2008, from <http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/033.pdf>
- Fraser, R. (2007). ISO Security Standards for e-Health [PowerPoint slides]. *2nd e-Health Congress*. 18 - 20 October 2007, Antalya, Turkey. Retrieved August 13, 2008, from [http://www.saglik.gov.tr/bilisim07/Dosyalar/Security\\_Standards\\_in\\_Health\\_e-Health\\_Congress\\_TurkeyRossFraser.pdf](http://www.saglik.gov.tr/bilisim07/Dosyalar/Security_Standards_in_Health_e-Health_Congress_TurkeyRossFraser.pdf)

- Fujitsu. (2006). *HealthCare Document Imaging Trend Report*. Retrieved September 21, 2008, from [http://www.fujitsu.com/downloads/COMP/fcpa/scanners/healthcare-document-imaging-trend\\_wp.pdf](http://www.fujitsu.com/downloads/COMP/fcpa/scanners/healthcare-document-imaging-trend_wp.pdf)
- Gerber, M., von Solms, R., & Overbeek, P. (2001). Formalizing Information Security Requirements. *Information Management & Computer Security*, 9(1), 32-37.
- Gomes, R., & Lapão, L.V. (2008). The Adoption of IT Security Standards in a Healthcare Environment. In S.K. Andersen, G.O. Klein, S. Schulz, J Aarts, & M.C. Mazzoleni (Eds.), *eHealth Beyond the Horizon – Get IT There - Proceedings of MIE2008 – The XXIst International Congress of the European Federation for Medical Informatics* (pp. 765-770). The Netherlands: IOS Press. Retrieved January 05, 2009, from [www.hst.aau.dk/~ska/MIE2008/ParalleSessions/PapersForDownloads/10.Sta/SHTI136-0765.pdf](http://www.hst.aau.dk/~ska/MIE2008/ParalleSessions/PapersForDownloads/10.Sta/SHTI136-0765.pdf)
- Hofstee, E. (2006). *Constructing a good dissertation: A practical guide to finishing master's, MBA or PhD on schedule*. Sandton, South Africa: EPE.
- Hübner, U., & Elmhorst, M.A. (Eds.). (2008). *eBusiness in Healthcare: From eProcurement to Supply Chain Management*. London: Springer-Verlag. Available from SpringerLink database.
- Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001:2005. *ISO Management Systems, Jan-Feb 2006*, 15-18. Retrieved June 27, 2008, from [www.iso.org/iso/info\\_security.pdf](http://www.iso.org/iso/info_security.pdf)
- International Organization for Standardization [ISO]. (2008, August 28). *New ISO standard provides information security guidelines for the health sector* [News]. Retrieved July 09, 2008, from <http://www.iso.org/iso/pressrelease.htm?refid=Ref1154>

- ISO 13335-1. (2004). *ISO/IEC 13335-1: Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management* (1st ed.). Switzerland: International Organization for Standardization.
- ISO 17799 FAQ. (n.d.). *Frequently Asked Questions about ISO27002 (ISO 17799)*. Retrieved March 14, 2008, from [http://iso-17799.safemode.org/index.php?page=ISO17799\\_FAQ](http://iso-17799.safemode.org/index.php?page=ISO17799_FAQ)
- ISO 17799. (2005). *ISO/IEC 17799: Information Technology – Security Techniques – Code of Practice for Information Security Management*. Switzerland: International Organization for Standardization.
- ISO 27001 Security. (n.d.). *ISO/IEC 27002*. Retrieved July 23, 2008, from <http://www.iso27001security.com/html/27002.html>
- ISO 27001. (2005). *ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems - Requirements* (1st ed.). Switzerland: International Organization for Standardization.
- ISO 27002. (2005). *ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management* (1st ed.). Switzerland: International Organization for Standardization.
- ISO 27799. (2008). *ISO/IEC 27799: Health informatics — Information security management in health using ISO/IEC 27002* (1st ed.). Switzerland: International Organization for Standardization.
- Janczewski, L., & Xinli Shi, F. (2002). Development of Information Security Baselines for Healthcare Information Systems in New Zealand. *Computers and Security*, 21(2), 172-192.

- Kokolakis, S.A., Demopoulos, A.J., & Kiountouzis, E.A. (2000). The Use of Business Process Modelling in Information Systems Security Analysis and Design. *Information Management & Computer Security*, 8(3), 107-116.
- Langabeer, J. (2008). *Health Care Operations Management: A Quantitative Approach to Business and Logistics*. Sudbury: Jones & Bartlett Publishers.
- Lineman, D.J. (2008). *PCI Policy Compliance Using Information Security Policies Made Easy*. Retrieved October 12, 2008, from <http://www.informationshield.com/papers/PCI-Security-Policies-Using-ISPME.pdf>
- Maker, J., & Power, M. (2007, September 23). Special Report: Manto Tshabalala-Msimanga - Top cop set on trail of Manto's missing medical file. *The Times*. Retrieved October 12, 2008, from <http://www.thetimes.co.za/SpecialReports/Manto/Article.aspx?id=570532>
- Maseti, O. (2008). A Model for Role-Based Security Education, Training and Awareness in the South African Healthcare Environment. In *Academic Dissertation, Nelson Mandela Metropolitan University*. South Africa.
- Murray, C.J.L., & Frenk, J. (2000). A framework for assessing the performance of health systems. *Bulletin of the World Health Organization*, 78(6), 717-731. Retrieved December 13, 2008, from [http://www.who.int/bulletin/archives/78\(6\)717.pdf](http://www.who.int/bulletin/archives/78(6)717.pdf)
- National Academies Press. (1997). *For the record: Protecting electronic health information*. Retrieved December 18, 2008, from [http://www.nap.edu/catalog.php?record\\_id=5595](http://www.nap.edu/catalog.php?record_id=5595)
- Nemasisi, E. (2007). A Legal Compliance Model for Privacy and Confidentiality in South African Rural Hospitals. In *Academic Dissertation, Nelson Mandela Metropolitan University*. South Africa.

- Nonprofit Risk Management Center. (2008). *Risk Management*. Retrieved October 23, 2008, from [http://www.communitydevelopmentworks.org/LinkClick.aspx?link=word\\_docs%2FTips+of+the+Month%2FJune+2008.doc&tabid=728&mid=3990](http://www.communitydevelopmentworks.org/LinkClick.aspx?link=word_docs%2FTips+of+the+Month%2FJune+2008.doc&tabid=728&mid=3990)
- NSW Department of Commerce. (2007). *Information Security Guidelines* (Commerce Report No. 07006). Retrieved June 12, 2008, from <http://www.gcio.nsw.gov.au/products-and-services/policies-guidelines/InformationSecurityGuidelineV1.1.pdf>
- O'Carroll, P.W., Yasnoff, W.A., Ward, M.E., Ripp, L.H., & Martin, E.L. (Eds.). (2002). *Public Health Informatics and Information Systems*. New York: Springer-Verlag.
- Perjons, E., Wangler, B., Wäyrynen, J., & Ahlfeldt, R-M. (2005). Introducing a process manager in healthcare: An experience report. *Health Informatics Journal*, 11(1), 45-61. Available from SAGE journals online database.
- Poole, V.R. (2005). ISO/IEC 17799:2005 and Future ISMS Standards [PowerPoint slides]. *Cyprus Infosec 2005 Workshop*. Retrieved January 06, 2009, from <http://www.cyprusinfosec.org/upload/7799%20workshop%20cyprus05.ppt#260,14,3>
- Poremba, S.M. (2008, September 10). Health information security standard issued. *SC Magazine*. Retrieved September 25, 2008, from <http://www.scmagazineus.com/health-information-security-standard-issued/article/116516/>
- Rodrigues, R.J. (2000). Information systems: The Key to Evidence-Based Health Practice. *Bulletin of the World Health Organization*, 78(11), 1344-1351. Retrieved July 24, 2008, from [http://www.who.int/bulletin/archives/78\(11\)1344.pdf](http://www.who.int/bulletin/archives/78(11)1344.pdf)

- Rowlands, D. (2007). *Report on ISO TC215 Health Informatics standards development meetings in Montreal, March 2007*. Retrieved July 17, 2008, from <http://www.e-healthstandards.org.au/downloads/TC215%20Montreal%20Report.pdf>
- Savage, G.T., Taylor, R.L., Rotarius, T.M., & Buessler, J.A. (1997). Governance of integrated delivery systems/networks: A stakeholder approach. *Health Care Management Review, 22*(1), 7-20. Available from PubMed database.
- Schlarman, S. (2002). The Case for a Security Information System. *Information Security Journal: A Global Perspective, 11*(1), 44-50. Available from informaworld™ online database.
- Siponen, M. (2002). Designing Secure Information Systems and Software: Critical Evaluation of the Existing Approaches and a New Paradigm. In *Academic Dissertation, University of Oulu*. Oulu, Finland.
- Siponen, M. (2003). Information Security Management Standards: Problems and Solutions. In: *Proceedings of the 7th Pacific Asia Conference on Information Systems*. 10-13 July 2003, Adelaide, South Australia. Retrieved November 17, 2008, from, <http://www.pacis-net.org/file/2003/papers/security/284.pdf>
- Smith, E., & Eloff, J.H.P. (1999). Security in Health-Care Information Systems - Current Trends. *International Journal of Medical Informatics, 54*(1), 39-54.
- Solanas, A., & Castellà-Roca, J. (2008). RFID Technology for the Health Care Sector. *Recent Patents on Electrical Engineering, 1*, 22-31. Retrieved August 15, 2008, from <http://www.bentham.org/eeng/samples/eeng%201-1/Solanas.pdf>
- Sprague, L. (2004, September 29). Electronic Health Records: How Close? How Far to Go? *National Health Policy Forum Issue Brief, No. 800*. Retrieved July 28, 2008, from [http://www.nhpf.org/library/issue-briefs/IB800\\_EHRs.pdf](http://www.nhpf.org/library/issue-briefs/IB800_EHRs.pdf)

- Sullivan, F., & Wyatt, J.C. (2006). *ABC of Health Informatics*. Oxford, UK: Blackwell Publishing.
- Taylor, S. (n.d.). *Information Security Management*. Retrieved March 29, 2008, from <http://www.security.auckland.ac.nz/FAQ.htm>
- Tessier, C. (2004). *Continuity of Care Record [PowerPoint Slides]*. Retrieved April 20, 2008, from [www.astm.org/COMMIT/E31\\_CCRJuly04.ppt](http://www.astm.org/COMMIT/E31_CCRJuly04.ppt)
- The ISO 27000 Directory. (n.d.). *An Introduction to ISO 27799*. Retrieved July 18, 2008, from <http://www.27000.org/iso-27799.htm>
- Tuyikeze, T., & Pottas, D. (2005). Information Security Management and Regulatory Compliance in the South African Health Sector. In: *Peer-reviewed Proceedings of the ISSA 2005 New Knowledge Today Conference*. 29 June – 1 July 2005, Sandton, South Africa: ISSA. Retrieved November 11, 2007, from [http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/038\\_Article.pdf](http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/038_Article.pdf)
- U.S. Congress. (1993). *Protecting Privacy in Computerized Medical Information* (Office of Technology Assessment Publication No. OTA-TCT-576). Washington, DC: U.S. Government Printing Office. Retrieved December 22, 2008, from <http://mccurley.org/papers/9342.PDF>
- VeriSign. (2008). *Information Security and Risk Management*. Retrieved December 12, 2008, from [http://entsecurity.verisign.com/managed\\_security\\_services/information\\_security\\_and\\_risk\\_management](http://entsecurity.verisign.com/managed_security_services/information_security_and_risk_management)
- Von Solms, R., Von Solms, S.H. (2006). Information Security Governance : Due Care. *Computers & Security*, 25(7), 494 – 497.
- Waegemann, C.P. (2007). *The Problem with Interoperability*. Retrieved April 2, 2008, from [http://www.medrecinst.com/pdf/pmd\\_peter.pdf](http://www.medrecinst.com/pdf/pmd_peter.pdf)

- Wagner, I. (1999, July 30). Ethical Issues of Healthcare in the Information Society. *Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, No. 13*. Retrieved March 13, 2008, from [http://ec.europa.eu/european\\_group\\_ethics/docs/avis13\\_en.pdf](http://ec.europa.eu/european_group_ethics/docs/avis13_en.pdf)
- Wallin, E., & Xu, Y. (2008). Managing Information Security in Healthcare: A Case Study in Region Skåne. In *Master Thesis, Lund University*. Sweden. Retrieved August 26, 2008, from <http://biblioteket.ehl.lu.se/olle/papers/0003129.pdf>
- Wikipedia<sup>a</sup>. (2008, June 23). *Risk management*. Retrieved June 23, 2008, from [http://en.wikipedia.org/wiki/Risk\\_management](http://en.wikipedia.org/wiki/Risk_management)
- Wikipedia<sup>b</sup>. (2008, September 15). *Information security management system*. Retrieved September 15, 2008, from [http://en.wikipedia.org/wiki/Information\\_Security\\_Management\\_System](http://en.wikipedia.org/wiki/Information_Security_Management_System)
- World Health Organization [WHO]. (2008). *The World Health Report 2008 - Primary Health Care (Now More Than Ever)*. Retrieved March 21, 2009, from [http://www.who.int/entity/whr/2008/whr08\\_en.pdf](http://www.who.int/entity/whr/2008/whr08_en.pdf)
- Yhan, G. (n.d.). *ISO 17799: Scope and implementation – Part 1 Security Policy*. Retrieved November 19, 2008, from <http://www.sahw.com//iso/ISO17799.pdf>



<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
	7.1 GENERAL	NEW CLAUSE	This clause contains specific advice about the clauses and security categories described in ISO 27002. It essentially motivates the need for the ISO 27799 and explicitly indicates that the guidance given in the ISO 27799 is in addition to, but not a replacement for that found in the ISO 27002.
5. SECURITY POLICY	7.2 INFORMATION SECURITY POLICY		
5.1 <i>Information Security Policy</i>			
5.1.1 Information security policy document	7.2.1 Information security policy document	>	<p><b>Control</b> The application of this security control is mandatory in healthcare. <b>SHALL</b></p> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>7.2.1 (a-e) Specific factors that are required to be included in the information security policy document. <i>Example:</i> <i>The need for and goals of health information security;</i></li> <li>7.2.1 (f-n) Factors which are unique to the health sector which must be considered. <i>Example:</i> <i>The rights of subjects of care;</i></li> <li>The policy framework must include documented policy, controls and procedures that cover interactions with third-parties. Where personal data crosses national or jurisdictional boundaries, the provisions of ISO 22857</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			must be included in the policy.
5.1.2 Review of information security policy	7.2.2 Review of the information security policy document	>	<p><b>Control</b> The control statement requires staged reviews such that the totality of the policy is addressed at least annually. It further requires the policy to be reviewed after the occurrence of a serious security incident.</p> <p><b>Implementation guidance</b> 7.2.2 (a-g) Additional factors that the review of the information security policy document must address.</p> <p><i>Example:</i> <i>The latest guidance and recommendations from health professional associations and from information privacy commissioners regarding the protection of personal health information;</i></p>
<b>6 ORGANIZATION OF INFORMATION SECURITY</b>	<b>7.3 ORGANIZING INFORMATION SECURITY</b>		
	<b>7.3.1 General</b>	<b>NEW MSC</b>	The need for an explicit and robust information security management infrastructure is stressed, especially where organizations rely upon managed services provided by third parties.
<b>6.1 Internal organization</b>	<b>7.3.2 Internal organization</b>		

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
6.1.1 Management commitment to information security	7.3.2.1 Management commitment to information security, information security coordination and allocation of information security responsibilities	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>7.3.2.1 (b) The need to have an Information Security Management Forum (ISMF) in place.</li> <li>At a minimum, one individual to be responsible for health information security.</li> <li>The ISMF to meet monthly or on a near-to-monthly basis.</li> <li>A formal scope statement which defines the boundary of compliance activity in terms of people, processes, places, platforms and applications.</li> </ul> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>The nature of management responsibility in organizations that are custodians of personal health information is explicated.</li> <li>Information access by subjects of care, reporting within the organizational structure and timely delivery of information are stated as required outputs of the adopted organizational structure (internal security organization).</li> </ul>
6.1.2 Information security coordination			
6.1.3 Allocation of information security responsibilities			
6.1.4 Authorization process for information processing facilities	7.3.2.2 Authorization process for information processing facilities	=	
6.1.5 Confidentiality agreements	7.3.2.3 Confidentiality agreements	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Confidentiality agreements applicable to all personnel accessing health information and specifying the</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<p>confidential nature of the information are required.</p> <p><b><u>Implementation guidance</u></b> Reference to the penalties applicable to personnel when a breach occurs, must be included.</p>
6.1.6 Contact with authorities	7.3.2.4 Contact with authorities, contact with special interest groups, and independent review of information security	=	
6.1.7 Contact with special interest groups			
6.1.8 Independent review of information security			
<b>6.2 External parties</b>	<b>7.3.3 Third parties</b>		
6.2.1 Identification of risks related to external parties	7.3.3.1 Identification of risks related to external parties	>	<p><b><u>Control</u></b> The application of this security control is mandatory in healthcare. <b>SHALL</b></p> <p><b><u>Implementation guidance</u></b> The importance of protecting the rights of subjects of care where external parties are involved is stressed. It is mentioned that the jurisdiction governing the subject of care shall apply, even if the external party is governed by a different jurisdiction.</p>
6.2.2 Addressing security when dealing with customers	7.3.3.2 Addressing security when dealing with customers	=	

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
6.2.3 Addressing security in third party agreements	7.3.3.3 Addressing security in third party agreements	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>7.3.3.3 (a-h) The security requirements that must be covered in a formal contract between the healthcare organization and the third party are specified. <i>Example:</i> <i>The arrangement for representation of the third party in appropriate health organization meetings and working groups;</i></li> </ul> <p><b>Implementation guidance</b> Where the flow of personal health information crosses jurisdictional boundaries, the ISO 22857 must serve as a directive.</p>
<b>7 ASSET MANAGEMENT</b>	<b>7.4 ASSET MANAGEMENT</b>		
<b>7.1 Responsibility for assets</b>	<b>7.4.1 Responsibility for health information assets</b>		
7.1.1 Inventory of assets		>	<p><b>Control</b> A designated custodian of health information assets is required.</p> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>Rules to maintain the currency of assets are required. <i>Example:</i> <i>The currency of a drug database;</i></li> <li>The unique identification of medical devices with special</li> </ul>
7.1.2 Ownership of assets			
7.1.3 Acceptable use of assets			

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			security considerations in relation to the environment in which they operate and to the electromagnetic emissions that occur during their operation is required.
<b>7.2 Information classification</b>	<b>7.4.2 Health information classification</b>		
7.2.1 Classification guidelines	7.4.2.1 Classification guidelines	>	<p><b><u>Control</u></b> All personal health information should uniformly be classified as confidential (i.e. this information will never cease to be sensitive).</p> <p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>• 7.4.2.1 (a-c) The unique characteristics of information assets in healthcare are explicated. <i>Example:</i> <i>The confidentiality of personal health information is often largely subjective, context-dependent and its confidentiality can shift over the lifetime of an individual's health record (due to for example changing societal attitudes).</i></li> <li>• The records of subjects of care who may be at elevated risk of access by those who do not have a need to know, must be identified.</li> <li>• The criticality of information, processes, IT devices, software, locations and personnel (as relating to the ongoing provision of healthcare) must also be classified through a risk assessment.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
7.2.2 Information labeling and handling	7.4.2.2 Information labeling and handling	>	<p><b><u>Control</u></b> Health information systems are required to inform users of the confidentiality of personal health information that can be accessed from the system and hardcopy output must be labeled as confidential when containing personal health information.</p> <p><b><u>Implementation guidance</u></b> The additional requirements in the control statement are re-stated.</p>
<b>8 HUMAN RESOURCES SECURITY</b>	<b>7.5 HUMAN RESOURCES SECURITY</b>		
<b>8.1 Prior to employment<sup>4)</sup></b>	<b>7.5.1 Prior to employment</b>		
8.1.1 Roles and responsibilities	7.5.1.1 Roles and responsibilities	>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>All involvement with the processing of personal health information must be documented in job descriptions of the relevant staff members.</li> <li>Special attention needs to be given to the roles and responsibilities of temporary or short-term staff such as locums, students, interns, etc.</li> </ul>
8.1.2 Screening	7.5.1.2 Screening	>	<p><b><u>Control</u></b> At a minimum, the identity, current address and previous employment of staff, contractors and volunteers at the time of job applications must be verified.</p> <p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>The importance of knowing how and where to contact health professional staff is emphasized.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<ul style="list-style-type: none"> <li>Other forms of check, e.g. by professional bodies and academic institutions are suggested.</li> </ul>
8.1.3 Terms and conditions of employment	7.5.1.3 Terms and conditions of employment	>	<p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>The confidentiality of personal health information survives the completion of employment in perpetuity. This must be stated in the terms and conditions of employment.</li> <li>With respect to clinical staff, the terms and conditions of employment must specify the rights of access of staff to the records of subjects of care and to associated health information systems in the event of third-party claims.</li> <li>The screening process should be repeated if there is a long period between the date of recruitment and the date of appointment of an employee.</li> </ul>
<b>8.2 During Employment</b>	<b>7.5.2 During Employment</b>		
8.2.1 Management responsibilities	7.5.2.1 Management responsibilities	>	<p><b>Implementation guidance</b></p> <p>Health information systems must be managed such that the concerns of subjects of care who do not wish their personal health information to be accessed by health workers who are neighbours, colleagues or relatives, are addressed.</p>
8.2.2 Information security awareness, education and training	7.5.2.2 Information security awareness, education and training	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Information security education and training must be provided on induction to all employees and, where relevant, third-party contractors, researchers, students and volunteers who process personal health information.</li> </ul>



<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
8.2.3 Disciplinary process	7.5.2.3 Disciplinary process	>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>Disciplinary processes must be known to the subject(s) of the disciplinary process as it must follow procedures that are reflected in policy.</li> <li>Disciplinary processes must comply with the agreements reached between health professionals and health professional bodies.</li> </ul>
<b>8.3 Termination or change of employment</b>	<b>7.5.3 Termination or change of employment</b>		
8.3.1 Termination responsibilities	7.5.3.1 Termination responsibilities and return of assets	>	<p><b><u>Implementation guidance</u></b></p> <p>The nature of employment in healthcare (e.g. staff progressing through training programmes and other “rotations”) is emphasized. As each type of position could require a fundamental change in access rights, it is recommended that such changes in employment be processed (in terms of termination of rights) similar to resignations.</p>
8.3.2 Return of assets			
8.3.3 Removal of access rights	7.5.3.2 Removal of access rights	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Termination of access privileges must be done as soon as possible (i.e. not necessarily upon termination of services).</li> </ul> <p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>The termination of access rights of potentially large numbers of temporary staff, especially in large hospitals,</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<p>with short-term access to personal health information, must be managed carefully.</p> <ul style="list-style-type: none"> <li>• Transactions that take place after the time of care must be taken into account in procedures on the removal of access rights.</li> </ul>
<b>9 PHYSICAL AND ENVIRONMENTAL SECURITY</b>	<b>7.6 PHYSICAL AND ENVIRONMENTAL SECURITY</b>		
<b>9.1 Secure areas</b>	<b>7.6.1 Secure areas</b>		
9.1.1 Physical security perimeter	7.6.1.1 Physical security perimeter	>	<p><b><u>Control</u></b> Secure areas (designated by security perimeters) must be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.</p> <p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>• The unique situation in healthcare settings, namely that operational areas are frequented by subjects of care, is emphasized. This requires special attention to be given to the instantiation of security perimeters.</li> <li>• Physical security measures for information must be coordinated with physical security and safety measures for subjects of care, because clients in healthcare are often unable to physically provide for their own personal safety and security.</li> </ul>
9.1.2 Physical entry controls	7.6.1.2 Physical entry control, securing offices, rooms	>	<p><b><u>Implementation guidance</u></b> Measures must be employed to ensure that the public are</p>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
9.1.3 Securing offices, rooms and facilities	and facilities, protecting against external and environmental threats, working in secure areas		only as close to IT equipment (servers, storage devices, terminals and displays) as physical constraints and clinical processes demand.
9.1.4 Protecting against external and environmental threats			
9.1.5 Working in secure areas			
9.1.6 Public access, delivery and loading areas	7.6.1.3 Public access, delivery and loading areas	>	<p><b><u>Implementation guidance</u></b>  Physical areas in healthcare where health information is gathered through interview and that contain systems where data are viewed on screen must be subject to additional scrutiny.  <i>Example:</i>  In emergency rooms companions or relatives could potentially be exposed to significant amounts of sensitive verbal and visual information on other subjects of care. The posting of notices to curtail the discussion of patient cases is often used in this regard.</p>
<b>9.2 Equipment security</b>	<b>7.6.2 Equipment security</b>		
9.2.1 Equipment siting and protection	7.6.2.1 Equipment siting and protection	>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>• Workstations must be situated so as to avoid unintended viewing or access by subjects of care and the public.</li> <li>• Healthcare organizations, especially hospitals, must ensure that the siting and protection guidelines for IT equipment minimize exposure to electromagnetic emissions.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
9.2.2 Supporting utilities	7.6.2.2 Support utilities, cabling security and equipment maintenance	>	<b><u>Implementation guidance</u></b> Network and other cabling in areas with high emissions from medical devices must be protected through the use of shielding.
9.2.3 Cabling security			
9.2.4 Equipment maintenance			
9.2.5 Security of equipment off-premises	7.6.2.3 Security of equipment off-premises	>	<b><u>Control</u></b> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>The incidental or perpetual off-site use of medical devices that record or report data must be authorized. <i>Example:</i> <i>Ambulance personnel</i></li> </ul>
9.2.6 Secure disposal or re-use of equipment	7.6.2.4 Secure disposal or re-use of equipment	>	<b><u>Control</u></b> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>All media containing health information application software or personal health information must be securely overwritten or destroyed when no longer required for use.</li> </ul>
9.2.7 Removal of property	7.6.2.5 Removal of property	>	<b><u>Control</u></b> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Removal of equipment, data or software from a site, or relocation within a site, must be authorized.</li> </ul>
<b>10 COMMUNICATIONS AND OPERATIONS MANAGEMENT</b>	<b>7.7 COMMUNICATIONS AND OPERATIONS MANAGEMENT</b>		

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
<b>10.1 Operational procedures and responsibilities</b>	<b>7.7.1 Operational procedures and responsibilities</b>		
10.1.1 Documented operating procedures	7.7.1.1 Documented operating procedures	=	
10.1.2 Change management	7.7.1.2 Change management	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>A formal and structured change control process must be used to ensure the appropriate control of host applications and systems and continuity of patient care.</li> </ul> <p><b>Implementation guidance</b> The disastrous consequences for patient care and safety due to inappropriate, inadequately tested or incorrect changes are emphasized. Therefore the change process must explicitly record and assess the risks of the change.</p>
10.1.3 Segregation of duties	7.7.1.3 Segregation of duties	>	<p><b>Implementation guidance</b> IT systems must have application functionalities that enforce approval of clinical processes by different role holders.</p>
10.1.4 Separation of development, test and operational facilities	7.7.1.4 Separation of development, test and operational facilities	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>The physical or virtual separation of development and testing environments from operational environments must be done.</li> <li>Rules directing the migration of software from</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			development to operational status must be defined and documented.
<b>10.2 Third party service delivery management</b>	<b>7.7.2 Third party service delivery management</b>		
10.2.1 Service delivery			<b>Implementation guidance</b> In order to simplify third party service delivery management, the use of a formal agreement which specifies the minimum set of controls to be implemented, is recommended.
10.2.2 Monitoring and review of third party services		>	
10.2.3 Managing changes to third party services			
<b>10.3 System planning and acceptance</b>	<b>7.7.3 System planning and acceptance</b>		
10.3.1 Capacity management	7.7.3.1 Capacity management	=	
10.3.2 System acceptance	7.7.3.2 System acceptance	>	<b>Control</b> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Suitable acceptance tests based on predetermined acceptance criteria shall be carried out prior to system acceptance.</li> </ul> <b>Implementation guidance</b> The extent and rigour of system acceptance tests must be scaled to a level consistent with the identified risks of the change.

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
<b>10.4 Protecting against malicious and mobile code</b>	<b>7.7.4 Protection against malicious and mobile code</b>		
10.4.1 Controls against malicious code	7.7.4.1 Controls against malicious code	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Appropriate prevention, detection and response controls to protect against malicious software and appropriate user awareness training SHALL be implemented.</li> </ul>
10.4.2 Controls against mobile code	7.7.4.2 Controls against mobile code	=	
<b>10.5 Back-up</b>	<b>7.7.5 Health information backup</b>		
10.5.1 Information back-up		>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>All personal health information SHALL be backed up in an encrypted format and stored in a physically secure site.</li> </ul>
<b>10.6 Network security management</b>	<b>7.7.6 Network security management</b>		
10.6.1 Network controls	7.7.6.1 Network controls	=	
10.6.2 Security of network services	7.7.6.2 Security of network services	>	<p><b>Implementation guidance</b></p> <p>The impact of the loss of network service availability upon clinical practice must be considered carefully.</p>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
<b>10.7 Media handling</b>	<b>7.7.7 Media handling</b>		
10.7.1 Management of removable media	7.7.7.1 Management of removable computer media	>	<p><b><u>Implementation guidance</u></b> 7.7.7.1 (a-b) Information stored on removable media must be encrypted and protected from theft while the media is in transit.</p>
10.7.2 Disposal of media	7.7.7.2 Disposal of media	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>When no longer required for use personal health information SHALL be securely overwritten or else the media destroyed.</li> </ul> <p><b><u>Implementation guidance</u></b> This control should be applied prior to the repair or disposal of any associated equipment (including medical devices that record or report data).</p>
10.7.3 Information handling procedures	7.7.7.3 Information handling procedures	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Media containing personal health information SHALL be physically protected or have their data encrypted.</li> <li>In the event that media contain unencrypted personal health information, the status and location of such media shall be monitored.</li> </ul>
10.7.4 Security of system documentation	7.7.7.4 Security of system documentation	=	



<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
<b>10.8 Exchange of information</b>	<b>7.7.8 Exchange of information</b>		
10.8.1 Information exchange policies and procedures	7.7.8.1 Health information exchange policies and procedures and exchange agreements	>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>The use of the ISO 22857, which contains specific guidance on health information exchange policies, is recommended. It is further mentioned that while this standard deals with information flow between health jurisdictions, it can be adapted, where necessary, to deal with exchange of data from one organization to another.</li> <li>The application of the following implementation guidance statement is mandatory in healthcare: <b>Information exchange SHALL be the subject of policy development and compliance audit. SHALL</b></li> <li>Information exchange agreements must specify the minimum set of security controls to be implemented.</li> </ul>
10.8.2 Exchange agreements			=
10.8.3 Physical media in transit	7.7.8.2 Physical media in transit		
10.8.4 Electronic messaging	7.7.8.3 Electronic messaging	>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>It is cautioned that the security of electronic messaging may involve procedures for health personnel that cannot be imposed upon subjects of care and the public.</li> <li>Email between health professionals should be encrypted in transit. Reference is made to the <i>Bibliography</i> which lists standards related to the use of digital certificates.</li> <li>Attention is drawn to Section 7.12.2.2 of the standard discussing consent prior to communication outside the organization.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
10.8.5 Business information systems	7.7.8.4 Health information systems	=	
<b>10.9 Electronic commerce services</b>	<b>7.7.9 Electronic health information services</b>		
10.9.1 Electronic commerce	7.7.9.1 Electronic commerce and online transactions	>	<u>Implementation guidance</u> <ul style="list-style-type: none"> <li>Care must be taken to check data involved in electronic commerce and online transactions with reference to whether it contains personal health information.</li> <li>In healthcare, data related to billing, medical claims, invoice lines, requisitions, and other e-commerce data from which personal health information can be derived, is of special concern.</li> </ul>
10.9.2 On-line transactions			
10.9.3 Publicly available information	7.7.9.2 Publicly available health information	>	<u>Control</u> <ul style="list-style-type: none"> <li>Publicly available health information must be archived.</li> <li>The source (authorship) of this information must be known and its integrity must be protected.</li> </ul>
<b>10.10 Monitoring</b>	<b>7.7.10 Monitoring</b>		
	7.7.10.1 General	<b>NEW CTRL</b>	The security requirements relating to audit and logging are identified to be amongst the most important - ensuring accountability and providing an incentive to users to conform to acceptable use.
10.10.1 Audit logging	7.7.10.2 Audit logging	>	<u>Implementation guidance</u> <ul style="list-style-type: none"> <li>A secure audit record must be created each time a user accesses, creates, updates or archives personal health information via a health information system.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<ul style="list-style-type: none"> <li>• The audit log must uniquely identify the user, uniquely identify the data subject (i.e. the subject of care), identify the function performed by the user (record creation, access, update, etc.), and note the time and date at which the function was performed.</li> <li>• When data content is updated, a record of the content before modification, together with the associated audit record, must be retained.</li> <li>• Messaging systems must keep a log of message transmissions but excluding the message content.</li> <li>• The retention period for audit logs must be carefully considered with particular reference to clinical professional standards and legal obligations.</li> </ul>
10.10.2 Monitoring system use	7.7.10.3 Monitoring system use	>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>• A health information system must have an available audit logging facility at all times during the system's use.</li> <li>• Health information systems must have facilities which provide for the analysis of audit logs and allows: <ul style="list-style-type: none"> <li>○ the identification of all system users who have accessed or modified a given subject of care's record(s) over a given period of time; and</li> <li>○ the identification of all subjects of care whose records have been accessed or modified by a given system user over a given period of time.</li> </ul> </li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
10.10.3 Protection of log information	7.7.10.4 Protection of log information	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>• The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>• Audit records SHALL be secure and tamper-proof.</li> <li>• Logging facilities and log information SHALL be safeguarded to prevent misuse or compromise.</li> </ul> <p><b><u>Implementation guidance</u></b></p> <p>The importance of the evidentiary integrity of audit records is emphasized.</p> <p><i>Example</i></p> <p><i>In coroners' inquests, investigations into medical malpractice, and other judicial or quasi-judicial proceedings, actions and the timing of events are sometimes determined through an examination of changes and updates to an individual's personal health information.</i></p>
10.10.4 Administrator and operator logs	7.7.10.5 Administrator and operator logs	=	
10.10.5 Fault logging	7.7.10.6 Fault logging	=	
10.10.6 Clock synchronization	7.7.10.7 Clock synchronization	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>• The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>• Health information systems supporting time-critical-shared care activities SHALL provide time synchronization to support tracing and reconstitution of activity timelines.</li> </ul> <p><b><u>Implementation guidance</u></b></p> <p>The importance of time synchronization services in cases where it is essential to accurately determine a clinical sequence of events is emphasized.</p>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
11 ACCESS CONTROL	7.8 ACCESS CONTROL		
11.1 <i>Business requirement for access control</i>	7.8.1 <i>Requirements for access control in health</i>		
	7.8.1.1 General	NEW CTRL	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>7.8.1.1 (a-c) Users of health information systems should only access personal health information if there is a healthcare relationship between the user and the subject of care (data subject), when the user is carrying out an activity on behalf of the data subject and when there is a need for data to support this activity.</li> </ul>
	11.1.1 Access control policy	7.8.1.2 Access control policy	>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<p>in emergency situations, is expressed.</p> <ul style="list-style-type: none"> <li>The use of a federated identity and access management solution is recommended based on the benefits of such a solution (e.g. reduced administration costs and support for higher level security access processes such as smart-card-based access).</li> </ul>
<b>11.2 User access management</b>	<b>7.8.2 User access management</b>		
11.2.1 User registration	7.8.2.1 User registration	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>A formal user registration process SHALL be implemented which ensures consistency between the level of authentication required and the level(s) of access becoming available to the user.</li> <li>User registration details SHALL be reviewed periodically to ensure that they are complete, accurate and that access is still required.</li> </ul> <p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>7.8.2.1 (a-b) The accurate capture of a user's identity and verified enduring professional credentials (or job title), are required. <i>Example</i> <i>Dr Joan Smith, born March 26th 1982, currently resident at a specific address, cardiologist.</i></li> <li>7.8.2.1 (c) Assignment of an unambiguous user identifier is required.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<ul style="list-style-type: none"> <li>• Mention is made of the difference between typical system users and subjects of care. Subjects of care are be able to:               <ul style="list-style-type: none"> <li>○ access all or part of their personal data online (i.e. system users with limited access); or</li> <li>○ use health applications to seek general health advice and information (of which the transaction will be recorded but the user will remain anonymous).</li> </ul> </li> </ul>
11.2.2 Privilege management	7.8.2.2Privilege management	>	<p>Role-based, workgroup-based and discretionary access control strategies are explicated.</p> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>• Health information systems must support role-based access control.</li> <li>• The application of the following implementation guidance statement is mandatory in healthcare:  <b>A system user can only access its services in a designated single role. <span style="background-color: black; color: white; padding: 2px;">SHALL</span></b></li> <li>• Systems must associated users with the records of subjects of care and allow future access based on this association.</li> <li>• Reference is made to the ISO/TS 22600-1 and ISO/TS 22600-2 which provides additional guidance on privilege management in health.</li> </ul>
11.2.3 User password management	7.8.2.3User password management	=	

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
11.2.4 Review of user access rights	7.8.2.4 Review of user access rights	>	<b>Implementation guidance</b> Consideration must be given to users who may need to access information in emergency situations where a subject of care may not be able to give consent.
<b>11.3 User responsibilities</b>	<b>7.8.3 User responsibilities</b>		
11.3.1 Password use		>	<b>Implementation guidance</b> When determining user responsibilities, organizations must respect the rights and ethical responsibilities of health professionals, as agreed in law and as accepted by members of health professional bodies.
11.3.2 Unattended user equipment			
11.3.3 Clear desk and clear screen policy			
<b>11.4 Network access control</b>	<b>7.8.4 Network access control and operating system access control</b>		
11.4.1 Policy on use of network services		=	
11.4.2 User authentication for external connections			
11.4.3 Remote diagnostic and configuration port protection			
11.4.4 Equipment identification in networks			



<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
11.4.5 Segregation in networks			
11.4.6 Network connection control			
11.4.7 Network routing control			
<b>11.5 Operating system access control</b>			
11.5.1 Secure log-on procedures			
11.5.2 User identification and authentication			
11.5.3 Password management system			
11.5.4 Use of system utilities			
11.5.5 Session time-out			
11.5.6 Limitation of connection time			
<b>11.6 Application and information access control</b>	<b>7.8.5 Application and information access control</b>		

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
11.6.1 Information access restriction	7.8.5.1 Information access restriction	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Health systems SHALL authenticate users and should do so by means of authentication involving at least two factors.</li> </ul> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>Special consideration should be given to the technical measures by which a subject of care is securely authenticated when accessing all or part of his/her own information (where permitted).</li> <li>Ease of use of such measures is emphasized, especially for handicapped subjects of care and provisions for access by substitute decision makers.</li> </ul>
11.6.2 Sensitive system isolation	7.8.5.2 Sensitive system isolation	=	
<b>11.7 Mobile computing and teleworking</b>	<b>7.8.6 Mobile computing and teleworking</b>		
11.7.1 Mobile computing and communications	7.8.6.1 Mobile computing and communications	>	<p><b>Implementation guidance</b></p> <p>Organizations are required to specifically assess the risks involved in healthcare mobile computing, prepare policy covering the necessary precautions and require mobile users to follow this policy.</p>
11.7.2 Teleworking	7.8.6.2 Teleworking	>	<p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>Organizations must prepare policy on the precautions to be taken when teleworking and ensure that teleworking</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
			<p>users abide by this policy.</p> <ul style="list-style-type: none"> <li>The importance of considering ethical and legal aspects in the design and deployment of health information systems that can be used for teleworking is emphasized from the perspective that in healthcare, teleworking can cross jurisdictional borders.</li> </ul> <p><i>Example</i> Physicians already routinely e-mail medical images, etc. across boundaries to obtain specialist opinions.</p>
<b>12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE</b>	<b>7.9 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE</b>		
<b>12.1 Security requirements of information systems</b>	<b>7.9.1 Security requirements of information systems</b>		
12.1.1 Security requirements analysis and specification		=	
<b>12.2 Correct processing in applications</b>	<b>7.9.2 Correct processing in applications</b>		

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
	7.9.2.1 Uniquely identifying subjects of care	<b>NEW CTRL</b>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>7.9.2.1 (a-b) Health information systems SHALL ensure that subjects of care can be uniquely identified in the system and SHALL be capable of merging duplicate or multiple records if such records were created unintentionally or during a medical emergency.</li> </ul> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>Attention is drawn to the fact that multiple records can exist for a patient due to a valid reason. <i>Example</i> <i>Provision of emergency care where adequate identification of a patient is not possible.</i> Therefore the system must have the capacity to merge multiple patient records. However, such merging must be done with great care and will require trained personnel and proper technical tools.</li> <li>Data from which personal identification can be derived must only be retained when necessary to do so. The full extent of use of deletion, anonymization and pseudonymization techniques is recommended to minimize the risk of unintentional disclosures.</li> </ul>
12.2.1 Input data validation	7.9.2.2 Input data validation	=	
12.2.2 Control of internal processing	7.9.2.3 Control of internal processing	=	

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
12.2.3 Message integrity	7.9.2.4 Message integrity	=	
12.2.4 Output data validation	7.9.2.5 Output data validation	>	<p><b>Control</b></p> <ul style="list-style-type: none"> <li>The application of this security control is mandatory in healthcare. <b>SHALL</b></li> <li>Health information systems SHALL provide information to assist healthcare professionals to confirm that the identity of the subject of care matches the retrieved electronic health record.</li> </ul> <p><b>Implementation guidance</b></p> <ul style="list-style-type: none"> <li>The task of ensuring that the patient record matches the subject of care under treatment can be a non-trivial task. <i>Example</i> <i>Some systems enhance security by including photographic IDs with each subject of care's record. Such enhancements may themselves create privacy problems, as they potentially permit the implicit capture of facial characteristics such as race that are not included as fields of data.</i> Furthermore, the requirements for identification and the availability of data to support it may differ between jurisdictions. Therefore great care must be taken to ensure that systems can be trusted to provide the information needed to match the subject of care with the retrieved data.</li> <li>Health information systems should make it possible to check that hardcopy print-outs are complete. <i>Example</i> <i>“page 3 of 5”</i></li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
<b>12.3</b> <i>Cryptographic controls</i>	<b>7.9.3</b> <i>Cryptographic controls</i>		
12.3.1 Policy on use of cryptographic controls	7.9.3.1 Policy on the use of cryptographic controls and key management	>	<b><u>Implementation guidance</u></b> Reference is made to ISO 17090-3 which contains guidance on policy for the issuance and use of digital certificates in healthcare and on the management of keys.
12.3.2 Key Management	7.9.3.2 Key Management	=	
<b>12.4</b> <i>Security of system files</i>	<b>7.9.4</b> <i>Security of system files</i>		
12.4.1 Control of operational software	7.9.4.1 Control of operational software	=	
12.4.2 Protection of system test data	7.9.4.2 Protection of system test data	>	<b><u>Implementation guidance</u></b> Actual personal health information should not be used as test data.
12.4.3 Access control to program source code	7.9.4.3 Access control to program source code	=	
<b>12.5</b> <i>Security in development and support processes</i>	<b>7.9.5</b> <i>Security in development and support processes and technical vulnerability management</i>		
12.5.1 Change control procedures		=	

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
12.5.2 Technical review of applications after operating systems changes			
12.5.3 Restriction on changes to software packages			
12.5.4 Information leakages			
12.5.5 Outsourced software development			
<b>12.6 Technical Vulnerability Management</b>			
12.6.1 Control of technical vulnerabilities			
<b>13 INFORMATION SECURITY INCIDENT MANAGEMENT</b>	<b>7.10 INFORMATION SECURITY INCIDENT MANAGEMENT</b>		
<b>13.1 Reporting information security events and weaknesses</b>	<b>7.10.1 Reporting information security events and weaknesses</b>		

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
13.1.1 Reporting information security events		>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>• 7.10.1 (a-c) Motivates why security incident management responsibilities and procedures must be established.</li> <li>• Information security incidents are defined to include corruption or unintentional disclosure of personal health information or the loss of availability of health information systems, where such a loss adversely affects patient care or contributes to adverse clinical events.</li> <li>• Organizations must inform the subject of care whenever their personal health information has been unintentionally disclosed and when lack of availability of health information systems may have affected their care adversely.</li> <li>• All types of incidents must be treated as if they could have had an impact from an information security point of view (e.g. a break-in could have led to theft of PCs).</li> <li>• An information security assessment must be done on all such incidents to evaluate the efficacy of the existing controls and the initial risk assessment where the need for the controls was established.</li> </ul>
13.1.2 Reporting security weaknesses			
<b>13.2 Management of information security incidents and improvements</b>	<b>7.10.2 Management of incidents and improvements</b>		
13.2.1 Responsibilities and procedures	7.10.2.1 Responsibilities and procedures	=	



<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
13.2.2 Learning from information security incidents	7.10.2.2 Learning from incidents	=	
13.2.3 Collection of evidence	7.10.2.3 Collection of evidence	>	<b>Implementation guidance</b> Organizations may need to consider the implications of collecting evidence for purposes of establishing medical malpractice, and may also need to consider inter-jurisdictional requirements.
<b>14 BUSINESS CONTINUITY MANAGEMENT</b>	<b>7.11 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT</b>		
<b>14.1 Information security aspects of business continuity management</b>			<b>Implementation guidance</b>
14.1.1 Including information security in the business continuity management process		>	<ul style="list-style-type: none"> <li>• Due to the rigorous availability requirements in healthcare, a major investment in terms of technology as well as training staff ought to be made.</li> <li>• Business continuity planning must be suitably integrated with the organization's plans for handling power failures, implementing infection control and dealing with other clinical emergencies.</li> <li>• Business continuity management planning must include health crisis management planning, because major incidents typically lead to staff shortages which limit the ability to successfully effect continuity management plans.</li> </ul> <p><i>Example</i> <i>SARS outbreak</i></p>
14.1.2 Business continuity and risk assessment			
14.1.3 Developing and			

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
implementing continuity plans including information security			<ul style="list-style-type: none"> <li>In order to ensure low risk and improvement in user (staff) awareness, it is recommended that a “programmatic” approach be used to test plans. Tests should build upon one another proceeding from desktop testing to modular testing to synthesis of likely recovery times and then finally to full rehearsals.</li> </ul>
14.1.4 Business continuity planning framework			
14.1.5 Testing, maintaining and re-assessing business continuity plans			
<b>15 COMPLIANCE</b>	<b>7.12 COMPLIANCE</b>		
	7.12.1 General	<b>NEW MSC</b>	<p><b><u>Implementation guidance</u></b></p> <ul style="list-style-type: none"> <li>A compliance auditing programme that addresses the full cycle of operations must be put into place. Such a programme must not only identify problem areas but also review outcomes and decide on updates to the ISMS.</li> <li>A 12 month to 18 month cycle is suggested for health organizations’ audit programmes, during which time all elements of the Standard, all areas of risk and all implemented controls must be covered.</li> <li>It is recommended for the ISMF to establish a graduated compliance auditing framework with self-audit by the process operators and managers at the bottom layer and audits at subsequent layers (e.g. internal auditing, controls assurance assessments, etc.) drawing confidence from the layers below it.</li> </ul>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
<b>15.1 Compliance with legal requirements</b>	<b>7.12.2 Compliance with legal requirements</b>		
15.1.1 Identification of applicable legislation	7.12.2.1 Identification of applicable legislation, intellectual property rights and protection of organizational records	=	
15.1.2 Intellectual property rights (IPR)			
15.1.3 Protection of organizational records			
15.1.4 Data protection and privacy of personal information	7.12.2.2 Data protection and privacy of personal information	>	<p><b><u>Control</u></b></p> <ul style="list-style-type: none"> <li>• Informational consent from subjects of care must be managed.</li> <li>• Where possible, such consent must be obtained before personal health information is e-mailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.</li> </ul> <p><b><u>Implementation guidance</u></b></p> <p><i>Example (legal requirement to obtain consent)</i>  Council of Europe Recommendation, R (97)5 On the Protection of Medical Data, Council of Europe, Strasbourg, 12 February 1997</p> <p><i>Example (professional ethical guideline requiring consent)</i>  World Health Association's Declaration of Helsinki regarding medical research on human subjects</p>

<u>ISO 27002</u>	<u>ISO 27799</u>	<u>FLAG</u>	<u>ANALYSIS OF ADDITIONAL GUIDANCE PROVIDED IN ISO 27799</u>
15.1.5 Prevention of misuse of information processing facilities	7.12.2.3 Prevention of misuse of information-processing facilities and regulation of cryptographic controls	=	
15.1.6 Regulation of cryptographic controls			
<b>15.2 Compliance with security policies and standards, and technical compliance</b>	<b>7.12.3 Compliance with security policies and standards, and technical compliance</b>		
15.2.1 Compliance with security policies and standards		>	<b><u>Implementation guidance</u></b> Compliance for the purpose of technical interoperability is emphasized from the perspective of large-scale health information systems which typically consist of many interoperating systems.
15.2.2 Technical compliance checking			
<b>15.3 Information systems audit considerations</b>	<b>7.12.4 Information systems audit considerations in a health environment</b>		
15.3.1 Information systems audit controls		=	
15.3.2 Protection of information systems audit tools			

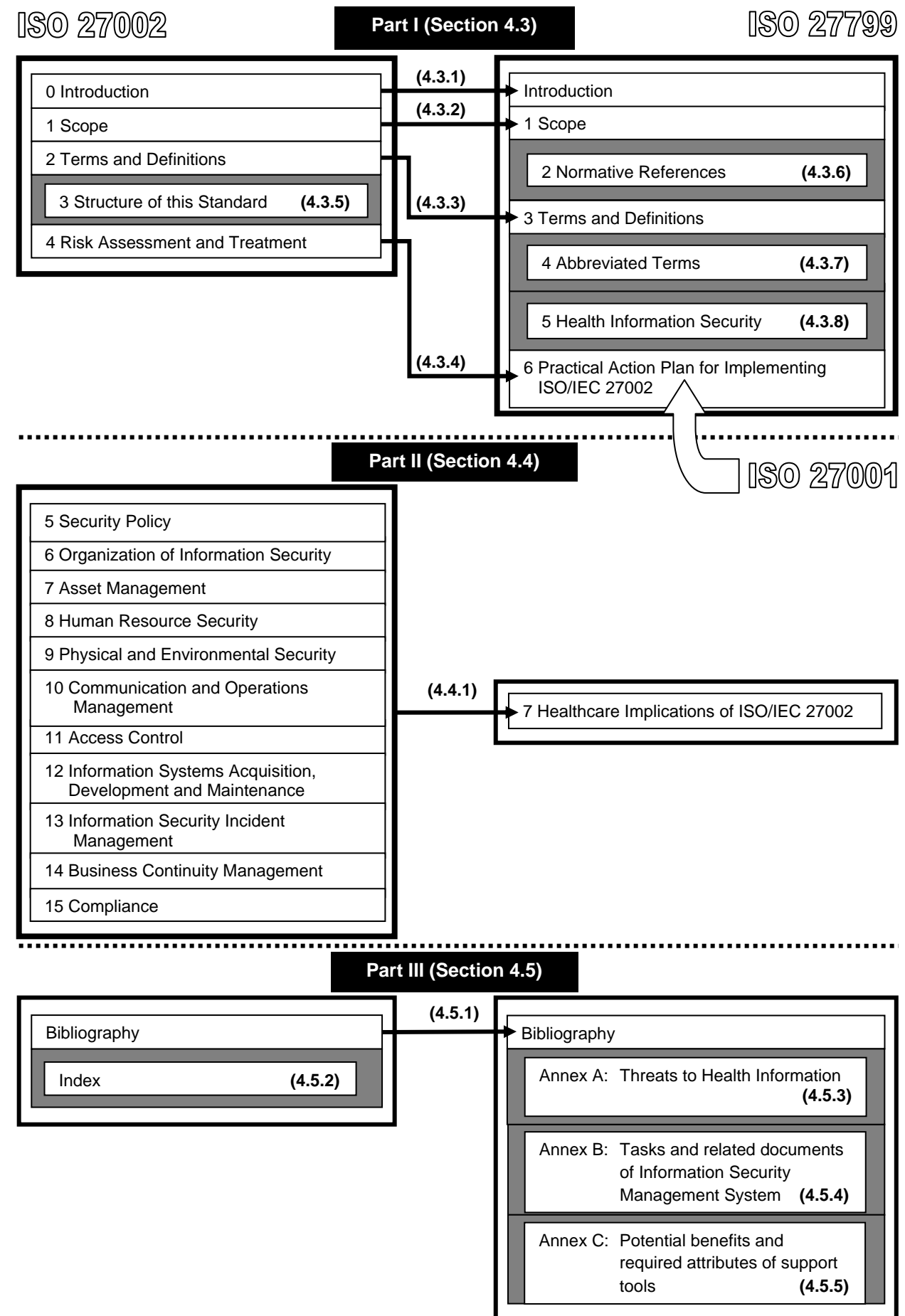


Figure 4.1 High Level Comparison of the ISO 27002 and ISO 27799 Standards