A MODEL FOR INFORMATON SECURITY MANAGEMENT

AND

REGULATORY COMPLIANCE

IN

THE SOUTH AFRICAN HEALTH SECTOR

TITE TUYIKEZE

A MODEL FOR INFORMATON SECURITY MANAGEMENT

AND

REGULATORY COMPLIANCE

IN

THE SOUTH AFRICAN HEALTH SECTOR

by

TITE TUYIKEZE

DISSERTATION

submitted in the fulfillment of the requirements for the degree

MAGISTER TECHNOLOGIAE

at the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

of the

NELSON MANDELA METROPOLITAN UNIVERSITY

SUPERVISOR: Dr. DALENCA POTTAS

December 2005

Dedication

My sincerest gratitude and appreciation are extended to:

- Our **Heavenly Father** who has created me;
- My Promoter, **Dr. Dalenca Pottas**, for all your advice, guidance and support... Without you, this research could not have been successful;
- In memory of my Parents, **Nyoni Dominique** and **Niragira Stéphanie**; your love, encouragement, support… will never be forgotten.

Pour vous tous, Que Dieu vous bénisse

Abstract

Information Security is becoming a part of the core business processes in every organization. Companies are faced with contradictory requirements to ensure open systems and accessible information while maintaining high protection standards. In addition, the contemporary management of Information Security requires a variety of approaches in different areas, ranging from technological to organizational issues and legislation. These approaches are often isolated while Security Management requires an integrated approach.

Information Technology promises many benefits to healthcare organizations. It helps to make accurate information more readily available to healthcare providers and workers, researchers and patients and advanced computing and communication technology can improve the quality and lower the costs of healthcare. However, the prospect of storing health information in an electronic form raises concerns about patient privacy and security.

Healthcare organizations are required to establish formal Information Security program, for example through the adoption of the ISO 17799 standard, to ensure an appropriate and consistent level of information security for computer-based patient records, both within individual healthcare organizations and throughout the entire healthcare delivery system. However, proper Information Security Management practices, alone, do not necessarily ensure regulatory compliance. South African healthcare organizations must comply with the South African National Health Act (SANHA) and the Electronic Communication Transaction Act (ECTA). It is necessary to consider compliance with the Health Insurance Portability and Accountability Act (HIPAA) to meet healthcare international industry standards.

The main purpose of this project is to propose a compliance strategy, which ensures full compliance with regulatory requirements and at the same time assures customers that international industry standards are being used. This is preceded by a comparative analysis of the requirements posed by the ISO 17799 standard and the HIPAA, SANHA and ECTA regulations.

Declaration

I, Tuyikeze Tite declare that:

- The work in this dissertation is my own work.
- All sources used or referred have been documented and recognized.
- This dissertation has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognized education institute.

_____

Tuyikeze Tite

12 January 2006

Table of Contents

List of Figures

List of Tables

List of Acronyms

CobiT	Control Objectives for Information and Related Technology
CEN	Comitté Européen de Normalization
CoE	Council for Europe
CPRI	Computer-based Patient Records Institute
DHHS	Department of Health and Human Services
ECTA	Electronic Communication and Transaction Act
GMITS	Guidelines for the Management of Information Technology Security
HIPAA	Health Insurance Portability and Accountability Act
HPCSA	Health Professions Council of South Africa
ISG	Information Security Governance
ISM	Information Security Management
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
ITGI	Information Technology Governance Institute
NRC	National Research Council
NIST	National Institute Standards and Technology
OECD	Organization for Economic Cooperation and Development
PAIA	Promotion of Access to Information Act
SALC	South African Law Commission
SANHA	South African National Health Act
SITA	State Information Technology Agency
UCP	Unified Compliance Project

Chapter 1 INTRODUCTION

The main purpose of **Chapter 1** is to present the problem statement, objectives and methodology of the research. Additionally, the relationship between corporate governance and information security is established. This chapter emphasizes that Executive Management and the Board of Directors are compelled to be committed and responsible for Information Security because it is required both by law and for good corporate governance within their organizations. It requires organization to have an effective Information Security compliance program ensuring the security and privacy of their customers' information.

In **Chapter 2** the reader is introduced to the general types of privacy and security concerns to emphasize that health information is a critical asset in a healthcare organization.

1.1 INTRODUCTION

In the current integrated, regulated and litigated environment, it is necessary to provide assurance to customers, business partners, regulators, and the courts that Executive Management have done due diligence in ensuring the security of their Information Technology (IT) infrastructure and their Information Systems (IS). This becomes more critical in the healthcare environment where health information is an extremely sensitive asset requiring an effective compliance program ensuring its privacy and security.

Information Technology facilitates the storage of large amounts of electronic health information and its dissemination to various healthcare business partners. In addition, IT enables the creation and analysis of large databases containing information from various sources. The absence of proper controls in the healthcare organizations can allow unauthorized users to access computer system and network resulting in the prevention of medical staff carrying out their duties and the sharing of the information of patients by unauthorized users (NRC, 1997). These concerns, inadequately addressed, can keep these organizations from investing in IT and result in patients loosing trust in their doctors (SALC, 2003).

There can be little doubt that information security, seen as the discipline to ensure the confidentiality, integrity and availability of electronic assets, is currently an extremely critical aspect in the strategic management of any organization. Von Solms (2005) argues that the data and information of the business have become its "life blood", and compromising this life blood, could kill the business. However, in many cases, Information Security is viewed only as a technical issue which is delegated to lower levers of IT and appears to lack the attention of top management and the Board of Directors (Entrust, 2004). Swindle & Corner (2004) suggest that Information Security needs to be considered as a corporate governance responsibility which should constitute risk management efforts, reporting and accountability on the part of the Executive leadership and Boards of Directors.

The IT Governance Institute (2001) defines **Corporate Governance** as the "set of responsibilities and practices exercised by the Board and Executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that enterprise's resources are used responsibly". However, attaining

the goal of this definition is not an easy task especially in the current dynamic business environment. The King Report (2001) clearly states that "Boards have to consider not only the regulatory aspect, but also industry and market standards, industry reputation, the investigative media, and the attitudes of customers, suppliers, consumers, employees, investors, communities (local, national and international), ethical pressure groups, public opinion, public confidence and political opinion, etc.." This could result as an endless list of activities related to the best way of directing and controlling the organization. This confirms that corporate governance is about sound leadership efforts (King Report, 2001). In order to achieve this sound leadership, the King Report (2001) emphasis that seven characteristics of good corporate governance must be in place. These are **Accountability**, **Discipline**, **Responsibility**, **Transparency**, **Independence**, **Fairness** and **Social responsibility**.

These seven characteristics will be briefly described in this section as extracted from the King Report (2001).

- **Accountability** is concerned with ensuring that decision makers and those who take actions on specific issues are accountable for their decisions and actions.

- **Responsibility** is concerned with those who fail to meet their duties or are involved in mismanagement face disciplinary action and penalties.

- **Discipline** requires commitment of senior management to follow behaviour that is universally accepted and deemed correct and proper.

- **Social responsibility** is the demonstration that an organization is aware and responds to ethical standards and human rights issues.

- The main concern of **Transparency** is ensuring that the organization reports an accurate organizational picture to the shareholders.

- **Independence** requires organization to install mechanisms which will avoid potential conflicts of interests such as the dominance by a large shareholder.

- **Fairness** relates to ensuring that the rights of various shareholders are acknowledged and respected regardless of the interest value contribution of the shareowner.

These characteristics provide a good primer for implementing an effective approach to corporate governance in any organization (Posthumus & von Solms, 2005). However, some organizations failed to effectively implement these characteristics of good corporate governance and corporate boards are now expected to comply with myriads of new laws or face harsh penalties such as lengthy jail time or financial penalties (Trillium Software, 2004).

There have been moves to make directors and senior executives personally accountable and responsible for the consequences of failures of internal control following the widely publicized failures of organizations such as the cases of Enron.corp, WolrdCom and other organizations which failed to meet corporate governance compliance (von Solms, 2001). Since internal control ultimately relies on Information Security, it follows that a well implemented Information Security program plays a key role in protecting the corporate managers. It becomes apparent that there is a need to elevate the importance of Information Security and integrate it into the overall corporate governance program (Corporate Governance Task Force, 2004) who further confirms that "the road to Information Security goes through corporate governance".

Information Security Governance is the term used to describe how Information Security is addressed as a part of the **Corporate Governance** responsibilities of an organization. Moulton & Coles (2003) defines Information Security Governance (ISG) as "the establishment and maintenance of the control environment to manage the risks relating to the *confidentiality*, *integrity* and *availability* of information and its supporting processes and systems". It becomes apparent, having this definition in mind that, Information Security is strategically important to any organization because it ensures that IT risks are kept to a minimum level and helps the organization to remain competitive while increasing their business value. It is necessary to first understand the relationship that links Information Security Governance and Corporate Governance to understand why the Information Security must be treated as a corporate governance issue.

1.1.1 The relationship between Information Security and Corporate Governance

Executive Management and the Board of Directors have started to realize that ISG is becoming their direct responsibility (von Solms, 2005) and that ignorance of ensuring Information Security can result in serious personal consequences,

specifically legally and the loss of the corporate reputation (Vericept Corporation, 2004). ISG describes the process addressing Information Security at an executive level. Corporate Governance Task Force (2004) states that ISG is considered to be a facet of the broader corporate governance strategy of the organization, which itself commences at the Board level (King Report, 2001).

The King Report (2001) on corporate governance helps to clarify why ISG should be addressed as corporate governance responsibility. It states that the Board is responsible and accountable to the shareholders of the company and must ensure that their organization produces business value and delivers a suitable return on shareholder investment. A good Information Security effort, according to Swindle and Corner (2004), is the key enabler to guarantee such return.

It can be summarized that ISG, which is a subset of organizations' corporate governance program deserves attention because it has become an important business responsibility and its accountability has escalated to the Board level. Von Solms (2001) further confirms that "ISG is a direct corporate governance responsibility and lies squarely on the shoulders of the Board of the company". Currently, the Board and Executive managers face abundant challenges to meet their corporate governance especially in this litigated business environment.

1.1.2 The Challenges of implementing Security standards and complying with Legislation

The ability to manage information risks is another critical requirement for business success in this technology-centric environment in which we currently work (Herold, 2001). An even more challenging environment, is created as the government regulates almost every aspect of running a business. These two issues combine to create substantial responsibilities on the part of business executives. This is especially noticeable in the healthcare environment.

There are various regulations which have an impact on IT. From the South African National Health Act (SANHA), Electronic Communication Transaction Act (ECTA), Traditional Health Bill in South Africa and Health Insurance Portability and Accountability Act (HIPAA) in the United States to various international privacy and security laws. What used to be a concern only for corporate legal counsel and network administrators has grown to be the focal point of executive and boardroom discussions (Herold, 2001).

The government is mandating what would otherwise be general IT best practices to force healthcare organizations to protect their customer information and prevent corporate misdeeds. These new government regulations have ushered in a new era for running healthcare transactions business. Healthcare Executives are now faced with many questions about how to effectively manage Information Security and stay out of legal trouble. General Information Security safeguards that are installed and revisited annually for the sake of compliance are not an effective way to manage these new regulatory challenges. Information Security controls implemented to meet the new regulation requirements can not solely provide the solution. Healthcare organizations are expected to have effective Information Security compliance programs in place and the task of implementing such compliance infrastructure is not simple especially with the increase of various **Security standards** and **Legislations** targeting the different stringent requirements.

South African healthcare organizations are required to establish a formal Information Security program to ensure an appropriate level of Information Security management, for example, through the adoption of an internationally recognized standard such as the ISO 17799 security standard. It is necessary to adopt the Healthcare Insurance Portability and Accountability Act (HIPAA) standards to overcome some of the criticisms of ISO 17799, such as being too general and not providing stringent solutions to specific requirements, as in the case of healthcare organizations.

The use of the ISO 22857 Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health information can ensure that the personal health information of patients is kept secure and private when personal health information is transferred internationally to other countries (ISO 22857, 2003). South African healthcare organizations, additionally, must ensure that they comply with the South African National Health Act (SANHA) and the Electronic Communication Transaction Act (ECTA) requirements to ensure due diligence practices. Ignorance of legal requirements is not an excuse but can result in heavy punishment and loss of credibility (Tuyikeze & Pottas, 2005).

This increase in government law requirements means Healthcare executive managers are now faced with many questions on how to effectively comply with these new regulatory requirements and simultaneously have in place security

mechanisms aimed at reducing security breaches of health information of the patients.

1.1.3 Privacy and Security concerns regarding Health Information

The security of medical Information Systems is a matter of great importance (Janczewski, 1998). It is easily imagined the significant consequences resulting from the implementation of corrupted medical information or publishing data about the health conditions of particular members of society.

Healthcare information systems provide many advantages when used for improved access, collaboration and data sharing among healthcare providers, patients, and researchers (Zhang et al, 2002). The main purpose of health information systems is to provide a fully-integrated electronic patient record. Briefly, it includes (CPRI toolkit, 1995):

- patients' histories
- families' histories
- results from specialties such as pathology, radiology, and endoscopies
- drug treatment
- procedures and problem lists.
- Additionally, it generates and stores plans for nursing care, clinical correspondence and dictated notes from ward rounds.

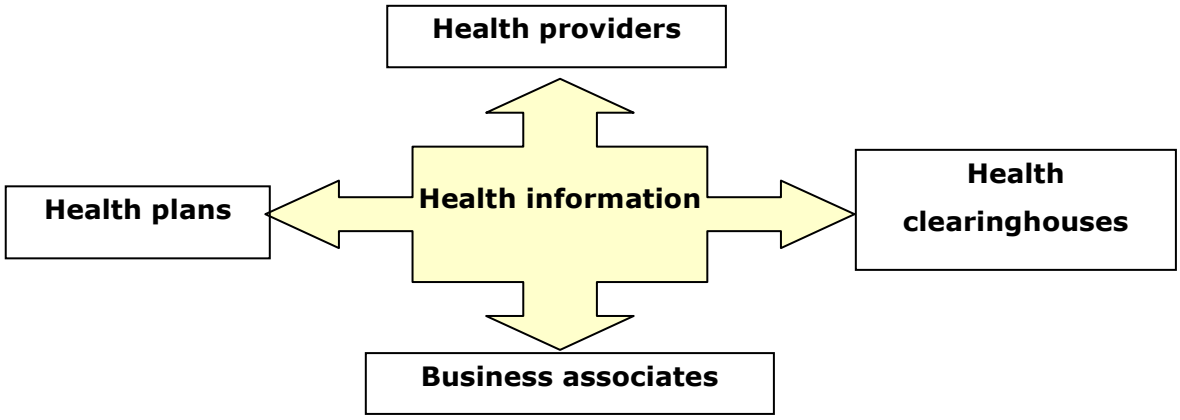
The use of electronic medical records presents an impeccable solution to providing effective medical services to patients and increased communication between healthcare business associates. However, the shift of medical records from paper to electronic formats has increased the potential for individuals to access, use, and disclose sensitive personal health data (CPRI toolkit, 1995).

Health information, as shown in Figure 1, is shared by various business partners to accomplish their tasks. These range (NRC, 1997) from:

- Health providers (provider of medical or health services such as physicians, hospitals, clinics, pharmacy)

- Health plans (health insurance issuer, medical aid, Medicaid)
- Health clearinghouses (entities that facilitate the processing of health information)
- Business associates (entities to whom the covered entity discloses protected health information enabling them to carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity eg., a transcription service).

Figure -1- Healthcare business associates



It is evident that Health information becomes vulnerable to multiple threats due to this increased number of people involved in healthcare business transaction. According to the National Research Council (1997), electronic medical records are potentially vulnerable to misuse from both authorized and unauthorized users who inappropriately access patient information for personal or economic gain. The highly personal and potentially destructive nature of the medical data creates significant concerns about its privacy and security. It becomes obvious that there is a need to implement safeguards aiming at ensuring its **Confidentiality**, **Integrity**, **Availability** and **Privacy** of health information. The question that arises is which security management approach should healthcare organizations follow, considering the myriads of security standards and guidelines that are currently available.

1.1.4 Protecting the Privacy and Security of health information

Many countries have adopted different regulation frameworks and security standards focusing on achieving data integrity, confidentiality and availability of health information due to the importance of security and privacy of such information. The following sections present an overview of these regulations and standards as related to the South African healthcare organizations environment.

1.1.4.1 Overview of ISO 17799, HIPAA, SANHA and ECTA

Healthcare executives are required to establish formal Information Security programs, for example, through the adoption of the ISO 17799 standard to guarantee to customers that healthcare organizations are doing their utmost to ensure the security of their health information. The benefits of this framework are to provide a code of practice that induces organizations to consider all factors when developing their security program. However, ISO/IEC 17799 recommends that it is used as a starting point for developing organization-specific guidance, with the particular emphasis that not all the guidance and controls in the code are applicable to all organizations. Conversely, additional controls not included in the code of practice document may be required (ISO 17799, 2000). Healthcare organizations may decide to deal with a subset of controls instead of considering the full list. Additionally, it is worthwhile to consider incorporating controls from other security standards dealing with specific organizational requirements, for example, the use of HIPAA standards by healthcare organizations.

The Healthcare Information Portability and Accountability Act (HIPAA) became law on August 21, 1996. The primary focus of HIPAA is to mandate that healthcare information becomes “portable” and “available” by legislating the use of uniform electronic transactions and other administrative measures (CMMS, 1996). The forcing of the healthcare industry to adopt uniform electronic transaction standards for healthcare information, necessitated its protection by including standards for how the information would be secured and safeguarded (CMMS, 1996). The portion of the HIPAA law that most impacts technology interests is the section on Administrative Simplification (Title II, Subtitle F). This section seeks to enforce uniform standards on the electronic interchange of health information (through the Transaction standard) and mandates guidelines for the security

(Security standard) and privacy (Privacy standard) of that information, whether in transit or stored.

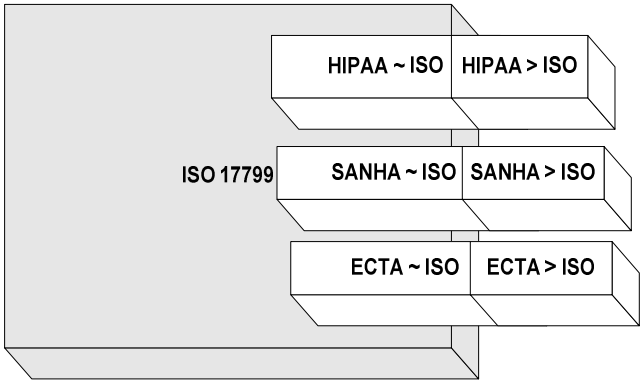
The utilization of best practices can serve as a manifestation of reasonable efforts by the healthcare organization to do the right thing. Nevertheless, it is important to highlight that proper Information Security Management practices alone do not necessarily ensure regulatory compliance and vice versa. South African healthcare organizations must comply with the South African National Health Act (SANHA) and the Electronic Communication Transaction Act (ECTA) to meet the legal requirements of the government.

The South Africa National Health Act (SANHA) or Act 61 of 2003 was signed into act by the South African president on 18 July 2004. SANHA provides a framework for a structured, uniform health system to unite the various elements of the national health system in a common goal to improve universal access to quality health services (SANHA, 2003). Chapter 2 "*Rights and duties of Users and Healthcare personnel*" is interesting as it contains a number of requirements aimed at protecting the privacy and security of health information.

The Electronic Communication and Transaction Act (ECTA), or Act No.25 of 2002 was signed into act by the South African president on 31 July 2002. It was the first South African law governing cyber activity. It facilitates the development and propagation of electronic communications and transactions within South Africa and aims to promote consumer confidence in electronic transacting and their online privacy (ECTA, 2003). The Act places a heavy burden on medical providers, insurers and claims clearinghouses, as well as other healthcare services partners who need to communicate electronically on a day-to-day basis to accomplish their tasks with the increased use of electronic communication transactions in healthcare business transactions.

There is little doubt that some sections of these government laws when examined more deeply address the security and privacy issues and therefore overlap sections of the Information Security Management framework, such as in the ISO 17799 security standard. This is illustrated in Figure 2. This can result in duplication of efforts and resources when Healthcare organizations are implementing new controls to comply with the new regulatory requirements.

Figure -2- Legislation and Security standards



LEGEND

~: For the topic of concern, the law and security standard requirements are the same.

>: For the topic of concern, the law includes a number of requirements not covered in the security standard.

Therefore, there is a need for implementing an Information Security compliance strategy aimed at eliminating efforts of implementing existing controls and duplicating security endeavors.

1.1.5 The importance for an Information Security compliance program

Kahn (2005) defines an Information Security compliance management as "an approach to Information Security program that is designed to help organizations manage information in a way that meets legal, regulatory, business and operational goals". The identification, implementation and management of the most effective set of controls are the first steps towards meeting the objective of this approach. The identification of most effective controls is always problematic and many approaches and techniques have developed to achieve this in the most objective way possible (von Solms, 1998). This is even more complex in the current changing IT environment with its legislation compliance requirements.

The major problem, currently, faced by Healthcare organization executives is how to effectively manage Information Security and stay out of legal trouble. This problem is solvable when there is a formalized approach intended to incorporate the new controls aimed at meeting the new regulatory requirements. A problem encountered when implementing these new controls is that Healthcare organizations duplicate controls with existing controls without knowing it. Therefore, this confirms that an Information Security Management compliance strategy, with the objective of combining regulatory and standards requirement,

would serve well to eradicate redundancy in following an ad hoc approach to compliance with various standards and legislations.

The compliance strategy will ensure that common elements across regulations and those already covered in an Information Security Management program will not be repeated unnecessarily. This will save on resources dedicated to meeting unnecessary requirements.

It is time for Healthcare organizations to move beyond fear, uncertainly and doubt where it relates to compliance. It is time for Healthcare organizations to begin architecting and implementing practical Information Management Compliance solutions. Healthcare organizations will meet their legal and regulatory requirements and realize significant business benefits by managing information according to its value, and by protecting the privacy, security of their information assets.

1.2 PROBLEM STATEMENT

There are a growing number of laws and security standards, currently, that require healthcare organizations to provide security controls and demonstrate compliance assurance. The problem addressed in this research is which compliance strategy should be followed to meet regulatory requirements while ensuring customers that best practices are being used.

Some of the associated problems are identified with this scenario in mind, by asking the following questions:

- If a healthcare organization has a well established Information Security Management framework such as ISO 17799, how much effort is required to meet the HIPAA standards?
- If a healthcare organization has a well established Information Security Management framework such as ISO 17799, how much effort is required to meet the National Health Act regulation requirements?
- If a healthcare organization has a well established Information Security Management framework such as ISO 17799, how much effort is required to meet the Electronic Communication Transaction Act regulation requirements?
- What compliance strategy should be followed to meet both legislative and the security standards requirements?

1.3 OBJECTIVES

The primary objective of this research project is to develop a model for Information Security Management and regulatory compliance program that will provide South African healthcare organizations with an approach towards Information Security Management, that ensures full compliance with governing regulations and at the same time provides customers with the assurance of meeting an international industry standard for health Information Security and privacy.

The following relevant sub-objectives will be addressed based on this primary objective:

- Identify a key set of standards and legislation pertaining to the South African health sector;
- Conduct a comparative assessment;
- Use the results of the comparative analysis to formulate a generic model for Information Security management and regulatory compliance.

1.4 METHOLOGY

The methodology will be of an investigative nature. An in depth literature study of the government laws (South Africa National Health Act 2004 and Electronic Communication Transaction Act 2002, HIPAA) and security standards (ISO 17799) will be done to highlight concerns pertaining to protecting the privacy and security of health information.

An investigative comparison between the South Africa National Health Act 2004, Electronic Communication Transaction Act 2002 and HIPAA Security, Privacy and Transaction and Code Set standards will be conducted to identify areas of convergence with the ISO 17799 security standard framework.

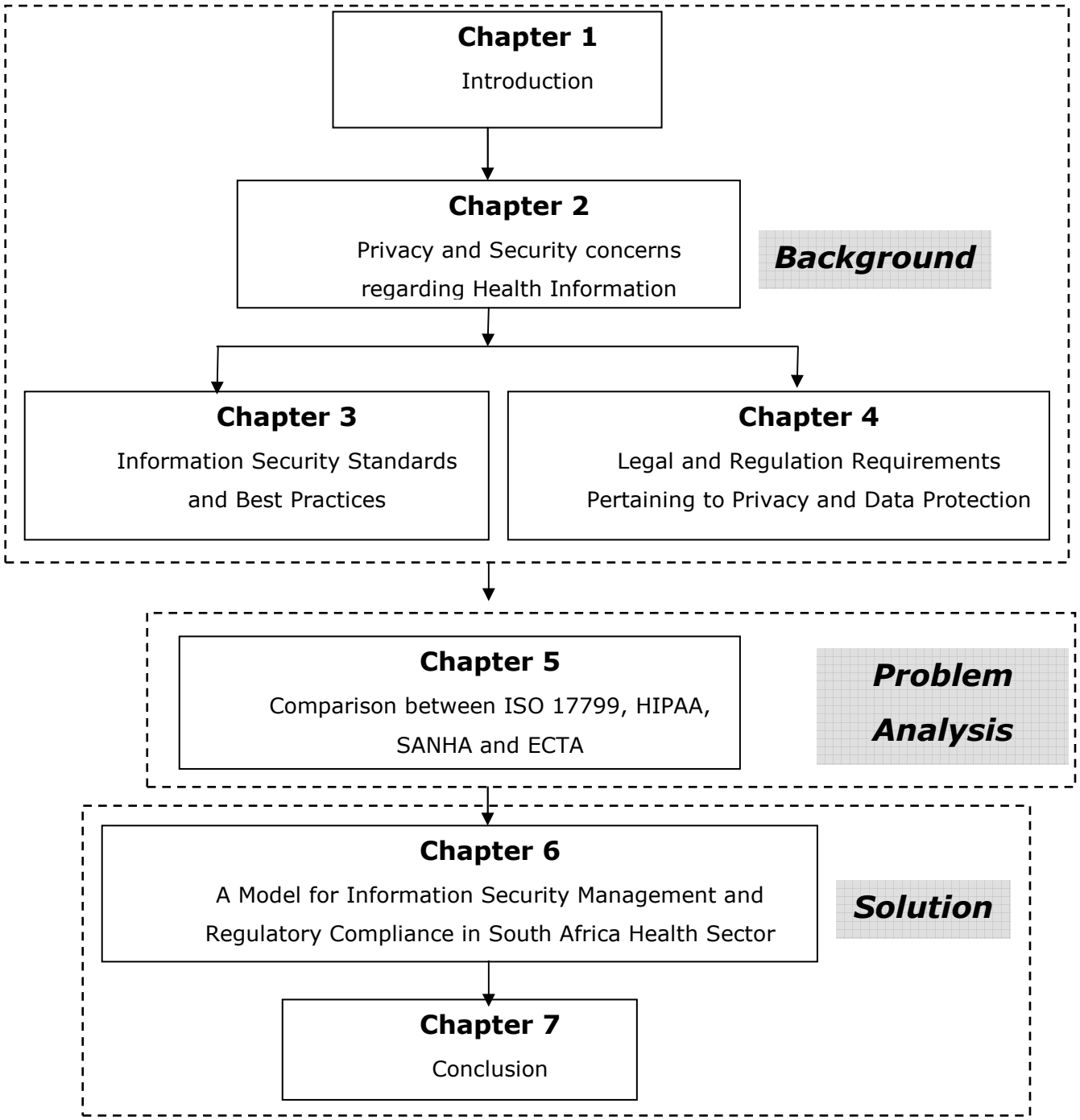
The information derived from the investigation of the comparative analysis, will be brought together to formulate a framework that will ensure regulatory compliance and at the same time ensure best practices are in use. This will help to reduce the security and privacy risks to a minimum level, while minimizing redundancy in the approach to complying with relevant legislations.

The results of this study will be reported in the form of academic projects and a dissertation.

1.5 LAYOUT OF THE DISSERTATION

The layout of the dissertation is depicted in Figure 3, and is divided into three parts: Background, Problem Analysis and Solution.

Figure -3- Layout of the dissertation



Chapter 1 highlights that senior management in the organization has started to realize that Information Security Governance is becoming their direct responsibility, and that serious personal consequences, specifically legal, could flow from ignoring Information Security. The challenges to ensuring good corporate governance are discussed. There is a necessity to create an Information Security compliance program. This chapter includes the problem statement and the methodology that will be used in the thesis.

Chapter 2 discusses the data flows within the healthcare industry and describes the general types of privacy and security concerns that must be addressed. These include the vulnerability and threats to data held by particular organizations and the privacy issues resulting from the widespread dissemination of data throughout the healthcare industry.

Chapter 3 describes the currently available Information Security standards and the best practices.

Chapter 4 describes the legal and regulation requirements pertaining to privacy and data protection.

Chapter 5 makes a comparison between the International standard ISO 17799 and HIPAA Security, Privacy, Transaction code sets standards, SANHA and ECTA. A comparison analysis between these laws and security standards is done to discover the convergence existing between them.

In **Chapter 6**, the result of the comparative analysis done in chapter 5 helps to provide a model for Information Security Management and regulatory compliance that meets both regulatory and security standards requirements.

Chapter 7 concludes by summarizing the concerns and the solutions provided in the thesis.

Chapter 2 PRIVACY AND SECURITY CONCERNS REGARDING HEALTH INFORMATION

The longstanding friction between patient privacy and access to information has been heightened by the transition to electronic health information and a push toward integrated information in support of healthcare delivery and health data networks (SALC, 2003). While these developments are intended to improve healthcare, they raise many questions about the role of privacy and security of health information.

The main objective of this chapter is to highlight that nowadays, there is a growing use of Information Technology (IT) within the healthcare industry to handle different sensitive healthcare transactions. Although, this provides numerous advantages, it may increase the inappropriate use of such critical information. This chapter provides an overview of the South African health Sector, to contextualize the discussion in terms of the focus of this research.

A discussion of some breaches of patient privacy and the resultant consequences will be provided. The chapter concludes by emphasizing the need for healthcare organizations to protect the privacy and security of medical information, which is the main focus of chapters three and four.

2.1 INTRODUCTION

The healthcare industry has continuously expanded from the single physician who treats a patient to multiple healthcare organizations that collect and analyze health information about patients (SALC, 2003). The confidentiality of health information is no longer a relationship solely between the healthcare provider and the patient (Oberholzer, 2001). Insurers, managed healthcare organizations, public health officials, researchers, and other parties with a legitimate need to access patient information must ensure they have protection mechanisms ensuring the privacy and security of such critical information.

Privacy and confidentiality have long been recognized as essential elements of the doctor-patient relationship (Klinck, 2000). It is essential for the medical profession (medical practitioners, dentists, psychiatrists and psychologists) to collate the health information of their patients into a complete medical record for the optimal care of the patient.

Each time a patient sees a doctor, is admitted to hospital, goes to a pharmacist or sends a claim to a health plan, a record is made of their confidential health information (HHS, 2001). This record is used for a wide variety of purpose including insurance functions, co-ordination of care, and research. Databases are established containing information about health and genetic materials enabling research on diseases and disorders with a genetic component. Generally cases, all these healthcare transactions are done without the knowledge of patient or consent for the use of his (her) health information (Sadan, 2001).

The South African healthcare organizations, like other health sectors worldwide, face the same challenges of ensuring the privacy and security of medical information.

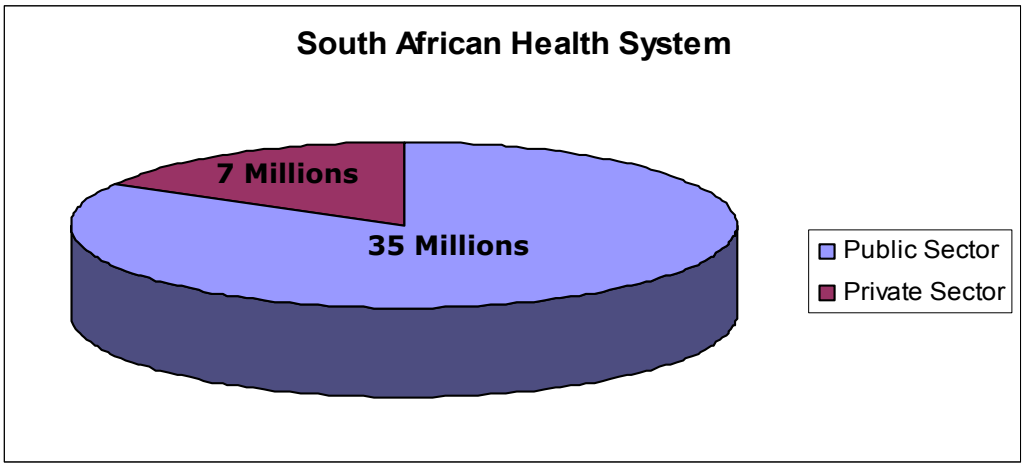
2.2 OVERVIEW OF SOUTH AFRICAN HEALTH SECTOR

Roemer (1991) states that "a health system is a combination of resources, organization, financing and administration that culminates in the health services offered to the population". The South African health system is composed of both public and private sectors with a significant difference between the two (Bassett, 2003).

Statistics obtained from safrica.info (2003) show that the public sector is under-resourced and over-used while the growing private sector, run largely along commercial lines, caters to middle- and high-income earners, who tend to be members of medical schemes (18% of the population), and to foreigners seeking top-quality surgical procedures at relatively affordable prices. The private sector attracts the majority of the health professionals.

The public health sector is under pressure to deliver services to about 80% of the population although the state contributes about 40% of all expenditure on health. However, most resources are concentrated in the private health sector, which maintains the health needs of the remaining 20% of the population. Figure 4 illustrates this disparity comprising both public and private sectors.

Figure -4- South African Health System



The South African government has realized that the use of IT in handling medical records is a necessity not a choice (safrica.info, 2003), considering the increasing number of people in both sectors (35 million in the public sector and seven million in the private sector).

The South African government depends on the State Information Technology Agency (SITA), which was established in 1999 with the objective of consolidating and coordinating its Information Technology. The objectives of the act, as stated in the SITA Act 38 of 2002 section 6 are (SITA Section 6, 2002):

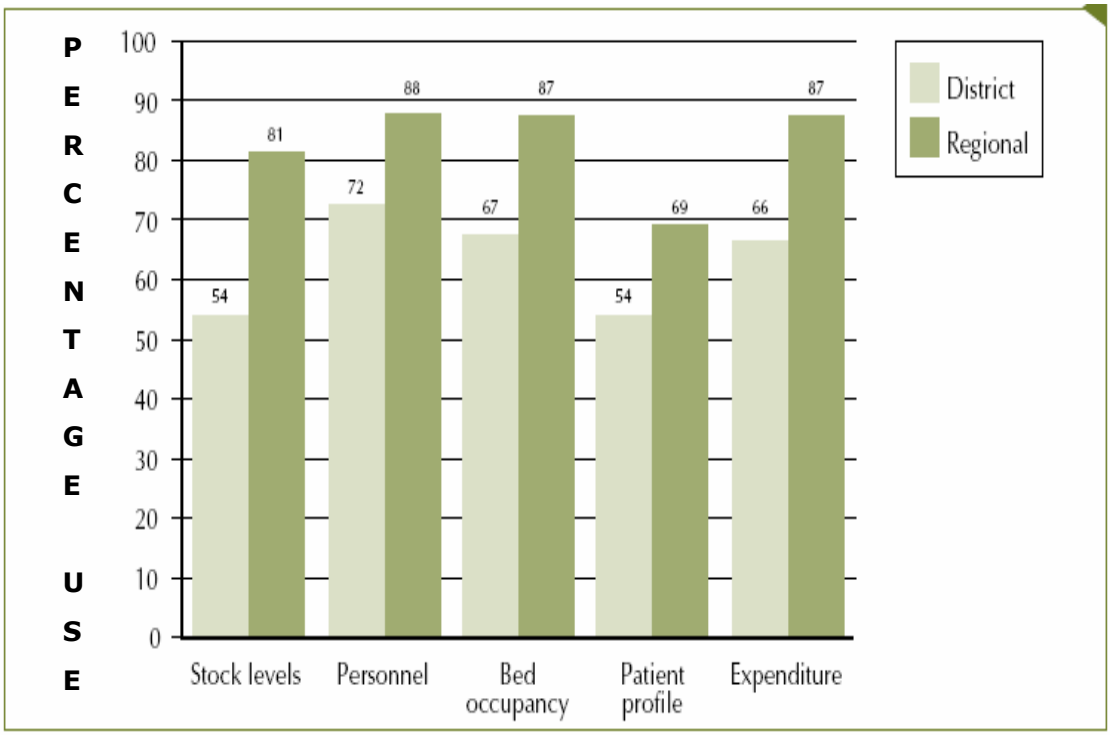
- "To improve service delivery to the public through the provision of information technology, information systems and related services in a maintained information systems security environment to departments and public bodies.

- To promote the efficiency of departments and public bodies through the use of information technology".

The South African health system faces many challenges related to staff shortages, deteriorating infrastructure, increased centralization, equipment failures and shortages, and an increased influx of (especially HIV/AIDS) patients. The public and private healthcare sectors are, however, showing confidence in the ability of IT to transform the industry and improve healthcare services (EthicSA, 2000).

The SA Health Review committee, in 1998, conducted a survey to discover which hospitals collect and utilize health information; respondents were asked whether they had Health Information Systems (HIS) in place, what format they used and whether information was collected within specific categories. Figure 5 provides the results found.

Figure -5- Percentage of hospitals which collect key categories of information, District/Regional



Source: South African Health Review 1998 Technical Report (Chapter 14)

As shown in Figure 5, the results suggest that regional hospitals collect more information of each type compared with district hospitals (although the differences were not statistically significant). It is seen that in both district and

regional hospitals, there is a relatively high use of IT in handling medical transactions compared to traditional paper work.

At a Health Informatics Association for Africa conference held in Johannesburg, delegates agreed that it was more prudent to increase investment in IT than in medical technology (Powe, 2003). "IT in healthcare is growing in popularity because of its ability to provide the medical industry with the information it needs to make informed decisions" (Powe, 2003).

It is crucial to initially examine the content and advantages associated with medical information to underline the need for ensuring data privacy and security of health information.

2.2.1 Contents of electronic health records

Originally, the health record existed in an abbreviated form to remind the medical personnel, who may have known for sometime about the familiar risk of the patient factors and their history of diseases or conditions. Care is now provided by a variety of locations and the bills are settled by multiple payers, and the health record is used to facilitate familiarity with the following patient criteria: status, document care, plan for discharge, document the need for care, assess the quality of care, determine reimbursement rates, justify reimbursement claims, pursue clinical or epidemiological research, and measure outcomes of the care process (NRC, 1997).

Currently, the content of electronic health records represents an attempt to translate the information from paper records into an electronic computerized format. Over time, it is anticipated that the content will significantly expand beyond that of paper records and potentially include on-line imagery (e.g., x-rays) and video such as telemedicine sessions (NRC, 1997).

The medical information contains the following according to Zhang et al (2002):

- Identifiable individual information: address, name, contact details…;
- Health information: patients' histories, family histories, risk factors, findings from physical examinations, vital signs, test results, known allergies, immunizations, health problems, therapeutic procedures and medications, and responses to therapy. They include the assessment from the provider and plans, advance directives, information on the assent and understanding of

therapy by the patient, and permission for disclosure of information for use by other care providers or bill payers.

The concerns about health information are growing as health information contains sensitive information such as HIV status, genetic information and psychiatric records. All this information combined provide the "life blood" of any healthcare organization. Ensuring the protection of such critical information results in numerous advantages on the part of the healthcare organization and also to its customers.

2.2.2 Advantages of electronic health records

Briggs (2000) defines an electronic health record as an electronic longitudinal collection of personal health information, usually based on the individual, entered or accepted by healthcare providers which can be distributed over a number of sites or aggregated at a particular source. The information is organized primarily to support continuing, efficient and quality health care. The record is under the control of the consumer and is to be stored and transmitted securely. Having this definition in mind, it is unquestionable, using this definition, that the electronic health record offers many potential advantages over the traditional paper-based records. These will be discussed briefly.

A. Improved access to health information: the primary benefit of using health records is access for authorized and authenticated users (NRC, 1997). Health information allows providers to access health information from a variety of locations and to share that information more easily with other potential users. Multiple users may access the information simultaneously.

B. Accuracy of personal health records can be improved: The use of medical information, allows information from a variety of healthcare providers to be collected and stored in a single record, providing a more complete and more accurate record of the personal health history of an individual. It can reduce the number of redundant queries and diagnostic tests and improve the availability of health-related information at the point–of-care delivery when used to increase communication among providers (Romanow Report & Informatics, 2002).

C. **Efficiency can be improved**: The use of electronic medical information can reduce the amount of time compared to that spent in managing medical paper work. Increased access, better logical organization, and greater legibility are reason enough to justify the move toward electronic medical information. Electronic data can be used to accomplish tasks that were impossible in the paper format even if access were not a problem. For example, data stored in electronic records can be organized and displayed in a variety of different ways that are tailored to particular clinical needs.

D. **Effectiveness can be improved**: Electronic health records hold the promise of improving clinical research. Currently, information about the effectiveness of tests or treatments, if stored, lies buried deep in paper files that cannot be analyzed economically. The search and retrieval capabilities of computerized record systems, in conjunction with automated analysis tools, enable faster and more accurate analysis of data (NRC, 1997). It improves the ability of the physician to access the latest information, select the best course of action and use evidence to guide their decisions (Romanow Report & Informatics, 2002).

Health information, additionally allows all instances of access to be recorded in audit logs maintaining a record of who accessed what information, when and about which patients. This is often impossible in a paper-based medical information situation. Paper records, according to the Romanow Report & Informatics (2002), are increasingly becoming obsolete and inadequate.

- They limit the flow of information;
- insufficiently document patient care;
- impede the integration of healthcare delivery
- create barriers to research, and limit the information available for administration and decision making.

It is obvious that the application of IT health environment provides numerous advantages comparing to paper records, and therefore prove the need that such critical information should be properly protected.

2.3 NEED OF DATA PRIVACY AND SECURITY OF HEALTH INFORMATION

Executive managers occasionally are in error when they believe that adopting security best practices to ensure **security** of information will equally ensure **privacy** protection. The two are related but pose separate challenges (KPMG, 2001). It is possible to secure health information without making it private; however, it is not possible to protect privacy without having security (KPMG, 2001). These two concepts must be considered as satisfying one does not mean the satisfaction of the other. Medical staff members must first understand clearly what is meant by these terms to show appropriate respect for patient privacy and security.

2.3.1 Security of health information

The security of medical information is a matter of great importance. The significant consequences resulting from the implementation of corrupted medical information or publishing private data about health condition information can be easily imagined. ISO 7799 states that Information Security can only be achieved if the organization has ensured that three key characteristics namely: **Confidentiality**, **Integrity** and the **Availability** of information are preserved.

2.3.1.1 Confidentiality

Humphreys et al (1998) states that confidentiality involves "protecting sensitive information from unauthorized disclosure or intelligible interception". An organization must make sure that this information is kept secret. In healthcare interactions, patients communicate sensitive personal information to the caregivers assuring they understand the medical conditions and treat them appropriately. Such information is termed confidential and it is necessary that those receiving it have a duty to protect it from disclosure to others who have no right to the information. Caregivers can breach confidentiality intentionally by directly disclosing patient information to an authorized person or inadvertently by discussing patient information in a way that an unauthorized person can overhear it.

2.3.1.2 Integrity

The ensuring of the integrity of information resources involves maintaining the correctness and comprehensiveness of that information (Humphreys et al., 1998). Information integrity plays an important role, particularly in a healthcare environment because it guides medical staff members in the decision making process. If such health information is not accurate or complete, this can result in unwanted situations which may even lead to death or cases of individuals being treated with inefficient medications. Systems that store, process or transmit electronic medical information must ensure that unauthorized modification to the information cannot be made without being detected. Any time information is used or electronically communicated; there needs to be a high confidence that such information is accurate (NEMA, 2001). Authorized modifications to health records must be tracked and mechanisms installed to protect the integrity of information while stored, processed or transmitted to other business healthcare partners.

2.3.1.3 Availability

An organization must guarantee that its information resources are accessible for use, by the relevant parties at the time needed to preserve the availability of health information. Gerber & von Solms (2001) state that ensuring the availability of information is crucial because without timely information, an organization would incapable of continuing normal operations. NEMA (2001) suggests that organization must have in place mechanisms and procedures to ensure that health information is continuously available even in the light of predictable equipment faults or power outages. Organizations need to plan against disasters to achieve this. These plans against disaster recovery can vary from simple backup tapes, to the use of very comprehensive processes which might include off-site support and backup systems (NEMA, 2001).

The preservation of the confidentiality, integrity and availability of health information demonstrates that the healthcare organization is trying all means possible to keep the risks at the minimum level. This ensures that the information retains its value to the organization and to its relevant stakeholders. However, Executive managers must realize that ensuring security does not guarantee privacy and vice-versa (KPMG, 2001).

2.3.2 Privacy of Health Information

Several definitions of the term **Privacy** are found in the literature. They vary based on the context in which the term is used. In its broadest sense, privacy refers to the right of a person to keep anything about himself (herself) private to himself (herself) and not to reveal it to anyone else (SALC, 2003). Dobson et.al (1995) defines it as "the right of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others". Privacy is often characterized as freedom from exposure to or intrusion by others. Allen (1995) distinguishes three major usages of the term privacy: "**Physical privacy**"," **Information privacy**", "**Decisional privacy**". These are defined as follows:

Physical privacy refers to freedom from contact with others or exposure of the physical body to others. Physical privacy is unavoidably limited in contemporary health care. Patients grant their caregivers access to their bodies for medical examination and treatment, but expect caregivers to protect them from any unnecessary or embarrassing bodily contact or exposure.

Information privacy refers to the prevention of disclosure of personal information. Information privacy is limited in healthcare by the need to communicate information about particular conditions and medical history to other caregivers of the patients. In disclosing this information, however, patients expect that access to it will be carefully restricted. It is this type of information privacy that will be referred in this project.

Decisional privacy refers to an ability to make and act on the personal choices of the individual without interference from others or the state.

Several issues are involved in considering privacy. Clearly, health information should be kept private. It should be used for approved purposes and shared only among authorized people. However, privacy is equally about individuals knowing why information is collected about them, who has access to it, how it will be used and by whom.

South African Law Commission (2003) argue that the concepts of privacy and security are closely related that they are often confusing. It is pertinent to look at the relationship that exists between them.

2.3.3 Relationship between Privacy and Security of Medical Information

Security and Privacy are two terms related but not interchangeable (EPIC Report, 2002). This distinction is obvious especially in the healthcare environment where the privacy of health information is of the utmost to any organization and its protection deserves a high priority. The relationship between privacy and security can be clarified by looking at different views from various authors:

Luck (2000) states that the concepts of security and privacy in health information systems are distinct but inextricably linked, like Siamese twins. The distinction can be simply expressed as follows, "security is the protection of computers from people, and privacy is the protection of people from computers" (Luck, 2000). Electronic Privacy Information Center (EPIC) Report (2002) further confirms that security and privacy are distinct but related: "Privacy is the right of an individual to control the circumstances in which their personal information is used, disclosed or collected. It should not be divulged or used by others against his/her wishes. Security on the other hand refers to all the ability to control access and protect information from accidental disclosure to unauthorized persons and from alteration, destruction or loss".

Dobson et al (1995) distinguishes between Security and Privacy in terms of **formal logic**. They state that infrastructural definitions such as security can be the subject of mechanical interpretation whereas structural definitions such as privacy remain in the domain of policy and legislation. Security can be defined as who is supposed to know what or who has access to what. Mechanisms to implement security can be made part of the social or technical infrastructure underlying the institution.

In conclusion on the distinction between Privacy and Security, it is apparent that Privacy and Security are two terms related but with different concepts. They are not interchangeable in the sense that the satisfaction of one does not mean that the other one is ensured. This proves that there is a necessity for a mechanism ensuring both the protection of Privacy and Security which constitutes the heart of this project.

These will be discussed comprehensively, especially in Chapter 6, which provides a compliance model combining both security controls and regulatory requirements ensuring the protection of Security and Privacy of health information.

Although, the protection of security and privacy provides numerous advantages to any healthcare organization, the original source of information must be protected to ensure the healthcare organizations are collecting correct information. It can be impossible to gather accurate information from patients who are uncertain if their information will be kept private without a strong trust between patients and medical staff.

2.3.4 Privacy is necessary to secure effective and high quality health care

Privacy is one of the key values on which our society is built but, it is more than an end in itself. It is necessary for the effective delivery of healthcare, both to individuals and populations (DHHS, 2000). The entire healthcare system is built upon the willingness of individuals to share the most intimate details of their lives with their healthcare providers. The absence of a strong trust between the patient and medical staff can result in disparities of having accurate patient information and a lack of high-quality health care.

The need for privacy of health information, in particular, has long been recognized as critical to the delivery of needed medical care (DHHS, 2000). The relationship between patient and clinician is based on trust. The clinician must trust the patient to give full and truthful information about their health, symptoms, and medical history. The patient must trust the clinician to use that information to improve his or her health and respect the need to keep such information private. Patients must provide healthcare professionals with accurate, detailed information about their personal health, behavior, and other aspects of their lives to receive accurate and reliable diagnosis and treatment. However, this is not easy to accomplish in some cases where such information is embarrassing and patients have a strong desire to keep it confidential. Such sensitive conditions include sexual assault, family violence, sexually transmitted diseases, unwanted pregnancy, suicide attempts, acute psychoses, drug overdoses and disfiguring trauma, to name but a few.

The provision of health information assists in the diagnosis of an illness or condition, in the development of a treatment plan, and in the evaluation of the effectiveness of that treatment. The absence of full and accurate information can mean a serious risk that the treatment plan will be inappropriate to the medical situation (DHHS, 2000). Patients benefit from the disclosure of this information to the health plans that fund and can help them gain access to needed care. Health plans and healthcare clearinghouses rely on the provision of this information to accurately and promptly process claims for payment and for other administrative functions that directly affect the ability of the patient to receive needed care, the quality of that care, and the efficiency with which it is delivered.

Individuals cannot be expected to share the most intimate details of their lives unless they have confidence that such information will not be used or shared inappropriately.

2.4 CONCERNS REGARDING PRIVACY AND SECURITY OF MEDICAL INFORMATION

Patients reveal highly sensitive information to healthcare professionals. The inappropriate use of this information could have seriously adverse consequences for the individual. A prime example of the inappropriate use of health records is provided by a 1996 study that was conducted in United States of America. This study documented 206 cases of discrimination as a result of access to genetic information that resulted in a loss of employment and insurance cover or eligibility for benefits (Briggs, 2000).

People provide information in one context and they often do not realize that this information is ultimately used for other purposes such as marketing and research and mostly without the patients consent (Sadan, 2000). This results in more concerns by the patients about the loss of privacy of their information.

2.4.1 Increasing public concern about loss of privacy

Today, it is virtually impossible for any person to be truly "left alone". Individuals are overwhelmed with requests for information from potential employees, retail shops, telephone marketing firms, electronic marketers, banks, insurance companies, hospitals, physicians, health plans and others. The greatest concern

from consumers is how this information will be kept by healthcare organizations and that it will not be used to harm them in the future.

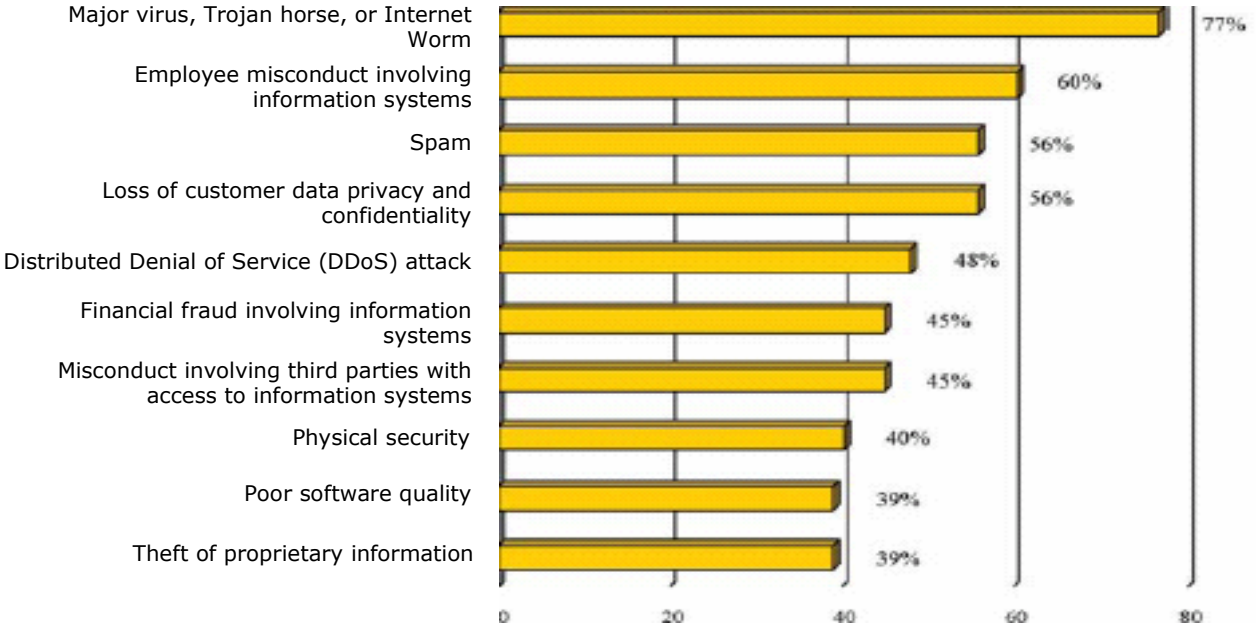
In a 1998 national survey done in America, 88 percent of consumers said they were "concerned" by the amount of information being requested, including 55 percent who said they were "very concerned". These worries are not theoretical because the personal information provided to these organizations is sold to other companies after promising to consumers not to do so (DHHS, 2000).

In 1993, a poll conducted by Lou Harris found that 75 percent of those surveyed worried that medical information from a computerized national health information system will be used for many non-health reasons, 38 percent are very concerned about the use of their information, 85 percent of respondents believed that protecting the confidentiality of medical records is "absolutely essential or very essential" in healthcare reform (Harris & Associates, 1995).

A Wall street Journal/ABC poll on September 16, 1999 asked Americans what concerned them most in the coming century. Loss of personal privacy was the first choice of 29 percent of respondents. All other issues, such as terrorism, world war and global warming had scores of 23 percent or less. However, pertaining to concerns about terrorism, this result may have been quite different if the same poll were taken after the events of September 11th, 2001.

Ernst & Young (2004) conducted a Global Information Security survey to examine the various dimensions of Information Security as practiced by global organizations. The question was posed: "What do the organizations perceive as their most pressing threats and how rationally are they addressing them?" Their top ten security concerns illustrated that loss of customer data privacy and confidentiality were among the first three that organizations perceive as their most threats. The result of this survey is shown in Figure 6.

Figure -6- Threat Matrix: Top Security Concerns



Source: Global Information Security Survey, 2004 (ERNST & YOUNG)

The concerns of the privacy and security of health information can be summarized into two categories according to the National Research Council (1997):

1. **Concerns about inappropriate release of health information within individual organizations:**

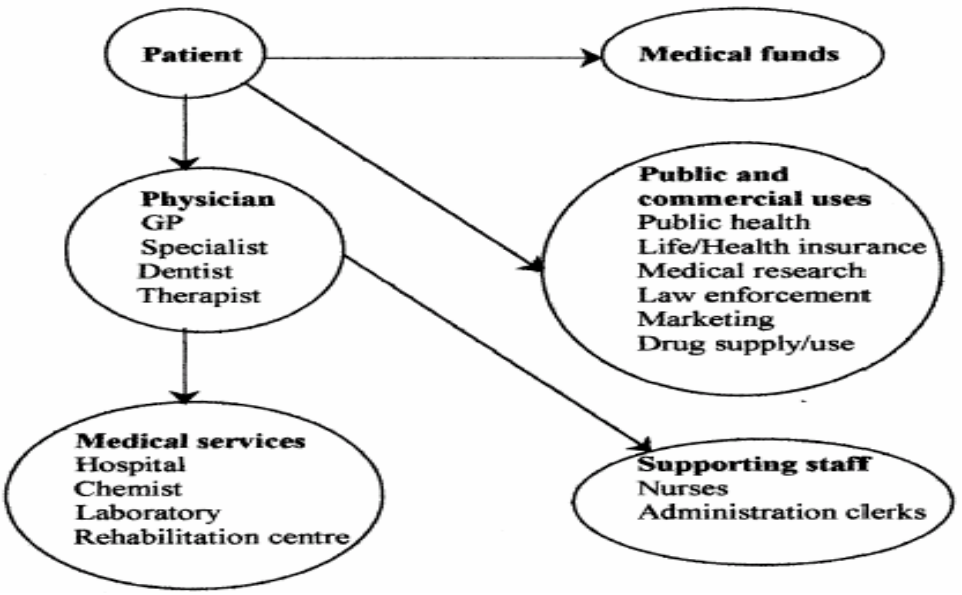
   This can result either from authorized users who intentionally or unintentionally access or disseminate health information for their personal or economic gain. Authorized users may take advantage of their legitimate authority to access information for which they have no valid need (often regarding a friend, relative, or celebrity), or they may reveal patient information to others often without the consent of the patient. Outside attackers may break into computerized information to steal, destroy, or render the system dysfunctional, preventing legitimate users such as doctors and nurses from accessing information critical to care.

2. **Concerns about the systemic flows of information through the healthcare and related industries.**

   This category involves systemic concerns which refer to the open disclosure of patient health information to parties who may act against the interests of the specific patient or may otherwise is perceived as invading their privacy. These

concerns arise from the many flows of data across the healthcare system, between and among providers, payers, and secondary users, with or without the knowledge of patient. Figure 7 shows for example a data flow for health information system related to South Africa healthcare environment.

Figure -7- The sharing of healthcare information



Source: Smith & Eloff, 1999

It becomes unarguable, as shown in Figure 7, that health information is being used by many parties for different purposes and this can result in an abundance of vulnerabilities and various threats. The following section provides a brief description of each of the different levels of threats that are the original sources of privacy and security breaches.

2.4.2 Major threats to information in healthcare organizations

Healthcare organizations are being endangered by different forms of threats, from employees who access data even though they have no legitimate access need, to outside attackers who infiltrate the IS of the healthcare organization to steal data or destroy the system. The following describes the major threats to medical information (NRC, 1997):

A. Insiders who make "innocent" mistakes and cause accidental disclosures

Accidental disclosure of personal information is probably the most common source of breached privacy that happens in myriad ways, such as overheard conversations between health care providers in the corridor or elevator, a laboratory technician noticing test results for an acquaintance among tests being processed, information left on the screen of a computer in a nursing station so that a passer-by can see it, misaddressed e-mail or fax messages, or misfiled and misclassified data.

B. Insiders who abuse their record access privileges

Examples of this threat include individuals who have authorized access to health data (whether through on-site or off-site facilities) and who violate this trust. Healthcare workers are subject to curiosity in accessing information they have neither the need nor the access right. This includes accessing information about the health of fellow employees or family members out of concern for their well-being. Healthcare workers, who access medical information to determine the possibility of sexually transmitted diseases in colleagues with whom they were having relationships. They are interested in potentially embarrassing health information (e.g., psychiatric care episodes, substance abuse, physical abuse, abortions, HIV status, and sexually transmitted diseases) about politicians, entertainers, sports figures and other prominent people which regularly finds its way into the media.

C. Insiders who knowingly access information for spite or for profit

This type of threat arises when an attacker has authorization to some part of the system but not to the desired data and through technical or other means gains unauthorized access. An example is a billing clerk who exploits a system vulnerability to obtain access to data on the medical condition of a patient. For example, the London Sunday Times reported in November 1995 that the contents of any individual's electronic health record in Great Britain could be purchased on the street for about £150, approximately R1500.00 of the current exchange rate.

D. The unauthorized physical intruder

The attacker, in this case, has physical entry to points of data access but does not possess authorization for system use or the desired data. An example of this threat is an individual who puts on a lab coat and a fake badge, walks into a facility and starts using a workstation or asking employees for health information.

E. Vengeful employees and outsiders, such as vindictive patients or intruders, who mount attacks to access unauthorized information, damage systems, and disrupt operations.

This is a very dangerous threat because the attacker has no authorization and no physical access which makes it difficult to mitigate the risks associated with this particular threat. An example is the intruder who breaks into a system from an external network and extracts patient records. It is evident that most providers are moving towards the use of networking and distributed computing technologies as they move toward electronic medical records. Therefore, this threat is a latent problem on the horizon.

Most of these threats constitute the original cause of the increase in patient privacy breaches.

2.5 BREACHES OF PATIENT PRIVACY

The growing amount of patient privacy breaches stem from several trends, including the growing use of interconnected health information systems and the increasing need of different healthcare partners searching for health information to accomplish their daily tasks (CMMS, 1996). Until recently, medical information was recorded and maintained on paper and stored in the offices of community-based physicians, nurses, hospitals and other healthcare professionals and institutions. This imperfect system of record keeping has in some ways created a false sense of privacy among patients, providers and others. The health information of patients has never remained completely confidential" (CMMS, 1996).

Some examples to illustrate different privacy breaches cases and the resulting consequences are discussed next.

I. In Russia, a Surgeon of Boris Yeltsin acknowledged that Yeltsin had failed to disclose details about the status of his health during an election campaign. His

advisors felt that such disclosure would adversely affect the outcome of the election (CNN Interactive, 1996). This example demonstrates how the disclosure of health information can negatively impact the lifestyle of prominent people and why these people may opt not to disclose this information. Business leaders, voters and foreign governments are interested in the health of politicians, celebrities and prominent citizens.

II. A breach of the health privacy of an individual can have significant implications well beyond the physical health of that person. These include the loss of a job; alienation of family and friends; the loss of health insurance and possible public humiliation. The following examples illustrate these possibilities:

    a. A banker who works as a country health board official gained access to the records of patients and identified several people with cancer and cancelled their mortgages (Medical Records, 1999);

    b. A physician was diagnosed with AIDS at the Hospital which he practiced medicine. His surgical privileges were suspended (Estate of Behringer - Medical Center at Princeton, 1999);

    c. A candidate for Congress nearly saw her campaign derailed when newspapers published the fact that she had sought psychiatric treatment after a suicide attempt (New York Times, October 10, 1992);

    d. In July 2001, Eli Lilly mistakenly revealed the e-mail addresses of 600 patients who were taking the antidepressant Prozac, resulting in charges by the Federal Trade Commission against the company (O'Harrow, 2001);

    e. In mid-February, 1999, the University of Michigan Center received a security-oriented wake-up call: several thousand patient records (including names, addresses, social security numbers, employment status, treatments and other information) were posted to the internet, via their web site, by accident. The information, used to schedule appointments, was not supposed to be available in such manner but an error in set-up caused the exposure. The records were quickly removed from Internet access but the damage was done. This serves to illustrate how an error can cause privacy breaches (Hancock, 1999).

III. The misuse of patient information can have equally severe consequences for the person who misuses the data. The HIV/AIDS Ministries Network cites the example of the mother of a 13-year old, an employee at a University Medical Centre, who took her daughter to work because she could not find a child minder. The girl retrieved confidential data of seven former hospital patients from the computer of the hospital. She called the former patients and informed them they were HIV-positive. The girl was sentenced to five years probation and psychiatric therapy (HIV/AIDS Ministries Network, 1995).

These examples highlight that breaches of patient privacy can result in negative consequences for the patients and the individual responsible for the disclosure. The scenarios described in Example II illustrate how breaches of health privacy can harm our personal health status.

The following section is aimed at determining the viewpoint of the patients with regard to the confidentiality of their medical data or how sensitive they are about their personal data.

2.6 THE VIEWPOINT OF THE PATIENT WITH REGARDS TO THE CONFIDENTIALITY OF THEIR MEDICAL INFORMATION

Patients, in South Africa, have the right to submit their complaints to the Health Professions Council of South Africa (HPCSA) that deals with medical staff who violate the patient right of protection of their health information. This Council deals mostly with patients who were tested for HIV without their consent, breaches of doctor / patient confidentiality or doctors who refused to treat people living with HIV (HPCSA, 2002).

A medical practitioner at Wendywood hospital, for example, admitted that he was guilty of testing a patient for HIV without counseling and disclosing her HIV status to her employer. He paid a R 10 000 admission of guilt fine to the HPCSA (HIV/AIDS Law and Human Rights Update, 2004). The HPCSA, in another case, investigated a doctor in Johannesburg, who allegedly withheld anti-retroviral medication from a patient who owed him money (HIV/AIDS Law and Human Rights Update, 2004).

This increase of persons becoming more concerned about their information privacy has gained wide attention even in other sectors. A survey of more than 1850 Americans conducted by California-based Impulse Research on behalf of

Chubb Group of Insurance Companies found that 65% of respondents would like to see organizations that fail to protect customer data fined and 63% want these companies criminally charged (finextra news, 2005).

2.6.1 Types of sensitive information

Lincoln & Essin identify four types of sensitive information from the perspective of the patient. These are discussed in the following sections.

Firstly, although personal medical information of the patient is accurate, it can be sensitive because it could harm the individual (Lincoln & Essin). The medical status of a person can be damaged multiple ways. For example, if it known that a prominent person has a sexually-transmitted but treatable disease, like syphilis, the situation can be personally embarrassing. In the U.S.A, diagnosis of cancer is sufficient to deny a person both insurability and livelihood. Furthermore, the diagnosis of a person who is HIV positive or who has contracted AIDS can complicate further matters. People fear infection and may discriminate against such a person based on his/her lifestyle (Oberholzer, 2001). AIDS possibly presents the greatest challenge in terms of confidentiality and privacy. It is questionable whether employers would employ risk-taking workers.

The second type of sensitive information is personal information that can be highly subjective (Lincoln & Essin). For example, psychiatric records may contain subjective judgments on the attitude, behaviour and potential placement of a patient.

The third type of sensitive information is, for example, the prognosis of a medical condition, considered proper for the treatment of the patient but is not diagnostically confirmed (Lincoln & Essin). An elevated blood pressure, possibly caused by anxiety or disease or anger, may be diagnosed as hypertension. Although the diagnosis has to be done to bill the patient, it can mark the patient as hypersensitive (Oberholzer, 2001).

The final type of sensitive information is the lists of patients that link their demographic data to some medical interest or condition (Lincoln & Essin). Healthcare institutions use these lists to promote proper healthcare but some use them for marketing purposes. Some lists can be used to raise money. The potential for misuse is evident and present safeguards may be inadequate to prevent possible gross violations of privacy.

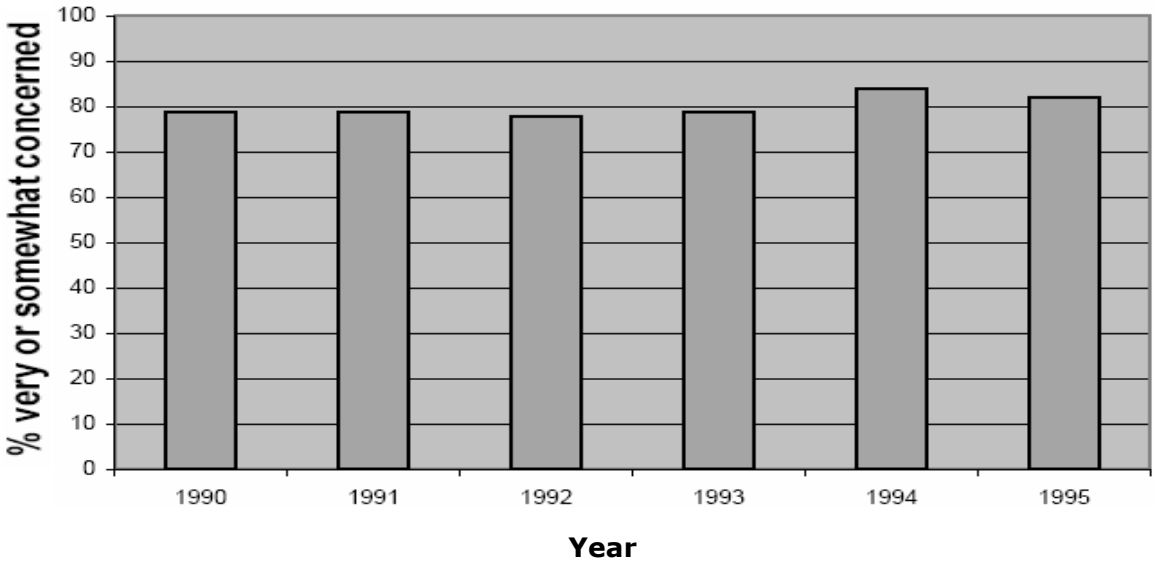
2.6.2 Privacy and Confidentiality Research and U.S. Census Bureau Survey

The American Statistical Association (1979) reported that issues of privacy and confidentiality were gaining more attention and were contributing to respondent suspicion and their reluctance to participate in surveys. The general idea is that people are becoming increasingly concerned that they are losing control over their personal information and they fear that if they divulge certain information it may be used against them (DHHS, 2000). The Census Bureau has a sound record for maintaining confidentiality but people still believe their confidentiality pledge and think that some census and survey requests invade their privacy (Mayer, 2002). This is demonstrated in the following surveys:

During the early to mid nineties, Louis Harris and Associates (1990; 1991; 1992; 1993; 1994; 1995), reported the results of a series of national public opinion surveys regarding privacy issues in general. This investigation did not specifically address attitudes about the Census Bureau. It is interesting, however, to note that the results suggest that public concerns about privacy remained consistently high over that period of time. The question "How concerned are you about threats to your personal privacy in America today – very concerned, somewhat concerned, not very concerned, or not concerned at all?" 46% and 33% were very concerned and somewhat concerned, respectively, in 1990 (HARRIS, L. and Associates, 1995).

Results were similar in the following years with 48% and 31% (1991), 47% and 31% (1992), 49% and 30% (1993) 51% and 33% (1994), and 47% and 35% (1995) of participants reporting that they were very concerned and somewhat concerned, respectively. These result indicate that a large majority of the population are, at least "somewhat concerned" about threats to their personal privacy, and that there has been no reduction by the public with their concern about their personal privacy from 1990 through 1995. There is possibly a slightly increasing trend as shown in Figure 8 (HARRIS & Associates, 1995).

Figure -8- Concerns about personal privacy threats



Source: Louis Harris and Associates (1990; 1991; 1992; 1993; 1994; 1995)

It can be summarized as shown figure 8, that concerns about the personal privacy threats has remained a pertinent issue in the six years of the survey. These concerns become even more critical when dealing with medical information because it contains sensitive information that patients will find objectionable if disclosed to unauthorized users.

2.6.3 The Fisher Medical Centre Patient Confidentiality Survey

In May 1996, a questionnaire was given to 330 patients at the Fisher Medical Centre in North Yorkshire, United Kingdom. Its principal objective was to give the patients information about the security and confidentiality of their medical records and at same time poll the views and concerns of the patients. The survey was carried out jointly by the Centre and Professor Mike Wells of the University of Leeds (Anderson, 1996).

A leaflet that elucidated the right to privacy of the patient accompanied the questionnaire. The leaflet stated the limits of the actions the hospital had with regards to the privacy and confidentiality of the record of the patient. It explained who will see the records; where the information will be sent and how the patient can ascertain what is contained in his/her records.

The authors further compare the results of this survey with those of the 15th Annual Symposium of Computers in Medicare Care, Panel on Patient Privacy and Confidentiality. 44.5 % of the questionnaires were returned to the practice; 57 % felt that they should explicitly give approval to keep their medical records on computer, although 61 % felt that it was more important to have their records accessible than to protect their privacy (Anderson, 1996).

This study reached the following conclusions (Anderson, 1996):

- Records can be made available to hospitals doctors;
- Records should not be shared with other agencies;
- Records should only be computerized if the patient consented;
- Records should be confidential between the doctor and the patient;
- Records should only be accessible to the doctors and the nurses within the practice.

Martin (2000) further argues that, as time has progressed, additional factors such as the use of administrative records, the advent of new data dissemination media and advances in technology (e.g., computers and data linking capabilities) have been added to the privacy and confidentiality equation. It is likely that new factors will continue to be added in the future. This makes more complex efforts to ensure protection of privacy and security of patient information.

It is clear from both scenarios discussed, that concerns about privacy and confidentiality have remained a pertinent issue in the opinion of the general population. Currently, it can be generalized that people worldwide are becoming increasingly concerned about the protection of personal information. Therefore, they are demanding their governments to force organizations to ensure that they have proper mechanisms in place ensuring the protection of such critical information.

2.7 PROTECTING PRIVACY AND SECURITY OF HEALTH INFORMATION

"In the last few years, the protection of computerized medical records and of other personal health information has become the subject of both technical research and political dispute in a number of countries" (Anderson, 1996).

Healthcare organizations must decide who has access to health information systems and whose needs for access are legitimate. A patient has a fundamental

right to his/her medical information. Third parties who may have a "need to know" must acknowledge the rights of the patient and request explicit permission or consent for each instance of collecting, processing, or other uses related to such sensitive information (NRC, 1997).

Security and privacy are not interchangeable issues as previously discussed. There is a necessity for healthcare organizations to have in place protection mechanisms ensuring the protection of both security and privacy. It can be generally confirmed that the protection of security of health information can be assured by the existence of a reasonable or adequate security standard framework; while privacy protection includes limits of a legal nature to the collection, handling, storage or transmission of personally identifiable or aggregate data collected from individual users.

Policies must be established to determine who can have access to what information. Healthcare organization must implement mechanisms preventing those without legitimate needs from gaining access to information. They must try to develop mechanisms to keep those who are granted access from divulging information to others (NRC, 1997). These mechanisms must balance the need for health information while ensuring that healthcare will not suffer because someone has been unable to gain access to important information (Fitzmaurice, 1998).

Individuals desire to keep their health information private but they agree that medical professionals should have access to their information as proved by the following survey:

Lincoln & Essin record the following statistics made at the 15th Annual Symposium of Computers in Medical Care, Panel on Patient Privacy and Confidentiality. 14000 University personnel, sharing a common university hospital facility, were reasonably well-informed and briefed on the risks of employees and colleagues who can pry into their medical records. They were asked whether they would want their healthcare records made particularly secure and more difficult for legitimate professionals to reach. Only 3% requested such added protection. This small percentage can be justified by numerous benefits on the behalf of the patients and the organization that results from such disclosure of health information.

Healthcare providers need access to health information to provide advice and make decisions which are in the interest of the health of the individual. Clinical

researchers need health information to answer questions about the effectiveness of specific therapies, patterns of health risks, behavioral risks or a genetic predisposition for a disease or condition (e.g., birth defects). Health insurers seek to combat rising costs of care by using large amounts of patient data in order to judge the appropriateness of medical procedures. Life insurance companies need medical information to improve their underwriting process and help detect possible instances of fraud in the use of health information.

Healthcare organizations will suffer as patients become less willing to seek care, or they withhold sensitive information unless proper ways can be found to balance the privacy rights of individuals against the legitimate needs of such organizations for patient information (U.S Senate, 1997). This will in turn impact their health status as they will be not receiving enough healthcare services.

2.8 CONCLUSION

Electronic Medical information provides numerous advantages over traditional paper-based records. It allows more accurate and reliable information available to healthcare providers, researchers, insurers, and administrators. It helps improve the quality of medical transactions processing and communication between different business partners. However, the increase sharing of medical information between various business partners raises privacy and security breaches problems.

People reveal information organizations to healthcare of the utmost sensitivity, for example their HIV status. This information is only useful to the patient when shared with his/her healthcare professionals. However, this information is sometimes used without their knowledge or consent (Sadan, 2001). The use of personal medical information for medical research with consent might be acceptable, but its use to cancel loans and similar for cancer and HIV positive patients, because they pose a credit risk, is unacceptable. It becomes necessary to ensure that any system of electronic health information must protect against this type of misuse of information to ensure the rights of patients to privacy and security are safeguarded. However, patients recognize that their information should not be difficult for legitimate medical professionals to access.

The dilemma of obtaining, using and sharing health information to provide care, while not breaching patient privacy, is a serious concern (Smith & Eloff, 1999). According to Dash (2000), the challenge for IT leaders is to strike a balance between safeguarding privacy and ensuring that security measures are flexible

enough so that caregivers are not denied access to information in an emergency situation. It may be that what the public desires is not absolute privacy but reasonable assurances that when personal information is collected, the healthcare providers, managed care organizations, and insurers will treat it with respect, store it in an orderly and secure manner and disclose it only for public health purposes and in accordance with publicly accountable principles of fairness (Gostin, 1997).

This chapter has shown that there are a growing number of patient privacy breaches resulting in public concern about the loss of privacy of their health information. It is indisputable that there is a need to protect the privacy and security of health information. This protection is complicated because ensuring privacy protection does not guarantee security protection and vice-versa. It is the combination of a framework with regulatory requirements that such protection can be satisfied. The U.S. Public Policy Committee of the Association for Computing (USACM) further believes that inadequate or poorly designed security standards, regulations, and legislation can have a negative impact on the privacy of medical records (SIMONS). In addition, the King Report (2001) on the Code of Corporate Practices and Conduct, states that the Board should ensure that the company complies with all relevant laws, regulations and codes of business practices to increase business enterprise value.

Chapter 3 deals with security standards frameworks and best practices that can be used to secure health information. **Chapter 4** is dedicated to the discussion of the legal and regulatory frameworks at national and international levels aiming at protecting privacy and the security of information.

Chapter 3 INFORMATION SECURITY STANDARDS AND BEST PRACTICES

The principal aim of **Chapter 3** is to assist healthcare management in the interpretation, application and understanding of the benefits and limits of internationally accepted approaches to information security standards frameworks and best practices. This will help healthcare organizations in making a best choice on which best practice approach should be implemented to ensure a comprehensive and complete Information Security program.

Chapter 4 is devoted to a discussion of legal and regulatory requirements pertaining to South African health sector.

"The central truth is that information security is a means, not an end. Information security serves the end of trust. Trust is efficient, both in business and in life; and misplaced trust ruinous both in business and in life ".

- Dan Geer (2005) -

3.1 INTRODUCTION

Information has grown to become arguably the most important asset in most organizations today. It is crucial, for this reason, to ensure that information and its associated information resources are well-protected. The introduction, management and maintenance of a high level of Information Security in an organization require a proper management methodology (von Solms, 1998). The task of protecting information in a satisfactory manner is difficult due to the increased interlinking of healthcare information systems with the IT systems of other business partners.

The Information Security is no longer only a domestic issue because it affects external parties (von Solms, 1999). It is important to realize that once healthcare organizations are trading electronically with other business partners, the direct control over information resources is no longer in the hands of that organization. The poor security practices of a business partner may threaten the security of that organization (von Solms, 1997). Therefore, it is evident that there is a need for a mutual trust between business partners and the best way to establish such trust is through a comprehensive IT security program. This is achieved through the implementation of well-recognized security standards or guidelines.

Von Solms (1999) makes a business case for the need of security standard in an interconnected eBusiness environment using the metaphor of driving a car.

"Driving the only motor vehicle on the farm requires very little safety and traffic regulations and it is fairly easy to drive safely around the farm. The only requirements would be some technical safety mechanisms to be in place and working satisfactory. When a driver drives on a public road, a totally different approach to road safety is introduced. One reckless driver poses a big threat to other vehicles and drivers. Any motor vehicle on a public road requires a valid

roadworthy certificate that will indicate that all technical safety and security mechanisms and features on the vehicle are present and functioning properly. The driver needs a driving license that will indicate that he/she has learned how to drive the vehicle in a secure way by using the technical safety features correctly and effectively. Further, a third party, i.e traffic officers will continuously ensure that the vehicle is functioning technically well and also that the driver obeys all road usage regulations. He concluded that BS 7799-2 can certainly provide the basis to ensure safe driving on the information super highway" (von Solms, 1999).

It is critical to highlight, using this business case, that if all the drivers on public road adhered to all the rules and regulations, there would be mutual trust between them which would ensure a safe driving environment. The same principle applies when healthcare organizations enter into inter-company trading between health providers, health plans, health clearinghouses and business associates. In accord with this metaphor of driving a car, Figure 7 illustrates an example of a complex healthcare transaction environment between various healthcare business partners.

A Medical practitioner working on his (her) own conducts his (her) business transactions requires a less effort for security issues because the system is not linked to other external ones. Hence, it is easy to control most of the business transactions and ensure their security. On the other hand, when there is an interlinking between various healthcare systems, as shown in Figure 7, then a holistic approach to Information Security and privacy becomes necessary. If one of the business partners does not properly implement an effective Information Security program, it can result in the assets of the other being at risk. This scenario is comparable to the previously mentioned business case of driving the motor vehicle on a public road, which necessitates more severe requirements than driving one motor vehicle around the farm. This is comparable to the medical practitioner business activities.

The information exchange and other relations between businesses, organizations and administrations, both at national and international levels, create a need for the use of recognized standards in the management of Information Security (Saliba & Saint-Germain, 2004). Healthcare organizations, as already mentioned, wanting to demonstrate good corporate governance, have a duty to their stakeholders to ensure they have effective Information Security ensuring integrity,

safekeeping, availability and privacy of sensitive and personal data. This will in turn increase trust and confidence to both customers and different business partners (von Solms, 2005). Mutual trust, according to Barnard & von Solms (1998), can optimally be obtained through a scheme where an IT environment is evaluated and certified according to a generally accepted set of standards.

It is important to note that having agreed to incorporate a security standard as a means to Information Security Governance efforts does not imply the end of the tasks for the Executives and the Board of Directors. It marks the beginning of their duties. The growing number of security standards and guidelines that require healthcare organizations to provide security controls and demonstrate compliance assurance necessitates healthcare executives and others responsible for ensuring compliance with the applicable security requirements pose the following questions:

- Where to begin on the road towards security compliance?
- What security standards or guidelines are better practices than others?
- Should an Information Security standard, a code of practice, or guidelines be used?
- Should one security standard or a combination be used to ensure a more balanced Information Security Management approach?

The following sub-problems areas are revealed from these questions:

- Terminology definition – for example, what is the difference between an "Information Security Standard" and a "Code of practice"?
- Confusion regarding the various internationally accepted approaches to Information Security Management, for e.g., should ISO17799 be deemed a standard or guideline?

The main focus of this chapter is to provide answers to these questions. The rest of this chapter is organized as follows: the next section is devoted to describing the various Information Security Management concepts and terminology, followed by a description of numerous security standards, guidelines and approaches that play an important role in ensuring best practice in general. ISO 17799, the only international security management standard, is discussed in detail as it constitutes the "heart" of this project. Nevertheless, it is necessary to emphasize that although ISO 17799 provides many advantages to security management and provides general guidance on a wide variety of topics, but it typically does not go into depth (NIST, 2002). It needs to be complemented by other existing

standards which result in a more balanced Information Security approach (IT Governance Institute, 2005).

The next section is devoted to the formulation of broad definitions for certain terms and concepts used generally to describe the management aspects of safeguarding IT resources to clarify these various Information Security Management terms and concepts generally related to this area. This will create a strong basis understanding for the various people involved in the process of managing Information Security. It has been previously mentioned that although Information Security is considered a technical view side, it needs to be regarded as a corporate issue (Entrust, 2004). It requires a common understanding of the terminology used from upper management to lower level employees.

3.2 ELUCIDATION OF TERMS AND CONCEPTS

The following terms need to be refined and clarified because the main objective of this chapter is to formulate a formal and comprehensive approach to IS management. The following "general" definitions from the "American Heritage Dictionary of the English Language", Third Edition are used (DICT, 1992).

3.2.1 Standards

"An acknowledged measure of comparison for quantitative or qualitative value; or a criterion. A degree or level of requirement, excellence or attainment" (DICT, 1992). Standards enable people in all walks of life to communicate at a level where all parties can understand one another. The result is that standards not only serve to eliminate confusion but serve to level the playing fields (Eloff & von Solms, 2000). The law does not, for example, enforce standards that are not supported by criminal or civil legislation, with the result that no offence would be committed should the standard be ignored or not followed (Gray, 1991). On the other hand, when organizations fail to adhere to certain standards, it can result in huge financial loss, owing to the loss of business opportunities and trust by customers. It is important to highlight that standards should be considered in terms of their approval which could be organizationally, nationally and internationally.

International standards can be defined as documented agreements containing exact criteria that must be followed consistently as rules, guidelines or definitions of characteristics to ensure that any materials, products, processes or services

are fit for their purpose (Oppliger, 1996). The International Standards Organization (ISO) and International Telecommunications Union (ITU-T) are good examples of international standards organizations that are accepted worldwide (Gray, 1991). On the other hand, at the national or public level, each country has its own standards body, for example, British standards Institution (BSI), the American National Standards Institute (ANSI) and the South African Bureau of Standards (SABS) are nationally accepted in the USA and in South Africa. At the organizational level, the term "standards" can be used to refer to a specific set of rules and requirements adopted in or prescribed for the company internally.

3.2.2 Guidelines

A statement or other indication of policy or procedure which determines a course of action (DICT, 1992). In terms of ISAC (1999) definition of the term "guideline", a guideline should consider certain guidelines in determining how to implement a standard. In the Information Security context, the term "guidelines" refers to the set of recommended actions or policy statements that can be performed or adhered to achieve a specific objective. Guidelines are laid down to remind users not to overlook or ignore specific security measures, even though the latter can be implemented in multiple ways (NIST, 1995). It is crucial to note that even though a guideline may form an integral part of a standard, the terms "standard" and "guideline" are not interchangeable. A standard shall be said to comprise a number of guidelines that should be followed to adhere to that standard. However, the reverse is not true as because not all guidelines form part of national or international standards.

3.2.3 Code of practice

A code of practice generally constitutes the result of years of experience. Organizations will, often by trial and error, chance upon certain practices, or actions that are certain to yield positive results. These practices are made available to other organizations. This ensures that, other organizations can benefit from their experience because they have tried and tested certain practices. Guidelines and code of practice are, to a certain extent, the same, with the main difference between them being that a code of practice is based purely on practical experience, whilst a guideline may not have had the experience (Eloff & von Solms, 2000).

3.2.4 Controls

A Control is an instrument or a set of instruments used to operate, regulate or guide a machine or vehicle (DICT, 1992). According to the ISAC (1999) definition, the concept "general controls" refers to the environment within which computer-based application systems are developed and maintained. These general controls, are used to ensure that applications are properly developed and implemented to ensure they operate securely. For example, a control implemented to realize the objective of a strong authentication is that set of measured steps to be effected in order to implement a mutual authentication protocol such as Kerberos (Eloff & von Solms, 2000).

3.2.5 Compliance

Compliance is a self-assessment carried out by an organization to verify whether a system that has been implemented complies with a standard (Bisson & Saint-Germain, 2003). This standard may be required for a national or international standard frameworks or regulatory requirements.

3.2.6 Certification

The term "certification" describes the method whereby an organization, a product or a process is tested and evaluated to determine whether or not it complies with a specific standard. It is conferred by an accredited certification body when an organization successfully completes an independent audit, thus certifying that the management system meets the requirements of a specific standard, for example, BS 7799-2.

3.2.7 Accreditation

Accreditation means attesting to and proving as having met a prescribed standard (DICT, 1992). It consists of the means by which an authorized organization (the accreditation body) officially recognizes the authority of a certification body to evaluate, certify and register an Information Security Management System (ISMS) of the organization with regards to published standards.

3.2.8 Benchmarking

Benchmarking means to measure according to specified standards to compare with and improve the measured product (DICT, 1992). The main objective of benchmarking is for management to check how well other organizations are doing. This informs them to where they should increase their efforts. Whitman & Mattford (2003) further states that benchmarking involves the process of seeking out and studying best practices used in other organizations that produce the results they desire in their organization.

3.2.9 Self-assessment

The term "self-assessment" describes the process which is carried out to determine the effectiveness of the IS controls implemented in an organization. This process is performed internally within the organization.

3.2.10 Legislation

The term "legislation" in the discipline of Information Technology, pertains to any legal requirements contained in a specifically Information systems-related law, which law enacts that such requirement be satisfied. The Electronic Communication Transaction Act (ECTA) constitutes an excellent example of the legal requirements pertaining to e-commerce in South Africa.

Healthcare management find it easier in choosing a more comprehensive and efficient security practices by having a good understanding of these critical terms and concepts used generally to describe the management aspects of safeguarding IT resources. It is very easy for a driver to make a decision of which roadmap to follow before starting the journey instead of driving by guessing during the journey.

3.3 ENSURING BEST PRACTICES IN MANAGING INFORMATION SECURITY

Several standards and collections of best practices are currently available, which prescribe how to manage the function of various organizations. Several private or partly private organizations have published suggested guidance in addition to the international standardization organizations. However, each of these standards addresses specifically a certain IT aspect: IT governance, Information Security

Management or just only technical aspect. Von Solms (2005) suggests that because of the convergences that exist between these standard frameworks, using them together can provide a synergy which can be beneficial to companies.

The main objective of this chapter is not to compare these standards frameworks but rather to discuss the possibility of combining them and whether this produces synergy. The choice of sets of these recommended best practices and standards is based on their level of popularity of acceptance by many organizations.

3.3.1 ISO 17799/BS 7799-2 Security Standard Framework

The business community has, for years, been searching for a practical Information Security standard – one that can provide organization with best practices and be universally or generally accepted internationally. Organizations like NIST, ANSI, ISO and others have been producing computer security standards and best practices for decades, most were technical and many academic and impractical in terms of meeting business needs (Gordan, 2005).

The trend in Information Security has recently changed from technical security controls to a concern for overall risk management. This shifts Information Security from a strict IT focus to a business practice issue (Gordan, 2005). Out of this change, one set of standards has emerged that allows business to establish and successful mitigate risk to an acceptable level. The BS7799 standards - the ISO/IEC 17799:2000 Code of Practice for Information Security Management and BS 7799:2002 Information Security Management System specification have gained worldwide acceptance in recent years and are almost universally recognized as quality information management. The acceptance and adoption of these standards is recognized and for certain industries is required by state and federal governments in Europe, the Asia-Pacific region, Canada, South America and some African countries.

The ISO 17799 recognizes that information exists in many forms. It can be printed or written on paper, stored electronically, stored electronically, shown on films, or spoken in conversation. ISO 17799 recommends that whatever form the information takes or the means by which it is shared or stored, it should always be protected (ISO 17799, 2000). Information Security consists of preserving the following elements (ISO 17799, 2000):

- **Confidentiality**: ensuring that information can only be accessed by those with proper authorization;
- **Integrity**: safeguarding the accuracy and completeness of information and the ways in which it is processed;
- **Availability**: ensuring that authorized users have access to the information and the associated assets whenever required.

3.3.1.1 The History of ISO 17799 and BS 7799-2 Security Standard

The British Standards Institution (BSI) has, for over a hundred years, carried out studies for the purpose of establishing effective, high-quality industry standards. BS 7799 was developed at the beginning of the nineties in response to industry, government and business requests for the creation of a common Information Security structure. In 1995, the BS7799 standard was officially adopted.

Four years passed before the publication in May 1999 of a second major version of the BS 7799 standard, which incorporated numerous improvements. It was during this period that the International Organization for Standardization (ISO) began to take an interest in the work published by the British institute.

In December 2000, ISO took over the first part of BS 7799, re-baptizing it ISO 17799. In September 2002, a revision of the second part of the BS7799 standard "Information Security management systems – Specification with guidance for use" was carried out to make it consistent with other management standards such as ISO 9001:2000 and ISO14001:1996 and with the principles of the Organization for Economic Cooperation and Development (OECD). It must be clarified that as of February 2005, BS7799-2:2002 [BS7799-2] has not yet been adopted by ISO. It has been accepted by many national standards' organizations, among which, is the South African National Standards (SANS) organization. A new version was published in November 2005 and it will be discussed in this section.

The BS 7799 security standard consists of:

- Part 1: Information Technology – Code of Practice for Information Security Management (ISO 17799)
- Part 2: Information Security Management Systems – Specification with guidance for use (BS 7799-2)

It is important to note that ISO/IEC has released a new edition of ISO 17799, officially called ISO/IEC 17799:2005 on 20 June 2005, to address some of the weakness in ISO 17799 (Rasmussen, 2005). Ted Humphreys (2005), Chair of the ISO/IEC JTC1/SC 27 Working group responsible for ISO/IEC 17799 and ISMS standards stated, "this new version of ISO 17799 will place Information Security on a truly international footing, addressing issues such as: security of external service delivery and the provision of outsourcing; addressing today's vulnerabilities, such as the management of patches; security prior to, during and termination of employment; greater focus on handling risks and incidents; dealing with mobiles, remote and distributed communications and processing of information; and keeping up–to-date with emerging business threats and requirements". ISO/IEC 17799-2005, in terms of controls area, contains 134 controls divided in 11 domains.

Additionally, ISO/IEC JTC1/SC27 (the standards committee that deals with ISO/IEC 17799) is in the process of preparing an ISMS requirement standard. The BS 7799 part-2:2002 will be withdrawn and replaced by the ISO/IEC 27001 standard when this work is finished and published by ISO/IEC (estimated publication date towards the end of 2005) (Humphreys, 2005). The BS7799-2:2002 will continue to be in force as the standard against which an ISMS will be certified until the final version of ISO/IEC 27001 is issued (itGovernace, 2005).

In this project, the new version of the ISO 17799 was not used for the comparison to the effect that the detailed comparison between ISO 17799 and these laws had already been concluded at the time of the release of the new version of ISO 177999. Therefore, the new version was studied only for the purpose of determining whether there are major changes (and not for detailed comparison).

The question that is raised is, what are the distinctions between Part 1 and Part 2 of the BS 7799 Security Standard?

3.3.1.2 BS 7799 Part 1 (ISO 17799) versus BS 7799 Part 2

The BS7799 Part 1 is an implementation guide, based on suggestions. It is used as a means to evaluate and build sound and comprehensive Information Security infrastructure. It details Information Security concepts an organization "should" do. BS 7799 Part 2 is an auditing guide based on requirements. Organizations are audited against Part 2 to be certified as BS 7799 compliant. It details

Information Security concepts an organization "shall" do. This rigidity precluded widespread acceptance and support (Carlson, 2001). This research focuses on ISO 17799, the Code of Practice regarded as a detailed comprehensive catalogue of guidance on what constitutes good security practice (ISO 17799, 2000).

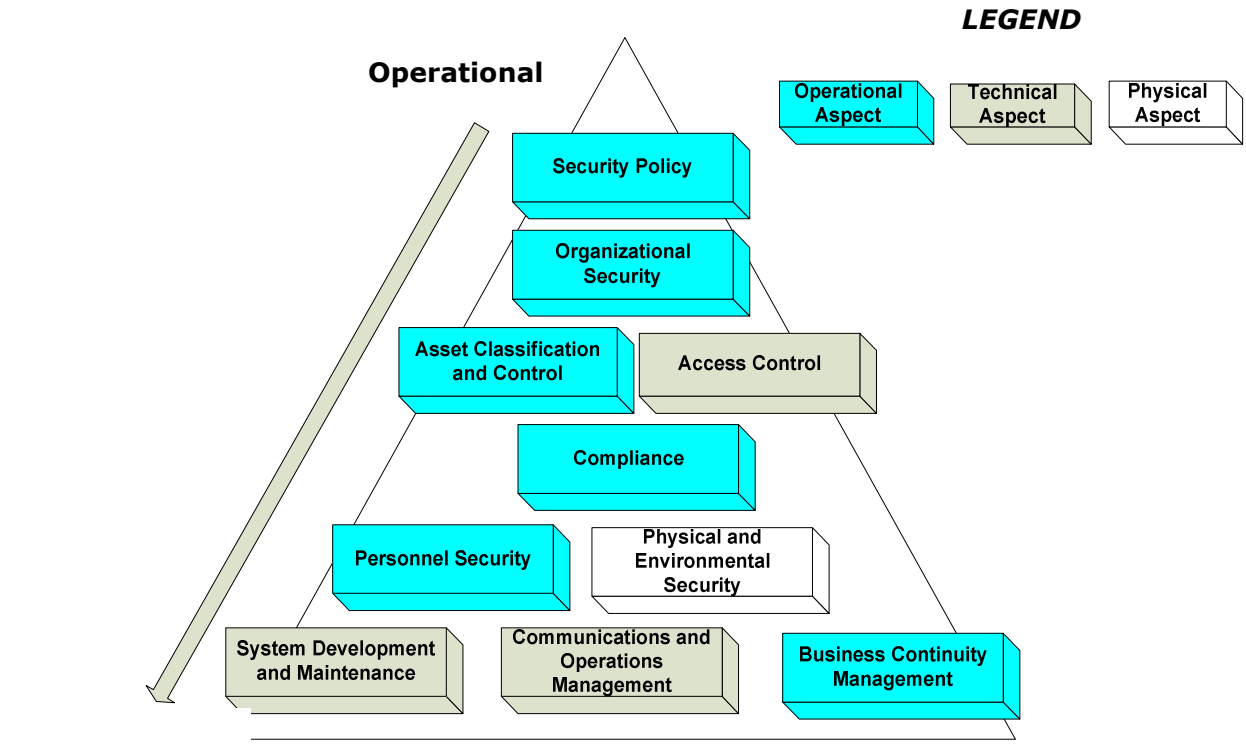
Both ISO 17799 and BS 7799-2 In terms of controls areas address the same 10 control areas that cover 36 control objectives and 127 controls.

- In ISO 17799, each control is illustrated with "best practice" advice;
- In BS 7799-2, each control is formulated into an auditable requirement.

Appendix B is devoted to giving a brief overview of each of its ten main domains to gain a depth understanding of the BS 7799 / ISO 17799 security standards

It is evident that ISO 17799 touches on all the Information Security aspects ranging from the organizational, physical and technical. Figure 9 illustrates a structure for the ten domains of the ISO 17799 standard. Each domain deals with a separate topic built around **Administrative**, **Technical** and **Physical** measures and are driven from the top down. The impact of ISO 17799 is felt from the management level all the way to the operational level.

Figure -9- ISO17799 domain structure



Source: Bisson & Saint-Rene, 2003.

3.3.1.3 Benefits of the ISO 17799/BS 7799-2 security standard

Obviously, complying with ISO 17799 standard or obtaining BS 7799-2 certification does not prove that an organization is totally 100% secure. The truth is, barring the cessation of all activity, there is no such thing as complete security. It is rare to guarantee a complete security while doing eBusines transactions (Bisson & Saint-Rene, 2003). Unexpected and unintentional mistakes by employees are still possible. Nevertheless, adopting ISO 17799 international standards confer certain advantages that security managers should take into account. These benefits can be generally noticeable at the organizational, legal, operating and commercial levels.

A. Organizational level benefits

Commitment - certification serves as a guarantee of the effectiveness of the effort put into rendering the organization secure at all levels and demonstrates the due diligence of its administrators. This in turn increases the trust of both business partners and the customers.

B. Legal level benefits

Compliance - certification demonstrates to competent authorities that the organization observes all applicable laws and regulations. This is where the standard complements other existing standards and legislation (for example HIPAA, SANHA, ECTA). A good security management includes effective mechanisms to maintain legality. This can only be accomplished when the regulatory requirements have been proven to be implemented based on the security standard framework. For example, BS 7799 has been recommended by the UK Data Protection Commissioner as means by which organizations can demonstrate they meet the requirements of the Data Protection Act 1998 (Callio Technologies, 2001).

C. Operating level benefits

Risk management - leads to a better knowledge of Information Systems, their weaknesses and how to protect them. Equally, it ensures a more dependable availability of both hardware and data because risks are well managed and kept at a minimum level.

D. Commercial level benefits

Credibility and confidence - means partners, shareholders and customers are reassured when they see the importance afforded by the organization to protecting information. Certification can help set a company apart from its competitors and in the marketplace. International invitations to tender are starting to require ISO 17799 compliance. Business partners increasingly want to know the security status of their partners. Companies see certification to BS 7799 as a prerequisite for doing business (Callio Technologies, 2001). This in turn increases the competitive advantage of the enterprise.

E. Financial level benefits

Reduced costs - are related to security breaches and the possible reduction in insurance premiums. The following of a well-established Information Security program has numerous advantages for the organization because it ensures that security controls are in place preventing threats and attacks that can prove costly to the organization.

F. Personnel level benefits

It helps **improve employee awareness** of security issues and their responsibilities within the organization. ISO 17799 requires organizations to have in place policies that everyone in the organization should follow. Additionally imposes disciplinary actions on those who take these policies and procedures negligently.

G. Minimizing business risk

It ensures controls are in place to **reduce the risk** of security threats and to avoid system weaknesses being exploited. It helps the organization develop a business continuity plan that will minimize the impact of any security breaches (Ashton, 2002).

The ISO 17799 and BS 7799-2 provide organizations with the assurance of knowing that they are protecting their information assets using criteria in harmony with an internationally recognized standard. Laws and regulations continue to change and BS 7799 incorporates a requirement for identifying which

laws are relevant and assures that compliance is addressed. Benefits are applicable to organizations of all size and all ISMS maturity levels.

The ISO 17799 Security Standard received a lot of acclamation since its approval; some organizations which were not impressed by its adoption advanced some criticisms related to this international standard. The following section discusses some of the criticisms from different authors.

3.3.1.4 The critics of the ISO 17799/BS 7799-2 security standard

Lawrence (2002) states that there was little consensus when the ISO adopted ISO 17799 in August 2000. "A carbon copy of the first half of the much-aligned BS 7799, the document drew sharp criticism from major IT nations, which charged it didn't meet the criteria of an international standard" (Lawrence, 2002).

A. A technical report but a not a standard

It was fast-tracked through the approval process in August 2000, and ISO 17799 had the support of many small countries but only one of the large G7 nations—the United Kingdom, where it was born as BS 7799. Canada and Germany have their own competing standard. The United States has the NIST publications. None of the large countries wanted to support a competing standard. Critics charged that ISO 17799 was passed too hastily, written unevenly and lacked sufficient guidance - that it told managers what to do without telling them how to do it (Sarah, 2003). They said it would have been fine as a set of recommendations but not as a standard (Lawrence, 2002).

Troy states "There are several different approaches to IT security out there; It was our feeling that in order to have a truly acceptable international standard, all of this had to be taken into consideration rather than taking it on a fast track from one source, the main security standard was presented as a fait accompli, and there was no significant opportunity for import from other work that had been done in the area"

Opponents said that the document made it seem that security were just a list of activities, rather than an ongoing process. All the check-list type material was placed in an appendix at the back of the document. This did not address the most fundamental criticism that ISO 17799 should not be classified a standard but rather a technical report (Sarah, 2003).

"When the U.K. brought BS 7799 to ISO, many international bodies would have been very agreeable to having that document become a technical report as opposed to a standard," says Alicia Clay, program manager for Information Security outreach with NIST, who is a representative on the committee that edits ISO 17799. "The expectation of a technical report is that it's more of a guideline. ISO 17799 reads more like a technical report, but technical reports tend not to carry the same kind of weight. People don't generally talk about conformance to reports" (Sarah, 2003).

B. In the Neutral Zone

ISO 17799 requires organizations to protect their information assets but does not specify how. The standard by staying technology neutral, has the ability to grow with the rapidly changing technology landscape. Nevertheless, it rarely attempts to provide guidance in evaluating or understanding existing security measures. This is a big drawback in the minds of the adopters. For instance, the standard recommends the use of adequate access control protection and defines many of the different technologies for access control-tokens, certificates and smart cards. However, it does not discuss the pros and cons of these technologies in different operational contexts. Likewise, it recognizes the need for firewalls but does not offer an explanation on the different types of firewalls packet filters, proxy servers and stateful inspection and how each is used. Equally absent is common sense advice, such as, only enabling necessary services (Lawrence, 2002).

Baumrucker (2000) states that "The ISO 17799 contains a good shell of information, yet lacks depth in new technologies (VPN, remote access, wireless) and recently focused-upon needs such as business continuity/disaster recovery. Such criticisms roll off the backs of ISO 17799 supporters".

C. Not for everyone

The ISO 17799 is open-ended in assessing the value of information resources. It requires adopters to inventory systems and assign values to all digital resources but does not say how this should be done. The Conducting of self-assessments leaves a lot of room for interpretation and mistakes, which is why BSI and other standard auditors recommend having a professional risk assessment conducted before starting an ISO 17799 compliance effort. "It needs to be in conjunction or partnered with outside professional services," says Darwin L. Martinez, Vice President of technology services for National Business Group. "In a large

organization, it can be a large engagement, an expensive engagement that only leads to having another long engagement and the likelihood of getting that kind of support in this economy is slim" (Sarah, 2003). This leads to cost. A copy of ISO 17799 is available through the ISO Web site (http://www.iso.org/) for 164 Swiss francs (roughly $95, depending on the exchange rate which is R665 on the current exchange rate). This initial investment is only a fraction of the cost of security assessments, penetration testing, auditors and consultants, which can run into the hundreds of thousands if not millions of Rand. This is why organizations with a solid working knowledge of their security threats have a better chance at using the standard.

The ISO 17799, even after implementation, is short on methodologies for measuring its effectiveness when put into practice. Each section contains language on the need for periodic policy reviews and regular compliance checks. It is silent on the mechanisms for these checks. Critics say that without such matrices, the standard has no way of proving its value to management.

It is necessary for the security managers to consider using other existing standards to complement the ISO 17799 and therefore fill the gap to overcome some of these criticisms. The next section will describe the complementarities between ISO17799 with various security standards.

3.3.2 Complementarity of ISO17799 and BS7799-2 with other existing Security Standard Publications

The ISO17799 is self-described as "a starting point for developing organization specific guidance." This implies that ISO17799 is not self-sufficient to provide a total security solution. Consequently, the need for additional guidance in some aspects appears conclusive.

3.3.2.1 ISO 15408:1999/ Common Criteria/ ITSEC

The ISO17799 and BS7799-2 were never meant to be technical standards, in the sense that they do not relate to the particularities of various technologies of the security requirements they address, therefore other standards need to come and fill the void.

One such standard is the international standard ISO/IEC 15408:1999 "Evaluation criteria for Information Technology Security" known as "Common Criteria (CC) for

Information Technology Security Evaluation". ISO 15408 was produced by a consortium of North American and European Union government bodies. It was published by the ISO/IEC JTC 1 working group in collaboration with the Common Criteria Project Sponsoring Organization, which published the Common Criteria. After its publication, it effectively evolved from, encompassed and replaced The ITSEC in Europe, Federal Criteria o USA, known as "Orange Book", and the Canadian Criteria. It has been accepted as a working standard by many other countries including Russia, Japan and Australia.

The standard was issued to define criteria as the basis for a common and comparable evaluation of IT security, focusing on the security of systems and products (ISO/IEC 15408). It provides the framework for testing the effectiveness of most security systems and individual security solutions. However, it is not intended to measure the effectiveness of the overall security program of an organization.

There are strong linkages between ISO 17799 and ISO 15408. The latter, certifies the levels of defences conferred by the security measures in IS (Bisson & Saint-Germain, 2003). It covers technical aspects which can be compared to ISO technical aspect of ISO17799. The combination of the use of the two standards where non -IT- security controls are handled by ISO 17799/BS7799-2 and security requirements of the system components are evaluated according to ISO 15408, may provide the best solution in designing and evaluating a system for security (Eloff & Frangopoulos, 2004).

3.3.2.2 ISO 13335 Guidelines for the Management of Information Technology Security (GMITS)

The ISO/IEC TR 13335 Information Technology—Guidelines for the Management of IT Security is a technical report subdivided into five parts. The report was published by ISO/IEC, which have established a joint technical committee, the ISO/IEC JTC1, Subcommittee SC 27 (IT Security Techniques), which is tasked to publish international standards e.g., ISO/IEC 17799:2000.

The report provides guidance on aspects of IT security management and is divided into five parts (ISO/IEC TR 13335):

a. Concepts and IT Models: The management tasks of IT security are outlined, providing an introduction to security concepts and models;

b. Managing and Planning IT Security: It contains guidelines that address essential topics on the management of IT security. These topics are useful for identifying and managing IT security;
c. Techniques for the Management of IT Security: Management Techniques are described and recommended in detail;
d. Selection of Controls: It provides guidance on the selection of safeguards considering the type of IT systems and the security concerns and threats;
e. Management Guidance on Network Security: it contains information on identifying and analyzing communication-related factors that should be taken into account when introducing network security.

The ISO 17799 sets out the best practices for managing Information Security and creating Security Policies, ISO 13335, called GMITS - Guidelines for the Management of IT Security - is its big brother. This standard deals more with the technological aspects of information and brings value-added content to risk assessment. The protective measures proposed in the fourth of GMITS guides (Part 4: Selection of safeguards based on high-level risk analysis) can be compared to the controls offered in ISO 17799 (Bisson & Saint-Germain, 2003).

3.3.2.3 NIST 800-14: Generally Accepted System/Information Security Principles (GASSP / GAISP)

The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST), a department of the US Department of Commerce, published this document. It is part of the 800 series of NIST (computer security). The publication Generally Accepted Principles and Practices for Security Information Technology Systems is a collection of principles and practices to establish and maintain system security. It is labeled as a special publication (NIST-14).

The goal of the standard is to provide a baseline for establishing or reviewing IT security programs. It aims to gain an understanding of basic security requirements of IT systems. It focuses on security practices and describes the intrinsic expectations of security provisions from a high viewpoint in the form of the principles (ITGI, 2004).

GASSP is not a technical document. Furthermore, it deals with the complete picture of Information Security in an organization, not just its IT aspect (Eloff & Frangopoulos, 2004). Therefore, it is predictable that it shares a lot in character

with ISO 17799, a standard addressing the broader spectrum of Information Security threats within the organization.

3.3.2.4 IT Infrastructure Library (ITIL)

The IT Infrastructure Library is a collection of best practices in IT service management. It is focused on the service processes of IT and considers the central role of the user. The first versions of the ITIL collection were published by the British Office of Government Commerce (OCG), which still holds the ITIL trademark. The OCG was commissioned to develop a methodology for the efficient and effective use of IT resources within the British government.

The goal of the Standard or Guidance Publication is the development of a vendor-independent approach for service management. The ethos behind the development was the recognition of increased dependence on IT, which has to be managed by high quality IT services (ITGI, 2004). The major reasons for implementing the guidance are as follow (ITGI, 2004):

- The definition of service processes within the IT organization;
- The definition and improvement of the quality of services;
- The need to focus on the customer of the IT;
- The implementation of a central help desk function.

The ITIL focuses on organizations of varying size. It targets those responsible for IT service management (Wallhoff, 2005). However, a major drawback of this standard is that it is only available as an English version although it supposed to be used internationally (ITGI, 2004).

3.3.2.5 COBIT

The first edition of Control Objectives for Information and related Technology (COBIT) was issued by Information Systems Audit and Control Foundation (ISACF) in 1996. The second edition was published in 1998, with additional control objectives and an Implementation Tool Set. The third edition currently available by the IT Governance Institute in 2000 has added the management guidelines, and several other detailed controls objectives.

(COBIT, 2000) maintain "The COBIT Mission: To research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted

information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals".

It was developed by IT auditors and made available through the Information Systems Audit and Control Association and COBIT provides a framework for assessing a security program and developing a performance baseline and measuring performance over time (ISACA, 2005). COBIT targets various organizations, public and private companies and external assurance professionals from the relevant target group. Three organizational levels are addressed: management, IT users and professionals.

The COBIT standard positions itself as "the tool for information technology governance" (COBIT, 2000). COBIT is therefore not exclusive to Information Security – it addresses IT governance, and refers amongst many other issues, to information security. An advantage of using COBIT is that it positions Information Security Governance framework, which is good because it provides an integrated structure for wider corporate governance (von Solms, 2005). The disadvantage, however, is that the Information Security Governance component of COBIT provides good guidance on the 'what' of Information Security governance but is not very detailed as far as the "how" is concerned.

The ISO 17799 is exclusively for Information Security and only address that issue. Its advantage are is that it is detailed in security controls but provides less guidelines on the methodology. The ISO 13335 and ISO 15408 standards deals more with the technological aspects of information which can be mapped to ISO 17799 technical standards.

It is evident, considering the brief overview of these security standards that although, the various worldwide guidance publications reviewed in this research project does focus on specific issues of the corporate governance, there are both similarities and differences between them. What is missing in one may be well addressed in the other; hence the importance of combining them to obtain a more balanced information technology infrastructure is revealed.

Table 1 illustrates a summarized comparison between these standards to prove the necessity of combining these standards based on the above discussion.

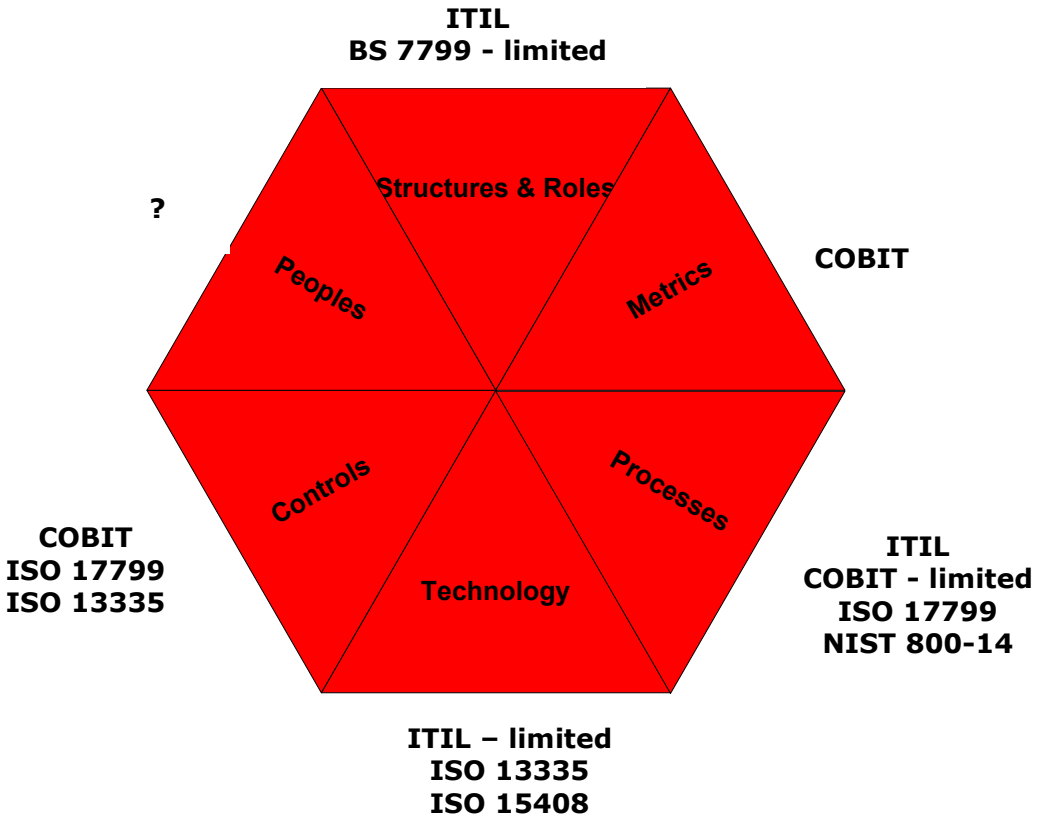
Table -1- Summarized Security standards comparison

ISO 17799	***ITIL***	***COBIT***	***NIST 800-14***	***ISO 13335***	***ISO 15408***
Provides security controls but does not define "how"	Provides IT processes, but is not strong in security	Provides IT controls and IT metrics, but is not strong in security	Provides IT security management but is not strong in the technology aspect	Provides IT Technical security controls but is not strong in "how"	Provides IT Technical security but does not address the whole IT infrastructure
To be used to improve security processes and controls	To be used as the delivery mechanism, where it describes "how"	To be used as the delivery where it describes "what"	To be used to improve security processes	To be used for the guidance of IT security management	To be used to improve the technology aspect

Source: Bisson & Saint-Rene, 2003.

It can be concluded that to implement sound IT governance which is subset of corporate governance, it is necessary to consider other standards publications. These provide more stringent specifications for a particular IT security area in order to fulfill the gap left by ISO 17799. The synergy of combining these frameworks can be substantial (Von Solms, 2005). The popularity of BS 7799-2 / ISO 17799 is due in part to its flexibility and its intersection with other information and IT security standards (Bisson, & Saint-Rene, 2003). Figure 10 illustrates ISO 17799 complementarity with other existing security standards.

Figure -10- Complementarity of ISO 17799 with other security standards



Conradie & Hoekstra, 2002: PriceWaterHouseCoopers

Executive Management as shown in Figure 10 can choose a combination of security standards based on the needed IT goals. At this stage, it is important to highlight that when using more than one standard, a mapping between the chosen standards is critical to ensure no duplication of efforts occurs. A recent report by the IT Governance Institute solves this problem, by providing a detailed mapping between the Detailed Controls Objectives of COBIT and ISO 17799 (COBIT Mapping: Mapping of ISO 17799 with COBIT) (ITGI, 2004).

The necessity of combination of security practices can be critical especially in a healthcare environment where healthcare organizations have more stringent security and privacy requirements that are not covered by ISO 17799. It is stated in ISO/IEC 17799, "this code of practice may be used as a starting point for developing organization-specific guidance, with particular emphasis on the fact that not all the guidance and controls in the code may be applicable to each organization. Conversely, additional controls not included in the code of practice

document may be required" (ISO17799, 2000). Additionally, it is crucial to mention that ISO 17799 as a code of practice for Information Security Management has a limited coverage for privacy of health information which is one the main targets of this project. This confirms the need for complementing the ISO 17799 standard with other practices specifically dealing with ensuring the security and privacy of health information.

It can be concluded that using ISO 17799 in managing Information Security can not stand alone and needs to be supported by other security standards and practices. The increase of stringent healthcare security standard means the need of complementing ISO 17799 in a healthcare environment becomes a necessity but not a choice.

The next section will describe the various security practices that healthcare Executive Management should take into account in addition to ISO 17799 to create a balanced healthcare Information Security program.

3.4 HEALTHCARE INFORMATION SECURITY STANDARDS AND BEST PRACTICES

The healthcare industry is as competitive and multifaceted as any industry in the world today. The healthcare information system provides many advantages when used for improved access, collaboration and data sharing among healthcare providers, patients, and researchers (Zhang et all, 2002). Therefore, it is obvious that there is a need of ensuring that such information is kept secure.

The recent trends of a rapid implementation of the enterprise-wide information and communication technology in healthcare and wide-area health information sharing around the world requires an increased interoperability among different information systems (Yun Sik Kwak, 2004). This increase of sharing electronic health information means a lot of attention has been directed in this arena to ensure that health information is kept secure and private during normal daily transactions.

The assurance of an appropriate and consistent level of Information Security for computer-based patient records, both within individual healthcare organizations and throughout the entire healthcare delivery system, requires organizations entrusted with healthcare information to establish formal Information Security programs (CPRI toolkit, 1995).

The importance of Information Security in managing computer-based patient records is recognized. There are numerous healthcare standards, some recognized at the international level, others developed by government agencies, public and private security practitioners. Nevertheless, it is not the intention of this project to review all of them as it is beyond the scope of this project. The main intention is to inform healthcare executives of their existence and thus, provide them with more choice for achieving best business practices in managing healthcare information systems.

The next section briefly discusses the health informatics international standards namely ISO TC 215, CEN/TC 215 activities and other security practices developed by different governmental bodies and other public and private organizations.

3.4.1 International Standards

Healthcare informatics is a dynamic area characterized by changing business and clinical processes, functions, and technologies. The effort to create healthcare informatics standards is equally dynamic (Blair). There are an increasing number of international healthcare standards but most of them are not security related. Some deal with Identifiers standards; Communications standards developed by Institute of Electrical and Electronic Engineers (IEEE) and Digital Imaging and Communications in Medicine (DICOM); and Content and Structure standards developed by Health Level 7 (HL7). Those which deal with ensuring the privacy and security of health information are ISO/TC 215 and CEN/TC 215. These are discussed in this project.

3.4.1.1 ISO/TC 215- Health informatics

The International Organization of Standardization (ISO) Technical Committee (TC) 215, Health Informatics was established to develop and harmonize International Standards (IS) for health informatics in 1998. The ISO TC 215 consists of 25 'P' (Participating: Europe-15, Asia-4, N. America-2, Oceania-2, Africa-2) and 14 'O' (Observer: Europe-6, Asia-5, S America-1, C. America-1, Africa-1) member bodies. The P-member body must provide experts in developing IS. It is important to note that South Africa is one of the two Participating African countries members.

The scope of TC 215 deals with the standardization in the field of information for health and health ICT to achieve compatibility and interoperability between

independent systems. Its purpose is to ensure compatibility of data for comparative statistical purpose (e.g. classifications), and to reduce duplication of effort and redundancies (ISO TC 215). The TC has published eight standards to date. Currently, there are approximately 75 standards under development in which a broad representation of current paradigm and multi-culture requirements have been met by the development processes. ISO TC 215 comprises five working groups:

a. ISO/TC 215 WG 1: Health Informatics - Health Records and Modelling Coordination

The scope of this workgroup is to develop standards to facilitate the capturing, safe communications, and trusted management of information concerning the total health process applied to one subject of care for individual and public health purposes. It coordinates the modeling of other relevant standards efforts such as those regarding terminology, messaging, and security (ISO/TC 215 Working group 1).

b. ISO/TC 215 WG 2: Health Informatics - Messaging and communication

This workgroup is concerned with a means of implementing the interchange in one or more syntax or communication modalities in clinical messaging, Medical device communication and business financial messaging (ISO/TC 215 Working group 2).

c. ISO/TC 215 WG 3: : Health Informatics - Health Concept and Representation

This workgroup focuses on the development of standards for representation of health concepts. These standards include formal models of representation and the description of health concepts; the principles of their organization within terminologies and their related systems (including controlled clinical terminologies and classifications); and issues concerning the context of their use in electronic health records (ISO/TC 215 Working group 3).

d. ISO/TC 215 WG 4: Health Informatics - Security

This workgroup focuses on defining standards for technical measures to protect and enhance the confidentiality, availability, and integrity of health information,

and the accountability of users, and the guidelines for security management in healthcare (ISO/TC 215 Working group 4).

e. ISO/TC 215 WG 5: Health Informatics – Health Cards

The scope of this workgroup is to develop standards in the field of healthcare usage of machine readable cards compliant with physical characteristics, including the dimensions defined in ISO/IEC 7810, Identification cards – Physical characteristics. The WG shall place special emphasis on standards of technology-independent data structures leading to interoperability and compatibility including the communication of data (ISO/TC 215 Working group 5).

The standards or guides published by ISO/TC 215 as found on the ISO general web site (www.iso.ch) or ISO/TC 215 home page (www.iso.ch/sdis) include the following:

- TS 17090-1:2002 Health Informatics – PKI framework and overview;
- TS 17090-2:2002 Health Informatics – PKI certificate profile;
- TS 17090-3:2002 Health Informatics – PKI management of certificate authority;
- TS 17117 :2002 Health Informatics – Controlled health term structure and high-level indicators;
- ISO/DIS 22857- Health informatics: Guidelines on data protection to facilitate trans-border flows of personal health information;
- TR 18307: 2001- Health informatics interoperability and common messaging and communication standards – Key characteristics;
- TS 18308:2004 Health informatics requirements for an electronic medical record architecture;
- ISO 18812 :2003 Health Informatics – Clinical analyser interfacing information system.

The ISO/TC 215 publication standards, is most interesting because it deals with security management is the ISO/DIS 22857 - Health informatics: Guidelines on data protection to facilitate trans-border flows of personal health information. It will be examined in the following section.

3.4.1.2 ISO 22857 - Health informatics: Guidelines on data protection to facilitate trans-border flows of personal health information

The ISO 22857:2004 provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders. This standard was developed by ISO/TC 215 WG4 and published 2004. It does not require the harmonization of existing national standards, legislation or regulations. It is normative only in respect of international exchange of personal health data. However, it may be informative with respect to the protection of health information within national boundaries and provide assistance to national bodies involved in the development and implementation of data protection principles. The standard covers both the data protection principles that should apply to international transfers and the security policy which an organization should adopt to ensure compliance with those principles (ISO 22857).

This International standard aims to facilitate international health-related applications involving the transfer of personal health data. It seeks to provide the means by which data subjects, such as patients, may be assured that their health data will be adequately protected when sent to, and processed in, another country.

This International standard does not provide definitive legal advice but comprises guidance. Legal advice appropriate to the application should be sought when applying the guidance to it. National privacy and data protection requirements vary substantially and can change relatively quickly. The standard in general encompasses the more stringent of international and national requirements, it nevertheless comprises a minimum. Some countries may have more stringent and particular requirements, and this should be checked (ISO 22857).

The ISO/TC 215 is currently busy developing ISO/NP 27799 Health Informatics – Security management in health using ISO/IEC 17799 with the prediction of publication date of 2007. It can be assumed that once this standard is available, it will receive much acclaim especially for healthcare organizations using ISO 17799 who are willing to incorporate more stringent security management.

3.4.1.3 CEN/TC 251 Health Informatics

The Comitté Europeen de Normalisation (CEN) is a European standards organization with 16 TCs. Two TCs are specifically involved in health care: TC 251 (Medical Informatics) and TC 224 WG12 (Patient Data Cards). The Technical Board of the European Standardization Committee (CEN/BT) approved the establishment of a Technical Committee for Medical Informatics (TC251) in March 1990. CEN/TC 215 is responsible for organizing and coordinating standards development in healthcare environment informatics and telematics at the European level (Waegemann, 1995). The CEN TC 251 on Medical Informatics includes work groups on: Modeling of Medical Records; Terminology, Coding, Semantics, and Knowledge Bases; Communications and Messages; Imaging and Multimedia; Medical Devices; and Security, Privacy, Quality, and Safety. The CEN TC 251 has established coordination with healthcare standards development in the United States through ANSI.

The scope of this standard deals with the standardization in the field of Health Information and Communications Technology (ICT) and is aimed at achieving compatibility and interoperability between independent systems. This includes requirements on the structure of health information to support clinical and administrative procedures, technical methods to support interoperable systems and requirements regarding safety, security and quality of health information (Klein, 2002). Its scope is very similar to that of the more recently formed ISO/TC 215 committee, which largely covers the same ground, but has emphasized the objective to not always develop new specifications but rather to endorse solutions developed by other bodies (Klein, 2002).

3.4.2 Government Agencies and other organizations

The development of computer-based patient record systems and healthcare information networks has created the need for more definitive confidentiality, data security, and authentication guidelines and standards (Blair, 2002). In addition to the international healthcare security standard, many organizations and other public or private organizations have developed numerous healthcare standards. It is not the intention of this project to mention all these standards as it is beyond the scope of this project.

The next section gives an overview of some of the more recognized security standards developed by various government and other competent bodies.

3.4.2.1 National Institute of Standards and Technology (NIST)

NIST was founded in 1901. It is a non-regulatory federal agency within the Technology Administration of the Commerce Department of the US. Its mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade and improve the quality of life. Numerous guidance can be freely downloaded at the NIST website (NIST, 1901). Among these documents are the NIST special publication 800-series, which can be particularly useful for organizations implementing Information Security Management.

NIST has shown interest in the health sector, which confirmed by the publication of NIST Special Publication 800-66 document. This Special Publication (SP) summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This SP helps educate readers about security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security safeguards set out in the Rule. It is designed to direct readers to helpful information in other National Institute of Standards and Technology (NIST 800-66) publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publications for consideration while implementing the Security Rule. Nevertheless, it is explained that this publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule and does not supplement, replace or supersede the HIPAA Security Rule itself (NIST, 800-66).

3.4.2.2 Center for Medicare and Medical Services (CMMS)

The Center for Medicare and Medical Services (CMMS) published HIPAA regulations standards for the security of electronic health information. It specifies a series of administrative, technical and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information (CMMS). The regulatory requirements are delineated into either required or addressable implementation specifications. These requirements are discussed in more detail in Chapter 4 which describes the legal and regulation requirements related to the healthcare environment.

3.4.2.3 Computer-based Patient Record Institute (CPRI)

The Computer-based Patient Record Institute (CPRI) is an organization of public and private entities that promotes the use of electronic health records. CPRI has recognized the importance of providing for Information Security in the implementation of computer-based patient records and has established the Work Group on Confidentiality, Privacy and Security. The Work Group was chartered to encourage the creation of policies and mechanisms to protect patient and caregiver privacy and to ensure information security. The Work Group is developing a series of security guidelines for organizations implementing electronic medical record systems as part of its efforts.

Products issued to date include guidelines for establishing Information Security policies, establishing Information Security education programs, managing Information Security programs, and establishing confidentiality statements and agreements. It has also developed a guide to security features for health information systems (CPRI toolkit, 1995).

CPRI has performed extensive work in the area of security for organizations using computer-based patient records such as:

- CPRI- Guidelines for Establishing healthcare Information Security Policies;
- CPRI- Guidelines for Information Security Education Programs;
- CPRI- Sample Confidentiality Statements and Agreements;
- CPRI- Security Features for Computer-based Patient Record Systems.

3.4.2.4 National Research Council (NRC)

The National Library of Medicine, as the one of the leading agencies within the United States government for facilitating healthcare applications of the national information infrastructure, identified in 1995 privacy and security as primary issues that needed to be addressed to facilitate greater use of IT within healthcare (CPRI toolkit, 1995). The National Research Council (NRC) initiated a study to observe and assess existing technical and non technical mechanisms for protecting the privacy and maintaining the security of healthcare information systems. The report of the findings and several security procedures were published by the National Research Council in 1997 in the book entitled "For the Record: Protecting Electronic Health Information".

The book contains an analysis of the state of healthcare security in place at several leading healthcare organizations. Chapter six provided recommendations for current and future healthcare security practices, which served as the foundation for the Department of Health and Human Services (DHHS) which proposed substantial efforts in the development of HIPAA Security Standard (NRC, 1997).

3.4.2.5 American Health Information Management Association (AHIMA)

The American Health Information Management Association (AHIMA) is the organization of health information management professionals. Health information management professionals have long focused on protecting the confidentiality of patient information (AHIMA) as the official custodians of medical records and health information within healthcare providers. AHIMA has developed a number of practices on (NRC, 1997):

- Authentication of Medical Record Entries;
- Confidential Health Information and the Internet;
- Destruction of Patient Health Information;
- Disaster Planning for Health Information;
- Disclosure of Health Information;
- Electronic Signatures;
- E-Mail Security;
- Facsimile Transmission of Health Information;
- Managing Health Information Relating to Infection with HIV;
- Managing Multimedia Medical Records;
- Patient Anonymity;
- Patient Photography, Videotaping, and Other Imaging;
- Protecting Patient Information after a Closure;
- Release of Information Laws and Regulations (by State);
- Release of Information for Marketing Purposes.

3.4.2.6 American Society for Testing and Materials (ASTM committee E31 - Healthcare Informatics)

The American Society for Testing and Materials (ASTM), organized in 1898, has grown into one of the largest voluntary standards development systems in the world. ASTM is a non-profit organization that provides a forum for producers,

users, ultimate consumers and those having a general interest (representatives of government and academia) to meet on common ground and write standards for materials, products, systems and services.

The ASTM, Committee E31 - Healthcare Informatics includes subcommittees addressing privacy (E31.17) and data and system security (E31.20). These committees have produced the following standards (CPRI toolkit, 1995):

- ASTM E1762 - Standard Guide for Electronic Authentication of healthcare Information;
- ASTM E1869 - Standard Guide for Confidentiality, Privacy, Access and Data Security Principles for Health Information Including Computer-Based Patient Records;
- ASTM E1902 - Standard Guide for the Management of the Confidentiality and Security of Dictation, Transcription, and Transcribed Health Records;
- ASTM PS100-97 - Provisional Standard Specification for Authentication of Healthcare Information Using Digital Signatures;
- ASTM PS101-97 - Provisional Standard Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information;
- ASTM E2017-99 —Standard Guide for Amendments to Health Information
- ASTM PS115-99 - Provisional Standard Specification for Security Audit and Disclosure Logs for Use in Health Information Systems;
- ASTM E1986-98 - Standard for Information Access Privileges to Health Information;
- ASTM E1987-98 - Standard Guide for Individual Rights Regarding Health Information;
- ASTM E1988-98 - Standard Guide for the Training of Persons Who Have Access to Health Information;
- ASTM Draft Standard Specification for Transmission of Healthcare Information Using Secure Messaging Protocols.

It can be summarized that currently, there is an increasing number of healthcare organization bodies ranging from international, governmental and private bodies. An awareness of the activities of these organizations can have incredible benefits. This can be noticeable, for example, in benchmarking. The organization typically benchmarks by selecting a measure with which to compare itself against the other organization in its market. It helps to highlight the gaps where more efforts are needed by measuring the difference between the ways the organization conducts its business in relation with the others.

It is necessary to ensure that should the organization decide to use the practices adopted by others, they should make sure that they face the same challenges of security requirements. What worked well from one organization might not work the same for the other and vice-versa. Therefore, the conducting of a risk analysis specifically drives the whole process of implementing the security solution.

3.5 CONCLUSION

Information is recognized as the "life blood" of any business and destroying this information is the same as killing the business. Hence, information needs to be protected and kept secure. Technical approaches are not sufficient. There can be not effective protection without a systematic management of information. ISO 17799 is an international standard that can serve as basis for Information Security Management best practice in any organization and can globally be communicated.

Certification with BS7799-2 will especially help those healthcare organizations who want to demonstrate to customers and other stakeholders that confidentiality; integrity and availability are always ensured. This in turn increases trust between business partners.

It is crucial to emphasize that ISO 17799 can not stand alone and it may be necessary to support it by more stringent and specific standards.

This chapter has shown that Healthcare Executives are required to incorporate healthcare security standard and practices as part of ensuring trust between their business partners and customers. However, proper Information Security Management practices alone do not necessarily ensure regulatory compliance and vice versa (Tuyikeze & Pottas, 2005). Healthcare Executive Management must be alert to reduce possible losses from any legal action. They must understand the current legal environment, stay abreast of new laws and regulations, and observe new issues as they emerge. **Chapter 4** clearly discusses the legal and regulatory requirements pertaining to the South African health sector.

Chapter 4 LEGAL AND REGULATION REQUIREMENTS PERTAINING TO PRIVACY AND DATA PROTECTION

The issue of information privacy is becoming part of the public debate and it is important to understand the substantial body of legal requirements already in place and evaluate the extent to which these rules address consumer concerns regarding the protection of their information.

The main objective of **Chapter 4** is to discuss data and privacy protection legislation on an international and national level to set the requirements needed to protect the personal privacy and health information of an individual. This is narrowed down to look at privacy protection in the Republic of South Africa and specifically in the health sector which constitutes the main objective of this project.

Chapter 5 is dedicated to the comparison between an ISM framework (ISO 17799) and the HIPAA, SANHA and ECTA regulations requirements.

"Privacy isn't a technology issue; it's a social issue. And there is a need for companies to really help consumers protect information – not just because it's the right thing to do, but because it's also good business. If a company doesn't earn the respect of its customers by respecting their privacy, those customers won't come back."

-HARRIET PEARSON, CHIEF PRIVACY OFFICER IBM CORPORATION-

4.1 INTRODUCTION

The growing value of information about individuals held by companies has become such a powerful and commercial asset that is doubtful whether companies still respect the privacy of the individual. The problem is that the processing of the information of individuals may occur without their knowledge and even without their being able to control what is stored, processed, sold or distributed. This truly questions the right of the individual to protect their personal privacy.

Privacy is a valuable aspect of personality (SALC, 2003). Sociologists and psychologists agree that a person has a fundamental need for privacy. It is clear that the individual has an interest in the protection of his or her privacy. The right of a person to privacy according to Neethling (1996), entails that such person should have control over their personal information and should be able to conduct their personal information affairs relatively free from unwanted intrusions. This is not easy with the expansion in the use of electronic commerce and technological environment that enables such information to be available to various business partners.

The keepers of the information of an individual can argue that they maintain tight security and privacy over this data. However, most often these controls benefit the keepers and provide little protection to the individual (Oberholzer, 2001). Therefore, there is a need to enhance such privacy protection to increase the trust between customers and the organizations dealing with their information.

"Privacy is not a solely a risk issue. Nor is it only an operational issue. It has become a strategic business issue that is holistic. And one that needs to be

applied enterprise-wide. If you do it right, its impact on customer trust can be enormous, and trust is ultimately the catalyst for trade" (KPMG, 2001). There is a need to ensure protection of such critical organization asset namely privacy.

Since antiquity, respect for patient privacy has been affirmed as professional responsibility of physicians (Smith, 2004). In the famous oath attributed to Hippocrates, ancient Greek physicians pledged to respect confidentiality in these words: "What I may see or hear in the course of the treatment or even outside of the treatment in the regard to the life of men, which on no account one must spread aboard, I will keep to my self, holding such things shameful to be spoken about" (Oath of Hippocrates, 1995). The Declaration of Geneva of the World Medical Association (1995) goes further in ensuring privacy of patient information. It contains the statement "I will respect the secrets which are confided in me, even when the patient has died". Today, the Oath by itself is no longer sufficient and is extended by international and national laws.

Countries have started to develop various data protection laws with the main objective of regulating these practices to ensure data and privacy protection. The first law was enacted in the Land of Hesse in Germany in 1970 (SALC, 2003). This was followed by national standards in Sweden in 1973, the United States in 1974, Germany in 1977, and France in 1978 (Flaherty, 1989). Currently, the adoption of these laws has increased in most countries. It was recognized early that information privacy could not simply be regarded as a domestic policy problem (SALC, 2003). The increasing ease with which personal data could be transmitted outside the borders of its country of origin produced an interesting history of international harmonization efforts and concomitant effort to regulate trans-border data flows (SALC, 2003). Therefore, it was necessary to have international laws governing such information.

4.2 INTERNATIONAL PRIVACY LEGISLATION

The information privacy movement from the early eighties saw the release of two crucial international documents:

- The 1981 **Organization for Economic Cooperation and Development** (OECD) Guidelines governing the protection of Privacy and Trans-border Data Flows of Personal Data;
- The **Council of Europe's 1981 Convention** for the protection of individuals with regard to the automatic processing of personal data.

4.2.1 Organization for Economic Cooperation and Development Guidelines on privacy and trans-border flows of personal data

The Organization for Economic Cooperation and Development (OECD), during the late seventies, perceived "a danger that disparities in national legislation could hamper the free flow of personal data across frontiers… Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and medical health transactions" (OECD, 1981). In 1980 the OECD approved and started applying some guidelines concerning the privacy of personal data.

The OECD guidelines, although broad, set up important standards for future government privacy rules. These guidelines support most current international agreements, national laws and self-regulatory policies. The guidelines were voluntary, however roughly half of OECD member-nations had already passed or proposed privacy-protecting legislation by 1980. 182 Americans companies claimed, by 1982, to have adopted the guidelines, although very few ever implemented practices that directly matched the standards.

The objectives of the OECD guidelines are as follows:

i. OECD member countries will accept certain minimum standards on the protection of privacy and individual liberties with regard to personal data;
ii. OECD member countries will reduce differences between relevant domestic rules and practices of member countries to a minimum;
iii. OECD member countries will take into consideration the interests of other member countries and the need to avoid undue interference with flows of personal data between member countries in protecting personal data;
iv. OECD member countries will restrict trans-border flows of personal data due to the possible risks associated with such flows.

The OECD (1980) has set up principles that should be followed to enforce these guidelines. The OECD (1980) defines personal data as "data conveying information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person".

It is important however to note that the OECD guidelines do not set out requirements as to how these principles are to be enforced by member nations.

Resultantly, OECD member countries have chosen a range of differing measures to implement the privacy principles. These principles provide basic ideas to other countries which are not OECD member into setting national laws aimed at protecting personal information. It can be argued that they are considered as universal best practices principles.

4.2.2 COE Convention on automatic processing of personal data

The Council of Europe came into being in on 1 October 1985. The main purpose of this convention was to ensure the protection of individuals with regard to automatic processing of personal data. The key principles are based on the OECD guidelines. Member countries were required to approve the convention by passing their own legislation, which has since been done by many Europeans countries.

The Convention defines personal data as "data that reveals racial origin, political or religious opinions or other beliefs, as well as personal data concerning health or sexual life" (COE, 1985). Additionally, it states that such personal data should be (COE, 1985):

1. Obtained fairly and processed lawfully;
2. Used only for the specified purpose for which it was originally obtained;
3. Adequate, relevant and not excessive to the purpose;
4. Accurate and up to date;
5. Accessible to the subject;
6. Kept secure;
7. Destroyed after its purpose is completed.

These principles are known as the **Principles of Data Protection** and form the basis of both legislative regulations and self-regulating control.

The COE and OECD instruments cover the same basic areas of activities but they represent differing philosophies as to the nature of the problem and the appropriate legal response. The European model, in particular, sees the establishment of a specialized supervisory agency as critical, while the OECD guidelines have been strongly influenced by the United States which tends to rely upon the courts as the primary mechanisms of enforcement of legal rights (SALC, 2003).

These crucial international instruments have had a profound effect on the enactment of national laws around the world, even outside the OECD member countries. They incorporate technologically neutral principles relating to the collection, retention and use of personal information.

There is an increase in the interconnection of computer systems and communication technology, and the Trans-border Data Flow (TDF) allows the free flow of information between different countries (Oberholzer, 2001). These TDF provide a framework to protect the privacy of the individual while advancing the free flow of data internationally. An OECD member country can refuse to transfer personal data internationally to another receiving country that does not have comparable protection laws (OECD, 1980). Such refusal will impact the country the economic sector of the country because of interruptions to the international flow of data (Caroline, 2004). Privacy is therefore an important trade issue, as data privacy concerns can create a barrier to international trade (Caroline, 2004). It becomes necessary to understand the various models aimed at the protection of personal information.

4.3 DATA PROTECTION MODELS

Depending on the application of these data protection models, they can be complementary or contradictory. Several are used simultaneously in most countries. All the models are used together to ensure data protection in the countries that are willing to protect privacy most effectively.

The models are described in the Electronic Privacy Information Center Report 2002 (EPIC, 2002). The Electronic Privacy Information Center is a public interest research centre in Washington, DC., established in 1994. EPIC focuses public attention on the protection of privacy besides other issues. Some of the valuable services offered by EPIC are its On-line Guide to Practical Privacy Tools, On-line Guide to Privacy Resources and a dictionary on Privacy. These data protection models are described by the South African Law Commission (SALC, 2003) with the objective of conducting an investigation into privacy and data protection in South Africa. These models are examined next:

4.3.1 Comprehensive laws

There is a general law that governs the collection, use and dissemination of personal information by both the public and private sectors in many countries

around the world. An oversight body ensures compliance. This is the preferred model for most countries adopting data protecting laws and was adopted by the European Union to ensure compliance with its data protection regime. A variation of these laws, which is described as a co-regulatory model, was adopted in Canada and Australia. This approach requires industry to develop rules for the protection of privacy that are enforced by the industry and overseen by the private agency (EPIC, 2002).

4.3.2 Sectoral laws

Some countries, such as the United States, have avoided enacting general data protection rules in favor of specific sectoral laws governing for example, video rental records and financial privacy. In such cases, enforcement is achieved through a range of mechanisms. A major drawback with this approach is that it requires the new legislation to be introduced with each new technology - protection frequently lags behind. The lack of legal protection for individual privacy on the Internet in the USA is a striking example of its limitations. There is the problem of the absence of an oversight agency. In many countries, sectoral laws are used to complement comprehensive legislation by providing more detailed protection for certain categories of information, such as telecommunications, police files or consumer credit records (SALC, 2003).

4.3.3 Self-regulation

Data protection can be achieved - at least in theory - through various forms of self-regulation, in which companies and industry bodies establish codes of practice and engage in self-policing. However, in many countries, especially the United States, these efforts have been disappointing, with little evidence that the aims of the codes are regularly fulfilled. Adequacy and enforcement are the major problem with these approaches. Industry codes in many countries have tended to provide only weak protection and lack enforcement. This is currently the policy promoted by the governments of the United States and Singapore (EPIC, 2002).

4.3.4 Technology

Data protection has moved into the hands of individual users with the recent development of commercially available technology-based systems. Users of the Internet and some physical applications can employ a range of programs and

systems that provide varying degrees of privacy and security of communications. These include encryption, anonymous remailers, proxy servers and digital cash.52 Users should be aware that not all tools are effective in protecting data privacy. Some are poorly designed while others are designed to facilitate law enforcement access (SALC, 2003).

4.4 PRIVACY LEGISLATION IN THE REPUBLIC OF SOUTH AFRICA

Privacy legislation in the Republic of South Africa is still in its early stages. The following is a time frame indicating the progress made on privacy legislation in RSA:

1. October 1994 - Initiate the establishment of the Open Democracy Act
2. December 1996 - South African Constitution (referencing privacy very briefly)
3. July 1998 - Open Democracy Bill, No 67
4. November 1999 - Data protection provisions from Open Democracy Bill
5. January 2000 - Green Paper on Electronic Commerce for South Africa
6. July 2002 - Electronic Communication Transaction Act (referencing privacy very briefly)
7. July 2004 - South African National Health Act (referencing privacy very briefly)

The right to privacy in South Africa is protected in terms of both the common law and the South African Constitution of 1996. The Constitution states in the Bill of Rights (Section 14 on privacy):

"Everyone has the right to privacy, which includes the right not to have:

a) their person or home searched;
b) their property searched;
c) their possession seized; or
d) their privacy of their communication infringed"

Section 32 on Access to Information states that:

I. "Everyone has the right of access to:
    a. any information held by state, and;

b. any information that is held by another person and that is required for the exercise or protection of any rights;

II. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state" (Constitution of the Republic of South Africa, 1996).

It is important to note that in RSA, apart from the Constitution itself, there is no legislation which deals specifically and fully with data protection. In view of the extent and seriousness of the threat to the personality of the individual, it is surprising to find that in South African legal system – unlike many other Western legal systems – measures for the protection of the individual (data protection) have not yet been enacted (SALC, 2003).

It should be noted that privacy and data protection are briefly referred to in some of the South Africa laws:

a. The **Promotion of Access to Information Act** (PAIA): recognizes the data protection principle that personal information should be accessible to the subject (PAIA, 2000);
b. The **South African National Health Act** (SANHA): provides that every patient is entitled to confidentiality of all health information, including health status, treatment or stay in a private or public establishment. This information is only to be disclosed if the user consents in writing or if a law or a court order authorizes the disclosure (SANHA, 2004);
c. The **Electronic Communication Transaction Act** (ECTA): ensures that protection of personal information that has been obtained through electronic transactions (ECTA, 2002).

The ECTA and PAIA have interim provisions dealing, respectively, with the correction of data and voluntary adherence to data protection principles. These sections are regarded as interim measures until specific data privacy legislation has been finalised (SALC, 2003). The above mentioned laws are further discussed in the next section.

Information privacy or data legislation will ensure the future participation of South Africa in the information market considering the international trends and expectations, if the country is regarded as providing adequate data protection by international standards (SALC, 2003).

The privacy and data protection becomes more important when dealing with medical information. The importance of health information is realized, and many countries have adopted different legislations and regulation frameworks ensuring its protection. The following section provides a discussion of those legal frameworks related to the South African health sector.

4.5 LEGAL AND LEGISLATION PERTAINING TO SOUTH AFRICAN HEALTH SECTOR

The healthcare industry is undergoing a radical revolution through the rapid adoption of IT solutions to meet the challenges of regulatory burdens, cost reduction and patient care. Some of these IT solutions include computerized physician order-entry initiatives, electronic medical records and electronic claims processing.

Medical data are considered to be amongst the most sensitive data for civil use because they contain detailed, personal information about patients and their health information. For centuries, the Hippocratic Oath has expressed the duty of the physicians to respect privacy of the patients. Today, this is no longer sufficient and is extended by legal and regulatory requirements of governments.

South African healthcare organizations must ensure that they comply with the South African National Health Act (SANHA), the Electronic Communication Transaction Act (ECTA) requirements, and Promotion of Access to Information Act (PAIA) to ensure due care and due diligence practices.

It is arguably necessary to consider adopting the Health Insurance Portability and Accountability Act (HIPAA) to incorporate best practices for protecting privacy and security of health information in addition of meeting with these laws frameworks requirements. This will ensure that healthcare organizations are meeting regulatory requirements while ensuring customers receive best practices for the security and privacy of health information. The following sections provide a discussion of these legislation frameworks.

4.5.1 South African National Health Act (SANHA)

The South Africa National Health Act (SANHA) or Act 61 of 2003 was signed into Act by the South African President Thabo Mbeki on 18 July 2004. SANHA provides a framework for a structured, uniform health system to unite the various

elements of the national health system, in a common goal, to improve universal access to quality health services (SANHA). A briefing media on the National Health Act by the Minister of Health Dr Manto Tshabalala-Msimang, highlighted that this act rests heavily on the Constitution with 50 sections of it relating directly to what is covered in this act. Section 27(2) of the Constitution, asserts that the State must take reasonable legislative and other measures to progressively achieve the right of access to healthcare services and reproductive health care, within its available resources.

The South African National Health Act is composed of 12 chapters. The following provides a brief description of those chapters:

I. **Chapter 1.** "Objects of Act, responsibility for health and eligibility for free health services" It gives the Minister of Health stewardship over the National Health System and the responsibility to protect, promote and maintain the health of the population;
II. **Chapter 2.** "Rights and duties of users and healthcare personnel" gives emphasis to some rights of every citizen;
III. **Chapter 3.** "National Health" describes the general functions of the national Department of Health and the Director General;
IV. **Chapter 4.** "Provincial Health" establishes provincial health services and outlines the general functions of provincial health departments;
V. **Chapter 5.** "District Health System for Republic" establishes the District Health System based on the principles of primary health care, promoting universal access to quality, equitable, responsive and efficient healthcare services that are accountable to the communities they serve;
VI. **Chapter 6.** "Health establishment" deals with one of the most interesting and innovative elements of the Act. The classification of health establishments, the certificate of need, the establishment of boards for hospitals, clinics and community health centres, the relationship between the public and private health establishments;
VII. **Chapter 7.** "Humans resources planning and academic health complexes" The Act mandates the National Department to develop a human resources policy and guidelines to ensure adequate distribution of health personnel; to provide for trained staff at all levels of the health system and to ensure the effective utilisation of health personnel;

VIII. **Chapter 8.** "Control of use of blood, blood products, tissue and gametes in humans" deals with complex issues such as the control and use of blood, blood products, tissue and gametes in humans;

IX. **Chapter 9.** "National Health Research and Information". The Act provides for the establishment of a National Health Research Ethics Council and Health Research Ethics Committees at every institution, health agency and health establishment at which health research is conducted;

X. **Chapter 10.** "Health officers and compliance procedures" requires the establishment of health officers responsible for the inspection of standards of compliance;

XI. **Chapter 11.** "Regulations" empowers the minister to make regulations on various issues covered in this Act;

XII. **Chapter 12.** "General provisions" empowers the Minister to appoint advisory and technical committees, to assign duties and delegate powers and to prescribe transitional arrangements as may be necessary.

This project will only deal with Chapter 2 section 17 ("Protection of health records") of this Act because it highlights the right to confidentiality and access to health records related issues.

4.5.2 Electronic Communication and Transaction Act (ECTA)

The Electronic Communication and Transaction Act (ECTA), or Act No.25 of 2002 was signed into Act by the South African President Thabo Mbeki on 31 July 2002 and came into effect on Friday, 30 August 2002. This marked the end of a process initiated by the South African Government in 1999 to establish a formal structure to define, develop, regulate and govern e-commerce in South Africa.

It is the first South African law governing cyber activity and the ECTA facilitates the development and propagation of electronic communications and transactions within South Africa and aims to promote consumer confidence in electronic transacting and online privacy (ECTA, 2002).

The main objectives of the ECTA (2002) include:

- "To provide the facilitation and regulation of electronic communications and transactions;
- To provide for the development of a national e-strategy for the Republic;
- To promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs;

- To provide for human resource development in electronic transactions;
- To prevent the abuse of information systems;
- To encourage the use of e-government services;
- And to provide for matters connected therewith".

With the increased use of electronic communication transactions in healthcare business transactions, the ECTA places a heavy burden on medical providers, insurers and claims clearinghouses and other healthcare services partners who need to communicate electronically on daily basis to accomplish their tasks. The ECTA is expected to facilitate electronic interchange relating to healthcare business transactions, for example, order-placement and processing, shipping and receiving, invoicing, payment, cash application data, insurance transactions, and other data associated with the provision of products and health services.

The ECTA is composed of 14 chapters with 95 sections. The following is a brief description of each chapter:

I. **Chapter 1.** "Interpretation, Objects and Application" defines critical words and phrases and sets out the main objects of the Act;
II. **Chapter 2.** "Maximising Benefits and policy frameworks" maximises the benefits the Internet offers by promoting universal access in under-serviced areas and ensuring that the special needs of particular communities, areas and the disabled are duly taken into account;
III. **Chapter 3.** "Facilitating Electronic Transactions" deals with the removal of legal barriers to electronic transacting;
IV. **Chapter 4.** "E-Government Services" facilitates electronic filling. It lists the requirements for the production of electronic documents and integrity of information;
V. **Chapter 5.** "Cryptography Providers" requires the suppliers of "cryptography" services or products to register names and addresses, the names of their products with a brief description in a register maintained by the Department of Communications.
VI. **Chapter 6.** "Authentication Service Providers" aims to provide the establishment of an Accreditation Authority within the Department, allowing voluntary accreditation of electronic signature technology.
VII. **Chapter 7.** "Consumer Protection" requires vendors to provide consumers with a minimum set of information, including the price of the product or service, contact details and the right to withdraw an electronic transaction before its completion.

VIII. **Chapter 8.** "Protection of Personal Information" establishes a voluntary regime of protecting any information capable of identifying an individual. Collectors of personal information may subscribe to a set of universally accepted data protection principles.

IX. **Chapter 9.** "Protection of Critical databases" requires the registration of critical databases and ensure certain procedures and technological methods to be used in their storage and archiving.

X. **Chapter 10.** "Domain Name Authority and Administration" establishes a Domain Name Authority to assume responsibility for the .za domain name space, which must be incorporated as section 21(1) of the Companies Act, 1973 (Act No.61 of 1973).

XI. **Chapter 11.** "Limitation of Liability of Service Providers" deals with limitation of the liability of service providers or so-called "intermediaries" and creates a safe harbour for service providers who are currently exposed to a wide variety of potential liability by virtue of merely fulfilling their basic technical functions.

XII. **Chapter 12.** "Cyber Inspectors" seeks to provide for the Department of Communications cyber inspectors responsible of monitoring Internet websites in the public domain and investigate whether cryptography service providers and authentication service providers comply with the relevant provisions.

XIII. **Chapter 13.** "Cyber Crime" seeks to make the first statutory provisions on cyber crime in South African jurisprudence.

XIV. **Chapter 14.** "General Provisions" contains certain provisions which give jurisdiction of courts trying an offence in terms of this Act.

The ECTA comprises 14 chapters and 95 sections but only certain sections impact the IT business. Michalson (2004), who was a member of the team responsible for drafting the ECTA on the instructions of the Department of Communications, confirms that: "You do not need to comply with the entire Act, when one scrutinizes the ECTA, only six chapters make mention of a fine or imprisonment for those convicted of an offence under the Act". These chapters are:

- Cryptography Providers (Sec 29-32);
- Authentication Service Providers (Sec 33-40);
- Consumer Protection (Sec 42-49);
- Protection of Critical databases (Sec 52-58);
- Cyber Inspectors (Sec 80-84); Cyber Crime (Sec 85-89);
- This project will in addition look at Chapter 8 Protection of personal information which constitutes one of the major objectives of this project.

4.5.3 Promotion of Access to Information Act (PAIA)

The Promotion of Access to Information Act (Act No. 2 of 2000) was enacted in accordance with Section 32(2) of the South African Constitution. The Open Democracy Bill of 1998 included comprehensive data protection provisions but the parliamentary committee removed these provisions from the Open Democracy Bill in November 1999. The committee realized that access to information should be dealt with in a separate bill and therefore, came the idea of the enactment of the PAIA in 2000.

The PAIA gives effect to the constitutional right of access to any information held by the State and any information that is held by another person required for the exercise or protection of any rights (PAIA, 2000). The PAIA brings into effect the right to access information as laid down in the Bill of Rights of the Open Democracy Bill. Procedures are laid down for accessing information from government as well as from private bodies subject to limitations that are spelled out. South Africa does not have a privacy commission; therefore, the Human Rights Commission was constituted to enforce the bill.

The Promotion of Access to Information Act (2000) covers the following:

a. Gives effect to constitutional right of access to any information held by the state;
b. Makes available information about functions of governmental bodies to the public;
c. Provides persons with access to their personal information held by private bodies;
d. Provides for the correction of personal information held by governmental or private bodies and to regulate the use and disclosure of that information;
e. Provides for protection of persons disclosing evidence of contravention of the law;
f. Provides for measures against serious misadministration or corruption in governmental bodies;
g. Provides for matters in connection herewith.

The main objective of this Act is to give the right of access to information needed to promote or protect individual rights. This right aims to assist people in

obtaining the necessary information to enforce and protect their rights. Information is requested from a person or private institution and the requester has to show that he/she is doing so pursuant to a specific right. The person or private institution, from which the information is requested, may refuse access on a number of grounds, one of which is the protection of private/confident information (PAIA, 2000).

The PAIA does not contain a general prohibition on the disclosure of certain information. Only information considered as personal information described below should be restricted. It merely provides for mandatory grounds of non-disclosure in relation to requests under the Act. The role of privacy in the PAIA is merely a restriction on the right of access to information.

Personal information means according to the PAIA (2000):

a. Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
b. Information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
c. Any identifying number, symbol or other particular assigned to the individual;
d. The address, fingerprints or blood type of the individual;
e. Personal opinions views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
f. Correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
g. The views or opinions of another individual about the individual;
h. The views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual;
i. The name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name

itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.

This means that information requested and that is not in any respect personally identifiable may be provided if the requester shows a right to such information. This implies that the mechanism for de-identification must be secure to such an extent that identification is not possible at all. A person who complies with the procedures set out in the Act is entitled to access to the records of both public and private bodies should there be no ground upon which access can be refused in terms of the Act (Sec 11(1)). Where public bodies are concerned, a requester is entitled to the information irrespective of his or her reason for seeking it (Sec 11(3)), but when private bodies are concerned, the record has to be required for the exercise or protection of any rights. It is possible that disclosures to third parties (i.e. anyone outside of the doctor patient relationship) relating to personal information made in the absence of consent may amount to unreasonable disclosure as envisaged in the Act where it is requested by a third party from a doctor or a medical scheme.

The Section 30 of this Act is interesting. It asserts "Access to health or other records related". This section aims to ensure that provisions are taken into account regarding access to health records and the disclosure of such critical information.

4.5.4 Traditional Health Bill

The Traditional Health Bill was introduced in the Assembly as a Section 76; and published in the Government Gazette No 24751 of 14 April 2003. The main objective of this bill is "To establish the Interim Traditional Health Practitioners Council of South Africa; to provide for a regulatory framework to ensure the efficacy, safety and quality of traditional healthcare services; to provide for the management and control over the registration, training and conduct of practitioners, students and specified categories in the traditional health practitioners profession; and to provide for matters connected therewith" (Traditional Health Bill,2003). This bill is composed of the following five chapters:

A. **Chapter 1.** Definitions
B. **Chapter 2.** Establishment and Governance of Interim Traditional Health Practitioners Council of South Africa
C. **Chapter 3.** Registrar, Staff of Registration Procedures
D. **Chapter 4.** Disciplinary Inquiries and Investigation by Council
E. **Chapter 5.** General and Supplementary Provisions

In the speech on the bill of the Traditional Health Practitioners by Deputy Minister of health, Mrs Nozizwe Madlala-Routledge, she highlights that the idea of the recognition and regulation of health practitioners by law is to bring together elements of the cultures of developed world and those of Africa into the practice of medicine. She added that the intention of the Bill is to bring all traditional healers under one regulatory body. This would help prevent any harmful practices and would be no different to the criteria set for modern doctors (Nozizwe, 2004).

The notion of traditional health practice is known but, it is not easy to define it in legal terms. One of the definitions supplied for "African Traditional Medicine" by the World Health Organization Centre for Health Development is "The sum total of all knowledge and practices, whether explicable or not, used in diagnosis, prevention and elimination of physical, mental, or societal imbalance, and relying exclusively on practical experience and observation handed down from generation to generation, whether verbally or in writing" (WHO).

This definition acknowledges that there are aspects of traditional health practice that cannot always be explained in terms of medical science but that this does not necessarily detract from their validity or value in caring for the health and wellbeing of people.

It can be difficult to estimate how many South Africans make use of traditional healers and how many traditional healers practice their trade as some are not officially recognized and some do not possess the technology facilities to register their patients. However, it is important to note that, there have been an increasing number of people interested in traditional medicine.

The World Health Organization (WHO) estimates that up to 80% of the population in Africa makes use of traditional medicine. In Sub-Saharan Africa, the ratio of traditional healers to the population is approximately 1:500, while medical

doctors have a 1:40 000 ratio to the rest of the population. According to Deputy Minister of Health Nozizwe Madlala, statistics indicate that more people in SA consult traditional health practitioners than they do medical doctors and other practitioners of allopathic medicine. A reason for this is because they do not have access to any kind healthcare and others have a strong cultural belief that traditional healers are capable of curing any disease and most of the diseases are believed to be caused by witchcraft.

Traditional healers play an influential role in the lives of African people and have the potential to serve as crucial components of a comprehensive healthcare strategy. It is vital to note that one should hesitate before making the decision to consult them as some of them have a lack of such knowledge, expertise, reality and use this profession to survive by getting income from patients. According to Steinglass (2002), "traditional healers tend to take a holistic approach to illness, treating the patient's spiritual and physical well-being together. With a terminal disease like AIDS, the spiritual side becomes very important".

For example, a traditional healer in Kwazulu-Natal argues that some traditional healers view HIV/AIDS as a "development of an old disease that can be treated by traditional healers only" Munk (1998). The interpretation of this statement can be confirmed false until today because there is no medication available for this epidemic disease.

It can be concluded that in order to ensure that traditional health practice continues to have currency and value and make a meaningful contribution to the national health system, it is necessary to systematise and regularize it. This can hold responsible traditional healers who practice false medications. The Traditional Health Bill allows patients to lay complaints if they feel that they have been mistreated by health practitioners.

The enactment of a law provides a lot of advantages, such as the protection of privacy and information from misuse. It is important to note that the whole process of compiling and implementing its regulatory requirements can demand a great effort from the government and it makes sense to look at other laws already implemented from other countries and customize them to solve related issues.

4.5.5 Healthcare Information Portability and Accountability Act (HIPAA)

The South African Council for Medical Schemes committee in 2000, held separate meetings with providers and funders in an effort to address problems experienced by healthcare providers with regard to the payment of claims. The two parties identified as important the need for greater standardization of data collection, IT systems and billing practices as a key to resolving the many problems afflicting the industry (Council Medical Schemes, 2002).

There was a need to refer to other work accomplished by other organizations such as the use of Health Level Seven (HL7) which was already adopted by HIPAA (Health Insurance and Accountability Act) regulations in America to achieve this objective. This application standard requires all healthcare players to use HL7 v.2 in conjunction with X12 for passing data between providers and payers. It can be seen that the recommendations finally drawn were mostly related to HIPAA standards requirement such as the use of security and accountability safeguards found in HIPAA security standard; *Written consent of the patient prior to the disclosure of health information*; *Notice about the use and disclosure of health information* and *Minimum necessary standard* found in HIPAA privacy standard. Most of these standards have been incorporated in the South African National Health Act (SANHA). Therefore, it becomes obvious that the incorporation of HIPAA standards requirements into South African health sector is an undisputable issue. This ensures best practices for ensuring the security and privacy of health information in the South African healthcare organizations.

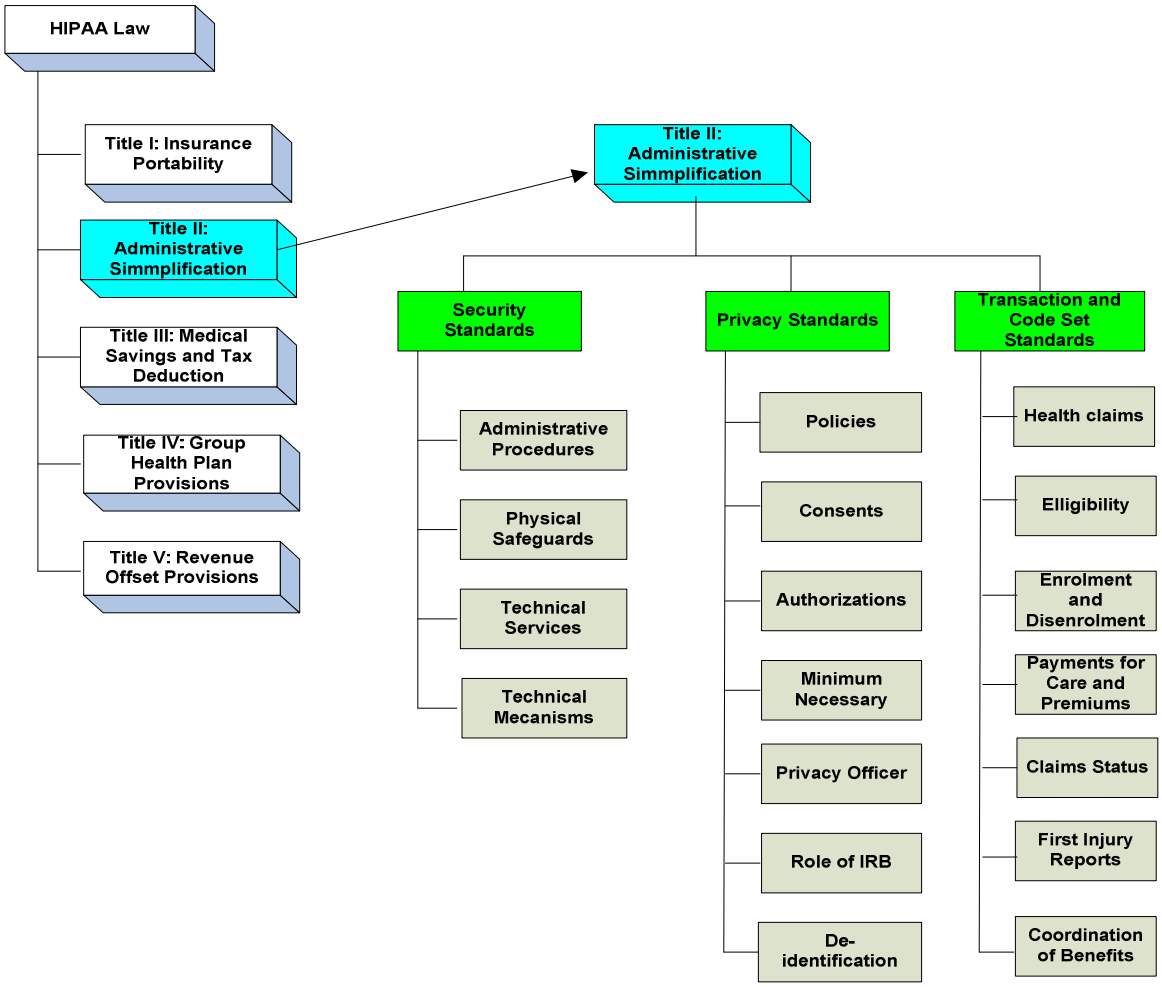
The Healthcare Information Portability and Accountability Act (HIPAA), Public Law 104-191 was signed into law by the President Bill Clinton on August 21, 1996. The primary focus of HIPAA is to mandate that healthcare information become "portable" and "available" by legislating the use of uniform electronic transactions and other administrative measures. The forcing of the healthcare industry to adopt uniform electronic transaction standards for healthcare information meant, it is necessary to protect that same information by including standards for how the information would be secured and safeguarded (CMMS, 1996).
The main objectives of HIPAA (1996) include:

- To improve the portability and continuity of health insurance coverage in the group and individual markets;

- To combat waste, fraud and abuse in health insurance and healthcare delivery;
- To simplify the administration of health insurance and for other purposes;
- To standardize healthcare transaction processing and communication;
- To ensure the privacy and security of health information.

The portion of the HIPAA law that most impacts IT technology interests is the section on Administrative Simplification (Title II, Subtitle F). This section seeks to force uniform standards in the electronic interchange of health information (through the Transaction standard) and mandates guidelines for the security (Security standard) and privacy (Privacy standard) of that information whether in transit or stored. These standards are discussed in more detail. Figure 11 illustrates the five titles of HIPAA law.

Figure -11- HIPAA Law



Source: Swindom, 2004

The US Department of Human Health and Services (HHS) has issued three rules (Security, Privacy and Transaction and Code Set) that covered entities should follow to implement the HIPAA law. HIPAA defines covered entities as:

a. **Health plan** means any individual or group plan that provides or pays the cost of medical care, including public and private health insurance issuers, healthcare management organizations or other managed care organizations, employee benefit plans, the Medicare and Medicaid programs, military/veterans plans and any other "policy, plan or program" for which a principal purpose is to provide or pay for healthcare services;
b. **Healthcare provider** means a provider of medical or health services and any other person or organization who furnishes, bills or is paid for healthcare in the normal course of business;
c. **Healthcare clearinghouse** means a public or private entity, including a billing service, re-pricing company, community health information system and "value-added" networks and switches that either processes or facilitates the processing of health information.

The following section is dedicated to the description of the HIPAA rules requirements namely Security, Privacy and Transaction and Code Set rules.

4.5.5.1 HIPAA Security Rule

The Department of Health and Human Services (HHS) made HIPAA a top priority for CIOs in publishing the HIPAA Security Rule on April 21, 2003 (Chell, 2005). The Security Rule establishes required and addressable specifications for the protection of electronic health information. The storage and/or transmission of this personal health information through electronic means must meet certain security protocols as required by the Security Rule. Generally, the Security Rule mandates the protection of the confidentiality, integrity and availability of electronic personal health information (HIPAA Administrative Simplification – HIPAA Security Rule, 2003).

The HIPAA Security Rule is divided into three broad areas of safeguards namely; *Administrative*, *Physical* and *Technical* and contains 42 security measures specifications that covered entities must implement to assure the confidentiality,

availability and integrity of electronic health information. The federal government, in each of these areas, has created a set of standards that healthcare organizations must meet to be compliant with this rule which is fixed by April 21, 2005 final compliance date.

Administrative safeguards are requirements designed to guard health information integrity, confidentiality, and availability. These are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of health information.

The Administrative security area is often referred to as the envelope that wraps around the entire Information Security program (Anderson, 2005). It communicates direction, establishes expectations and outlines disciplinary actions for non-compliance. This is an area where significant effort should be focussed since it provides the fundamental principles upon which the entire Information Security program is based. It serves as the central source of documentation for HIPAA compliance reviews.

It is crucial to note that for every standard, the Security Rule provides a number of implementation specifications. The HHS makes a distinction between implementation specifications that are required and those that are addressable. If a standard that is marked Required (R), means the covered entities must implement policies and/or procedures that meet the implementation specification; on the other hand, for Addressable (A) specifications, covered entities must assess whether each implementation specification is a reasonable and appropriate safeguard in their environment based on the likely contribution it would make the protection of health information. Should it be appropriate they must implement as written else they must document why it is inappropriate and implement an equivalent alternative measure that is reasonable and appropriate.

Table 2 outlines the required and addressable measures of the Administrative Safeguards requirements.

Table -2- Administrative Safeguards Standards

Administrative Safeguards (164.308)			
Standards	Section	Implementation specifications	R
Security Management Process	164.308(a)(1)	Risk Analysis	R
		Risk Management	R
		Sanction Policy	R
		Information System Activity Review	R
Assigned Security Responsibility	164.308(a)(2)	Assigned security responsibility	R
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	A
		Workforce Clearance Procedure	A
		Termination Procedures	A
Information Access Management	164.308(a)(4)	Isolating healthcare clearinghouse function	R
		Access authorization	A
		Access establishment and modification	A
Security awareness and training	164.308(a)(5)	Security reminders	A
		Protection from malicious software	A
		Log-in monitoring	A
		Password management	A
Security Incident Procedures	164.308(a)(6)	Response and reporting	R
Contingency plan	164.308(a)(7)	Data backup plan	R
		Disaster recovery plan	R
		Emergency mode operation plan	R
		Testing and revision procedure	A
		Applications and data criticality analysis	A
Evaluation	164.308(a)(8)	Systems evaluations	R
Business Associates contracts and other arrangements	164.308(b)(1)	Written contract or other arrangement	R

Source: Swindom, 2004

Physical safeguards are requirements designed for the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards and intrusion. Physical safeguards cover the use of locks, keys and administrative measures used to control access to computer systems and facilities. Physical security measures play a large role in the assurance of Information Security for electronic storage and transmission media. The old Information Security axiom holds true "Anything I can touch, I can own". The lack of control for physical access to information assets, implies not whether information assets will be compromised, but more a question of when (Anderson, 2005). Table 3 shows the standards, section and implementation specifications of physical safeguards. These are marked Required (R) or Addressable (A).

Table -3- Physical Safeguards Standards

Physical Safeguards (164.310)			
Standards	Section	Implementation specifications	
Facility Access Controls	164.310(a)(1)	Contingency operation	A
		Facility Access Plan	A
		Access Controls & Validation Procedures	A
		Maintenance Records	A
Workstation Use	164.310(b)	Workstation use	R
Workforce Security	164.310(c)	Workforce security	R
Device and Media Controls	164.310(d)(1)	Disposal	R
		Media Re-use	R
		Accountability	A
		Data Backup and Storage	A

Source: Swindom, 2004

Technical safeguards are requirements designed for the protection, controlling and monitoring to access of health information. These safeguards ensure the prevention of unauthorized access to medical information that is transmitted over a communication network. Table 4 shows the Technical Safeguards Standards.

Table -4- Technical Safeguards Standards

Technical Safeguards (164.312)			
Standards	Section	Implementation specifications	
Access Controls	164.312(a)(1)	Unique User Identification	R
		Emergency Access Procedure	R
		Automatic Logoff	A
		Encryption and Decryption	A
Audit Controls	164.312(b)	Audit controls	R
Integrity	164.312(c)(1)	Mechanisms to Authenticate electronic health information	A
Person or Entity Authentication	164.312(d)	Person or entity authentication	R
Transmission Security	164.312(e)(1)	Integrity Controls	A
		Encryption	A

Source: Swindom, 2004

4.5.5.2 HIPAA Transaction and Code Set Rule

HIPAA directed the Secretary of Health and Human Services (HHS) to adopt standards for the electronic exchange of administrative and financial healthcare transactions to improve the efficiency and effectiveness of the healthcare system. These are commonly referred to as the Electronic Data Interchange (EDI) standards, and include defined and numbered transactions, formats and data elements. These standards were established to eliminate redundant tasks, lower administrative costs associated with paper-based processes and identify new opportunities to use EDI to streamline information flows and improve overall data quality (HIPAA Administrative Simplification - Transaction and Code Set Rule, 2000).

The Transaction and Code Set rule addresses both the content of the information to be exchanged and the specific formats in which information is to be exchanged. Healthcare providers and health plans will be required to accept only transactions submitted in standard form in accordance with the adopted HIPAA transaction standards. These provisions were to be effective October 2002, but a subsequent act signed by President Bush in December 2001 extended the deadline by one year by filing for an extension. All medical offices that submit electronic transactions must comply with the Transaction and Code Set rule by October 16,

2003 (HIPAA Administrative Simplification - Transaction and Code Set Rule, 2000).

Section 1173 lists the transactions and sets out requirements for the specific standards to adopt: unique health identifiers, code sets, security standards, electronic signatures, and transfer of information among health plans.

At present, this rule encompasses the following standard electronic transaction formats preponderantly derived from the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12. ANSI X12 subcommittee N covers standards in the insurance industry, including health insurance; hence these are X12N standards. X12N standards include transactions for claims/encounters, attachments, enrolment, disenrolment, eligibility, payment/remittance advice, premium payments, first report of injury, claim status, referral certification/authorization, and coordination of benefits. They include (HIPAA Administrative Simplification - Transaction and Code Set Rule, 2000):

- X12N 837 - Healthcare Claim for Dental, Professional and Institutional;
- X12N 835 - Healthcare Claim Payment/Advice;
- X12N 834 - Benefit Enrolment and Maintenance;
- X12N 820 - Payroll Deducted and Other Group Premium Payment for Insurance Products;
- X12N 278 - Healthcare Services Request for Review and Response;
- X12N 276 - Healthcare Claim Status Request;
- X12N 277 - Healthcare Claim Status Response;
- X12N 270 - Healthcare Claim Eligibility Inquiry;
- X12N 271 - Healthcare Claim Eligibility Response;
- X12N 148 - Report of Injury or Illness;
- X12N 186 - Life and Annuity Lab Report;
- X12N 275 - Patient Information.

It is important to note that this list of transactions is expected to increase over time as other transactions are adopted (HIPAA Administrative Simplification - Transaction and Code Set Rule, 2000). The Transaction and Code Set rule also requires the use of Code Sets which are values that are used in the data fields to identity conditions, procedures and entities in addition to the standardization of healthcare transaction standards. Under HIPAA, local procedure codes will be eliminated and replaced with National Standard HCPCS Level II and CPT codes.

4.5.5.3 HIPAA Privacy Rule

The final Rule for privacy was published on December 28, 2000 and compliance was required by April 14, 2003. The Privacy Rule standards addresses the use and disclosure of the health information of an individual — called "protected health information" by organizations subject to the Privacy Rule — called "covered entities," and standards for their privacy rights to understand and control how their health information is used. The Office for Civil Rights (OCR) within HHS has the responsibility for implementing and enforcing the Privacy Rule with respect to voluntary compliance activities and civil money penalties (HIPAA Administrative Simplification – Privacy Final Rule, 2002).

A major goal of the Privacy Rule is to assure that the health information of individuals is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the health and well being of the public. The Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing. The Rule is designed to be flexible and comprehensive, given that the healthcare marketplace is diverse to cover the variety of uses and disclosures that need to be addressed (HIPAA Administrative Simplification – Privacy Final Rule, 2002).

The final privacy rule entails that covered entities must protect individually identifiable health information against deliberate or inadvertent misuse or disclosure. Consequently, health plans and providers must maintain administrative and physical safeguards to protect the confidentiality of health information and protect it against unauthorized access. These entities must inform individuals about how their health information is used and disclosed and ensure them access to their information. Written authorization from patients for the use and disclosure of health information for most purposes is required with the exception of healthcare treatment, payment and operations (and for certain national priority purposes). Table 5 provides the standards and implementation specifications addressed in the HIPAA Privacy Rule.

Table -5- Privacy Rule Standards

Privacy Rule Standards (45 CFR Parts 160 - 164)		
Standards	Section	Implementation specifications
Patient Access	164.524	Right to inspect and copy
	164.526	Right to amend
General Rules for Use and Disclosure	164.502(a)	Permitted Uses and Disclosures
	164.502(a)(b)	Permissive not Mandatory
	164.502(b), 164.514(d)	Minimum Necessary
	164.502(a)	Incidental Uses and Disclosures
	160.103, 164.502(e), 164.532(d)(e)	Business Associates
	164.502(a), 164.508	Authorization
Specific Rules for Use and Disclosure	164.501, 164.506, 164.520(c), 164.522	Treatment, Payment, and Healthcare Operations
	164.510(a)	Facility Directories
	164.510(b), 164.522	Those involved in Providing Care (Next of Kin)
	164.501, 164.508(a)(3)	Marketing
	164.501, 164.514(f), 164.522	Fundraising
	164.512(j)	Averting a Serious Threat to Health or Safety
	164.512(d)	Health Oversight Activities
	164.512(e)	Judicial and Administrative Proceedings
	164.512(f)	Law Enforcement
	164.512(b), 164.514(e)	Public Health Activities
	164.512(a)	Required by Law
	164.512(i), 164.514(e)	Research
	164.512(c)	Victims of Abuse, Neglect, or Domestic Violence
	164.512(l)	Workers' compensation
Administrative Requirements of Covered Entities	164.500, 164.520	Notice of Privacy Practices
	164.530 (c)	Safeguards
	164.530 (b)	Training
	164.530 (a)	Privacy Officer

	164.528	Accounting for Disclosures
Special Rules for Certain Types of Entities	164.504(a)(c)	Hybrid Entity
	164.504 (d)	Affiliated Covered Entity
	164.504(g)	Multiple Covered Function Entity
	164.504 (f)	Group Health Plan
	164.501, 164.520	Organized Healthcare Arrangement
Enforcement and Compliance	160.306, 160.312	Complaints
	160.308, 160.310, 160.312	Compliance Reviews
	160.201	Penalties

Source: HIPAA Administrative Simplification - Transaction and Code Set Rule, 2000

4.6 CONLUSION

Currently, privacy has become an asset and like any significant asset, it will become even scarcer with the inter-trading of various companies. Resultantly, the protection of privacy is becoming an important competitive differentiator for leading organizations worldwide, in industries from financial services to health care, to consumer and technology markets (KPMG, 2001).

Organizations are viewing privacy protection as a way to increase stakeholder trust as well as mitigate risks, improve customer satisfaction and potentially generate new revenues (Vericept Corporation, 2004). Consumers are particularly concerned about privacy of their information, especially whether they can trust organizations to safeguard their information. Trust is not the only reason people buy from a company, but without it they will go elsewhere (KPMG, 2001).

Many countries, realizing the importance of privacy and the data of patients, have adopted different legal and regulations at national and international level to ensure the protection of such information.

It is vital to emphasize that complying with regulatory requirements is mandatory for any organization and ignorance of the law is not an excuse. Ignorance of the law can result in the loss of credibility, heavy punishment and the loss of business opportunities (Tuyikeze & Pottas, 2005). However, organizations should strive to balance the challenges of meeting data protection requirements with clear

business interest in using customer information to identify potential business opportunities, both inside and outside of the organization (KPMG, 2001).

Chapter 4 has demonstrated that there are a growing number of regulations that include requirements for organizations to provide security controls and demonstrate compliance assurance. The challenge encountered by most organizations is what compliance strategy should be followed to meet regulatory requirements while ensuring that the existing efforts already implemented are maintained (Tuyikeze & Pottas, 2005). Therefore, a comparative analysis of compliance requirements is required, which in this paper is focused on the ISO 17799, HIPAA, SANHA and ECTA. The result of this comparison will help to ensure that security controls are not being duplicated in endeavors to satisfy requirements from the various standards and laws. This is the main focus of **Chapter 5**.

Chapter 5 COMPARISON BETWEEN ISO 17799, HIPAA, SANHA AND ECTA

The main objective of this **Chapter 5** is to compare an Information Security Management standard (ISO 17799) with the laws applicable to typical South African healthcare organizations. These are not only applicable laws in the South African context but have been selected as defined by the scope of this research project. The comparison shows that there can exist an overlap between them and therefore, there is a need for a comparative analysis of compliance requirements. The result of such comparison will help ensure that security controls are not being duplicated in the endeavours to satisfy the requirements for the various security standards and laws.

This chapter concludes by emphasizing the need for a framework which ensures full compliance with regulatory requirement while ensuring patients that best practices for Information Security Management are being used concomitantly ensuring the privacy and security of their medical information.

Chapter 6 is dedicated to a discussion of the phases that constitute this compliance model.

"Multiple regulations and standards coupled with regulatory overlap leads to redundancy in compliance effort at high cost".

- Teller-Kanzler, 2005 -

5.1 INTRODUCTION

The Information Security and privacy regulatory environments grow more stringent and complicated every day. The enactment of new laws and regulations is forcing organizations to re-evaluate their Information Security practices in order to ensure they comply with these new law requirements (Teller-Kanzler, 2005). The challenge that faces most organizations is how to find easy ways to meet these regulations while spending less money with least effort.

Total compliance with existing, emerging and anticipated government regulations is a daunting goal (ITCI, 2005). Organizations in fact, are often seesawed between overlapping, over-focussed and uncoordinated regulations which are laid down along geographic, industry, and situation-specific lines (Accenture, 2004). The issue of compliance is further confused by the existence of a multitude of non-mandatory security standards that where used by organizations where adequate regulations have not yet existed. The proliferation of legislation together with existing standards has made the compliance challenge an undeniable fact for example, the overlapping between laws themselves and/or with security standards. It, therefore, is necessary to identify what security controls are already implemented and those which are lacking to meet with the new regulatory requirements.

5.2 OVERLAP BETWEEN SECURITY STANDARDS AND REGULATORY REQUIREMENTS

Regulatory overlap, according to Lineman (2005), is the crux of the problem that many organizations face today. He further added that there is a tendency to treat each incoming regulation as a discrete project to minimize its impact on production systems and allow project teams to focus on meeting the regulatory deadlines. The downside to this approach, however, is redundant development

and ill-placed investment in incompatible solutions with, the increased likelihood of error and integration problems later (Brewer, 2005).

In many cases, the requirements addressed by the government laws involve different terms which words but have same meaning themselves and with the security standards as illustrated in Table 6.

Table -6- Security Standard and Regulatory requirements meaning overlap

Standard	Section	Subsection	Specification
ISO 17799	9.1.1. Access controls	9.1.1.1 Policy and business requirements	Organizations should implement policies for information dissemination and authorization, e.g. the need-to-know principle and security levels and classification of information.
SANHA	II. Rights and Duties of Users and Healthcare Personnel	15(1) Access to health records	A health worker or any healthcare provider that has access to the health records of a user may disclose such personal information to any other person, healthcare provider or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of his or her duties where such access or disclosure is in the interests of the user.
HIPAA Privacy Rule	IV. Limiting Uses and Disclosures to the Minimum Necessary	164.502(b) &164.514(d) Minimum necessary	A covered entity must make reasonable efforts to use, disclose and request only the minimum amount of health information to accomplish the intended purpose of the use or disclosure. A covered entity must implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary.

Please refer to the **Appendix A** for a complete detailed comparison. The designations for the comparison are provided in Table 7.

This redundancy is equally found in other security standards and regulatory requirements not covered by this project. A recent research conducted by

Network Frontiers (2005), for example proves some interesting similarities of the control objectives found in more than one security standard and regulatory requirements as described in the following example. The control objective that states that "*Organization must have auditing and monitoring procedures*" is found the following eight regulatory requirements: SOX 404; 12 CFR Series, Appendix III.C.3; 17 CFR 240.15d-15; 17 CFR 240.17a-4.(f)(3)(v); Sec 17 CFR 240.17Ad-7.(f)(4); MasterCard SDP 1.7; IRS Rev Proc. 98-25 & 6.03; ESIGN 101 (e) and the following four security standards: (ISO 15489-2.5.2; COBIT M2; PCAOB Audit #2 & 49; FFIEC Management Handbook, pge35 (Teller-Kanzler, 2005).

An important consequence of any redundancy is the high-costs uncured due to duplication of the existing controls with the new regulatory requirements (ITCI, 2005). For example, in 2005, public companies in America reported that of the IT costs of companies between 30 to 50 percent of the total compliance bill was due to redundant development and manual processing (Brewer, 2005). Organizations, according to CEO Network Frontiers Cougias (2005) must identify similar controls objectives found in multiple security standards and regulatory requirements in order to reduce compliance efforts and increase their return on investment.

One of the largest difficulties that face most organization is that laws are typically written for what must be implemented but not the implementation method (Jendrey, 2005). Additionally, there is flexibility that is built around the regulatory requirements, government does not limit entities to a specific technology to meet with these government laws; but, the trade-off is that there is little guidance regarding technology given to entities that do not already have a robust security program (McLaughlin, 2005). There is a need for "crosswalks" to bridge this gap that compares existing industry security standards and regulatory s requirements to reveal similarities and differences between the various laws and standards.

5.3 THE CROSSWALK BETWEEN SECURITY STANDARDS AND REGULATORY REQUIREMENTS

The Meridian dictionary (1992) defines a crosswalk as a "specially paved or marked patch for a pedestrian crossing a street or road." There is unfortunately, no specially paved road or marked path to walk on toward compliance with security standards and regulatory requirements. Following this analogy, there are in fact, many security regulations (roads) and security standards (paths) and there is no one map leading from point A to point B. There are, interestingly some

similarities (lanes) between these roads and paths that can be used to join them. A pedestrian wants to cross from point A to B quickly and it becomes simple for him to pass these lanes through a shortcut instead of going the long way around. The same scenario applies to the current compliance dilemma with multiple security standards and regulatory requirements. The major challenge that faces executive managers responsible for ensuring compliance is how easily they can cross from one security standard or government regulatory requirement to another without spending significant effort. It therefore is necessary to conduct an IT controls mapping which will reveal any similarities and disparities between them.

The realization of the importance of crosswalks or the mapping of security controls between the various security standards and/or regulatory requirements, has received much attention from different organizations, such as WEDI, ISACA, ITCI, etc…

The Workgroup for Electronic Data Interchange (WEDI), a healthcare industry group with a formal consultative role under the HIPAA legislation defines crosswalk or data mapping as "the process of matching one set of data elements or individual code values to their closest equivalents in another set of them". Typical examples that illustrate similarities and differences between various regulations and security standards are available at the WEDI website Workgroup for WEDI's web site (WEDI). Each document identifies best practices extracted from a range of existing security rules and standards, including HIPAA Security Rule, ISO 17799, the Cryptographic Message Syntax Core Security Requirements (CMSCSR), the Federal Information Security Management Act of 2002 (FISMA) and the Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) for HIPAA (Schwartz, 2005).

The Information Systems Audit and Control Association (ISACA) on COBIT Mapping solve the same problem. This organization provides mapping between COBIT and ITIL, ISO/IEC 17799:2000, ISO/IEC TR 13335, ISO/IEC 15408:1999 Common Criteria/ITSEC, TickIT, NIST 800-14 and COSO. A complete description is available on the website of the IT Governance publication's (ITGI).

Another example is the Unified Compliance Project (UCP), which was launched by Information Technology Compliance Institute (ITCi) on July 11, 2005. The Unified Compliance Project represents a cooperative research and development effort by

the IT Compliance Institute and Network Frontiers, a compliance and consultancy organization. Network Frontiers engaged in a massive investigation to reveal the overlap in standards and regulations. ITCI (2005) argues that the UCP is the first independent initiative to exclusively support IT compliance management by revealing the overlap between complex regulatory requirements. The UCP most importantly supports, a strategic approach to IT compliance that reduces cost, limits liability and leverages the value of compliance-related technologies and services across the enterprise by focusing on commonalities across regulations, standards-based development, and simplified architectures, (Cougias, 2005). Cass Brewer, editorial and research director at the IT Compliance Institute, maintains "To reduce IT costs and make smart investments in sustainable compliance efforts, companies need to gain a unified view of their total compliance burdens,"

The 2005 Unified Compliance Project of ITCI deals with:

- Various Regulatory requirements sources: Namely Sarbanes-Oxley, PCAOB, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), California SB 1386, the European Union Data Protection Directive, the UK Data Privacy Directive, Turnbull guidance, HIPAA, and GLB;
- IT frameworks: COBIT, HIPAA standards, SAS 94, and others;
- IT impact zones: IT security, physical security, business security, staff management, leadership and operational management, auditing and other zones.

The UCP divides the regulatory and standards requirements into twelve critical IT Impact Zones. These include: Leadership and High Level Objectives; Audit and Risk Management; Design and Implementation; Systems Acquisition; Operational Management; IT Staff Management and Outsourcing; Records Management; Technical Security; Physical Security; Systems Continuity; Monitoring, Measurement and Reporting; and Privacy (ITCI, 2005). However, Cougias (2005) confirms that this project is still at an early stage of development.

These crosswalks should, according to Lineman (2005), address common elements once for multiple uses and therefore can save both of time and efforts for the organization which would otherwise be wasted on duplicate security controls already implemented. It can be argued that, in order to accomplish this target, the organization should use an already established framework, such as

ISO 17799, to create a security benchmark perform a gap analysis and work to close the gap. The identification of this gap between the security standards and regulatory requirements definitely entails performing a comparison which will reveal existing efforts already implemented and gap that needs to be applied to meet the new regulatory requirements.

5.4 COMPARISON BETWEEN ISO 17799, HIPAA, SANHA AND ECTA

The regulatory requirements of the government as examined with a deeper insight and discussed in Chapter four show that there is little doubt that some sections address the security and privacy issues and therefore have some overlap sections with the Information Security Management framework. This can result in a duplication of efforts and resources when healthcare organizations are implementing controls to comply with the new regulations requirements. Therefore, a comparison is needed to reveal any similarities and differences between them.

A comparison of each of the 127 ISO 17799 controls against SANHA, ECTA and HIPAA regulation requirements were made and the result of the comparison is provided in Appendix A. The ISO 17799, which covers the broad area of Information Security Management, serves well as a basis for this comparison. The comparison between ISO 17799 and HIPAA security standards has been done by URAC (2004), an independent and non-profit organization which is well-known as a leader in promoting healthcare quality through its accreditation and certification programs and it will be referred to again in this project. The comparison gauged the HIPAA Security standards requirements as being similar partially covered, Not covered, and Exceeding the ISO 17799. The previous comparison was taken further to include HIPAA Privacy standards, Transaction and Code Set standards, SANHA and ECTA. The designations for the comparison and their meanings are provided in Table 7.

Table -7- Designation of the comparison

Designation	Meaning
HIPAA_SSMp	HIPAA Security Standards mapping
HIPAA_SSEq	HIPAA Security Standards equation
HIPAA_PSMp	HIPAA Privacy Standards mapping
HIPAA_PSEq	HIPAA Privacy Standards equation
HIPAA_TCSMp	HIPAA Transaction and Code Sets Standards mapping
HIPAA_TCSEq	HIPAA Transaction and Code Sets Standards equation
SANHA_Mp	SANHA Standards mapping
SANHA_Eq	SANHA Standards equation
ECTA_Mp	ECTA Standards mapping
ECTA_Eq	ECTA Standards equation
#	**Not covered:** For the topic of concern, the ISO 17799 control is not covered at all in regulation requirements
<	**Partially covered:** For the topic of concern, the ISO 17799 control exceeds the regulation requirements.
~	**Similar coverage:** For the topic of concern, the regulation requirements and ISO 17799 are approximately the same
>	**Exceed:** For the topic of concern, the regulation includes at least one requirement not included in ISO 17799. The goal with this is to point out areas where ISO 177999 does not fully contain the regulation requirements.

Table 8 provides the percentage values of the result of the comparison performed in **Appendix A**.

Table -8- Comparison result summary

Laws versus ISO 17799	Matching sum	Percentage
HIPAA_Sec ~ ISO 17799	77	55 %
HIPAA_Sec > ISO 17799	19	14 %
HIPAA_Sec # ISO 17799	26	18 %
HIPAA_Sec < ISO 17799	18	13 %
HIPAA_Priv ~ ISO 17799	5	3 %
HIPAA_Priv > ISO 17799	28	19 %
HIPAA_Priv # ISO 17799	107	71 %
HIPAA_Priv < ISO 17799	10	7 %
HIPAA_Trans ~ ISO 17799	1	1 %
HIPAA_Trans > ISO 17799	20	14 %
HIPAA_Trans < ISO 17799	2	2 %
HIPAA_Trans # ISO 17799	121	83 %
SANHA ~ ISO 17799	7	5 %
SANHA > ISO 17799	15	11 %
SANHA # ISO 17799	104	74 %
SANHA < ISO 17799	14	10 %
ECTA ~ ISO 17799	5	3 %
ECTA > ISO 17799	32	21 %
ECTA < ISO 17799	16	11 %
ECTA # ISO 17799	99	65 %

Additionally, a graphical representation is used which depicts the particular 127 ISO 17799 controls relating to their coverage in HIPAA Security, Privacy, Transaction and code set standards, SANHA and the ECTA. Each graph shows the extent to which the ISO 17799 security controls are covered by these regulations. These graphs are illustrated respectively in the following Figures 12, 13, 14, 15 and 16.

Figure -12- HIPAA Security Standards and ISO 17799 comparison

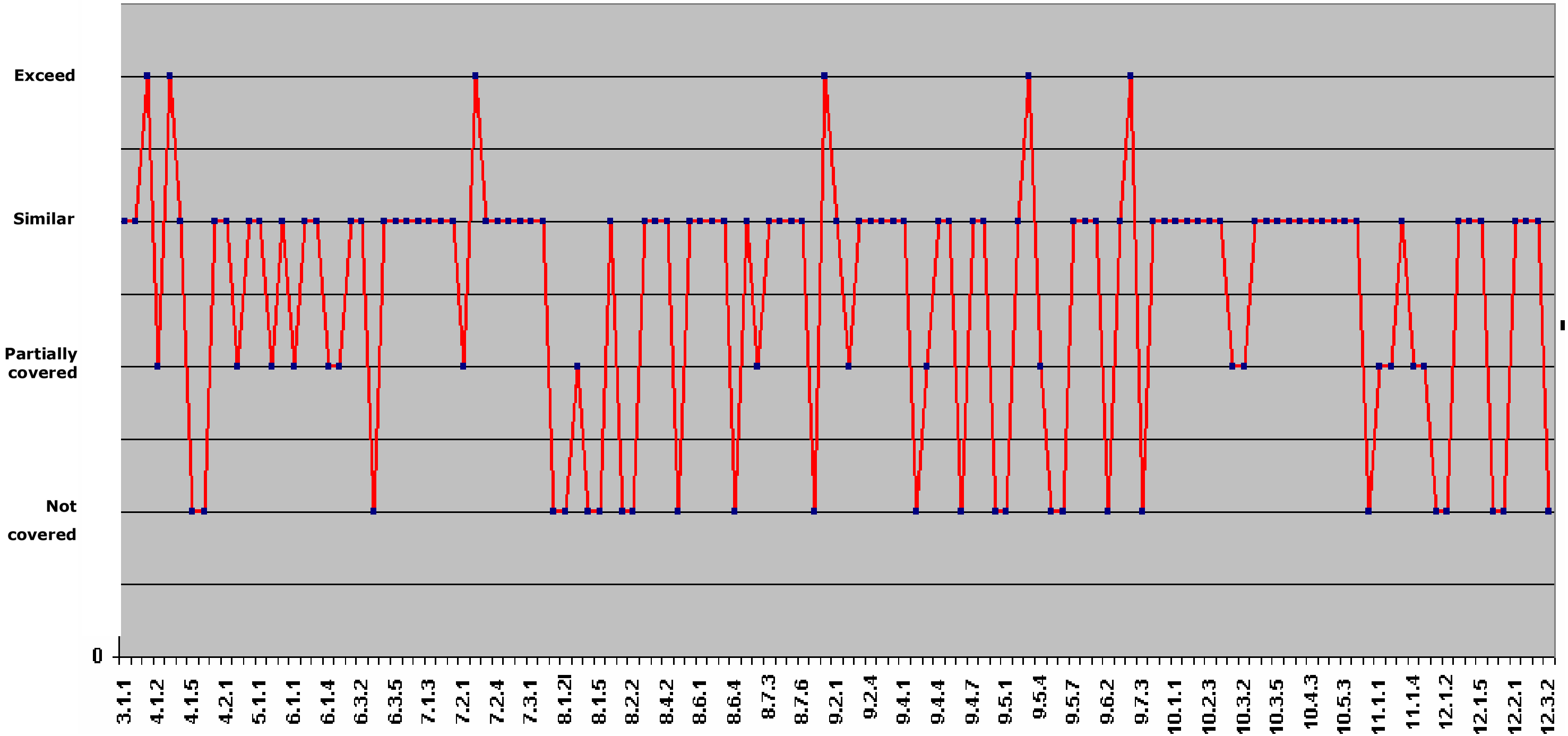


Figure -13- HIPAA Privacy Standards and ISO 17799 comparison

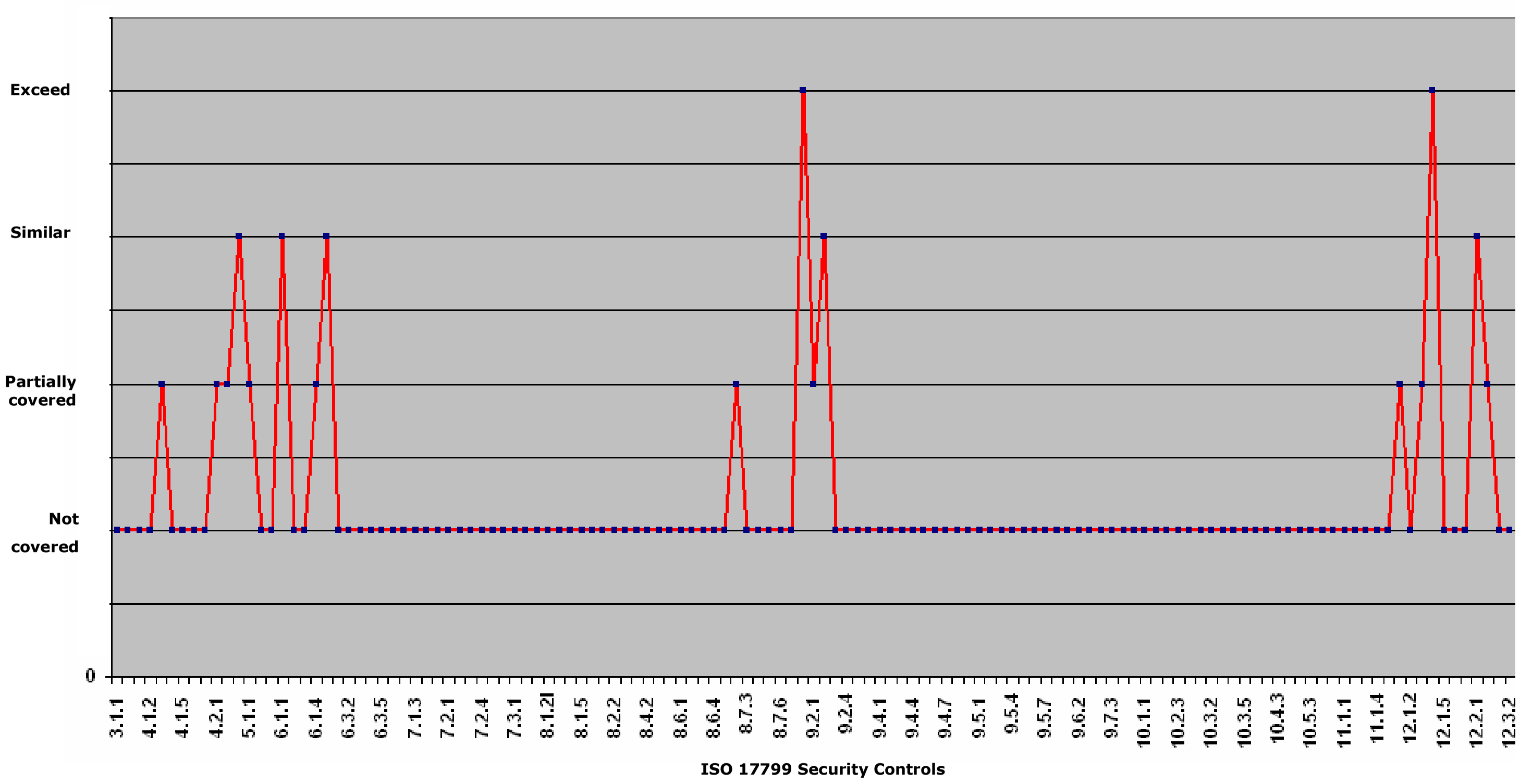
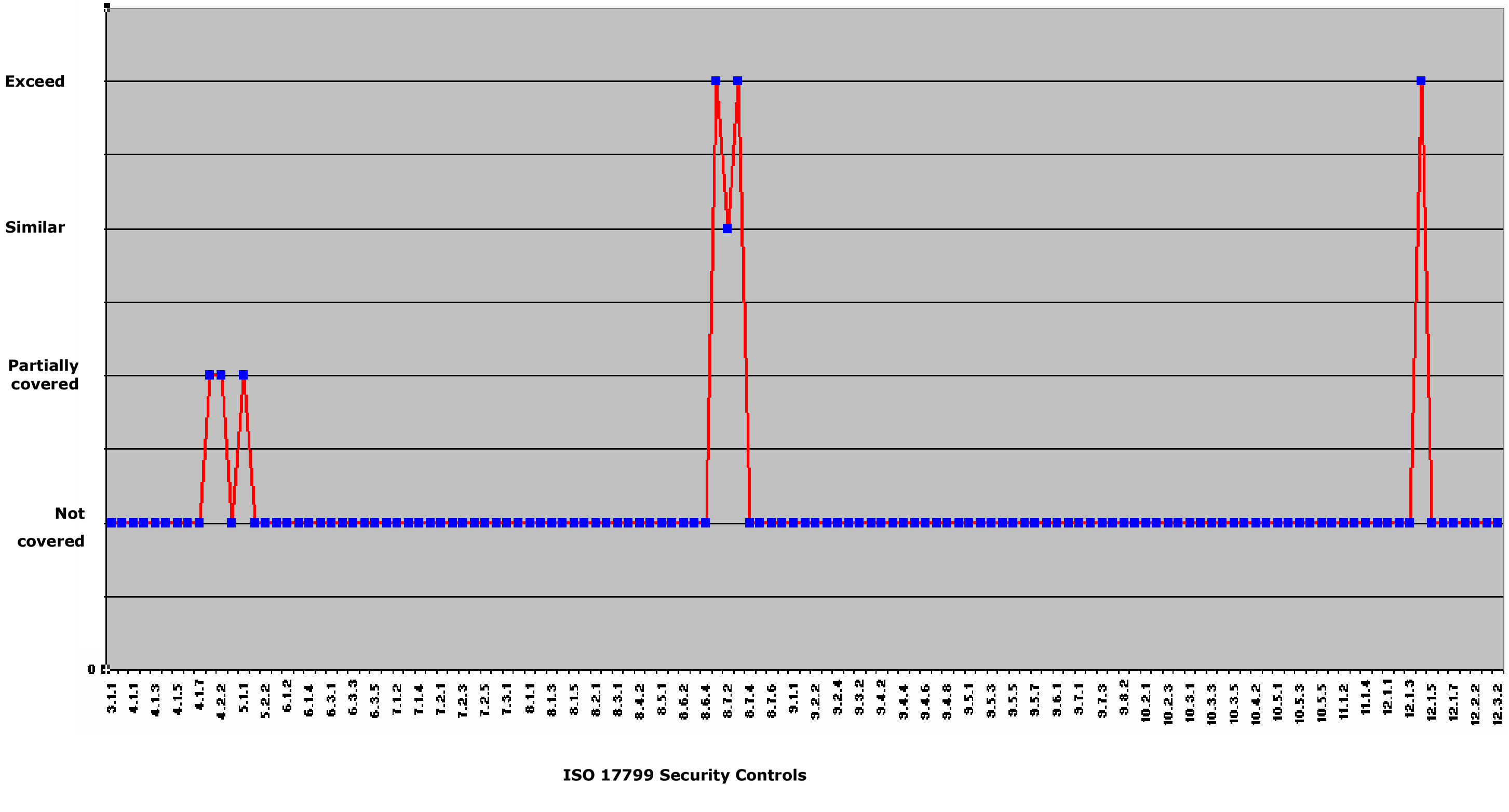


Figure -14- HIPAA Transaction and Code Sets Standards and ISO 17799 comparison



ISO 17799 Security Controls

Figure -15- SANHA Standards and ISO 17799 comparison

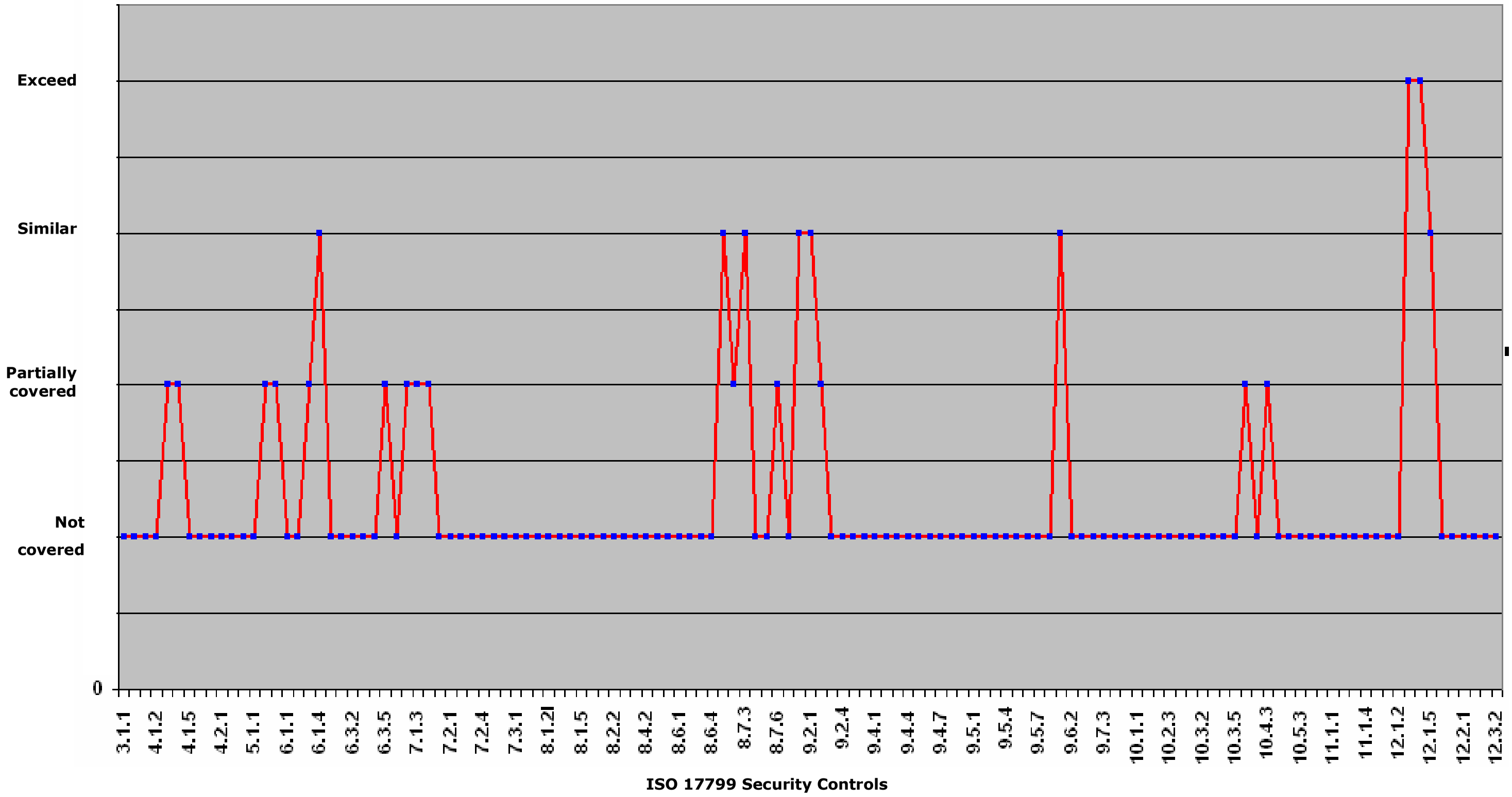
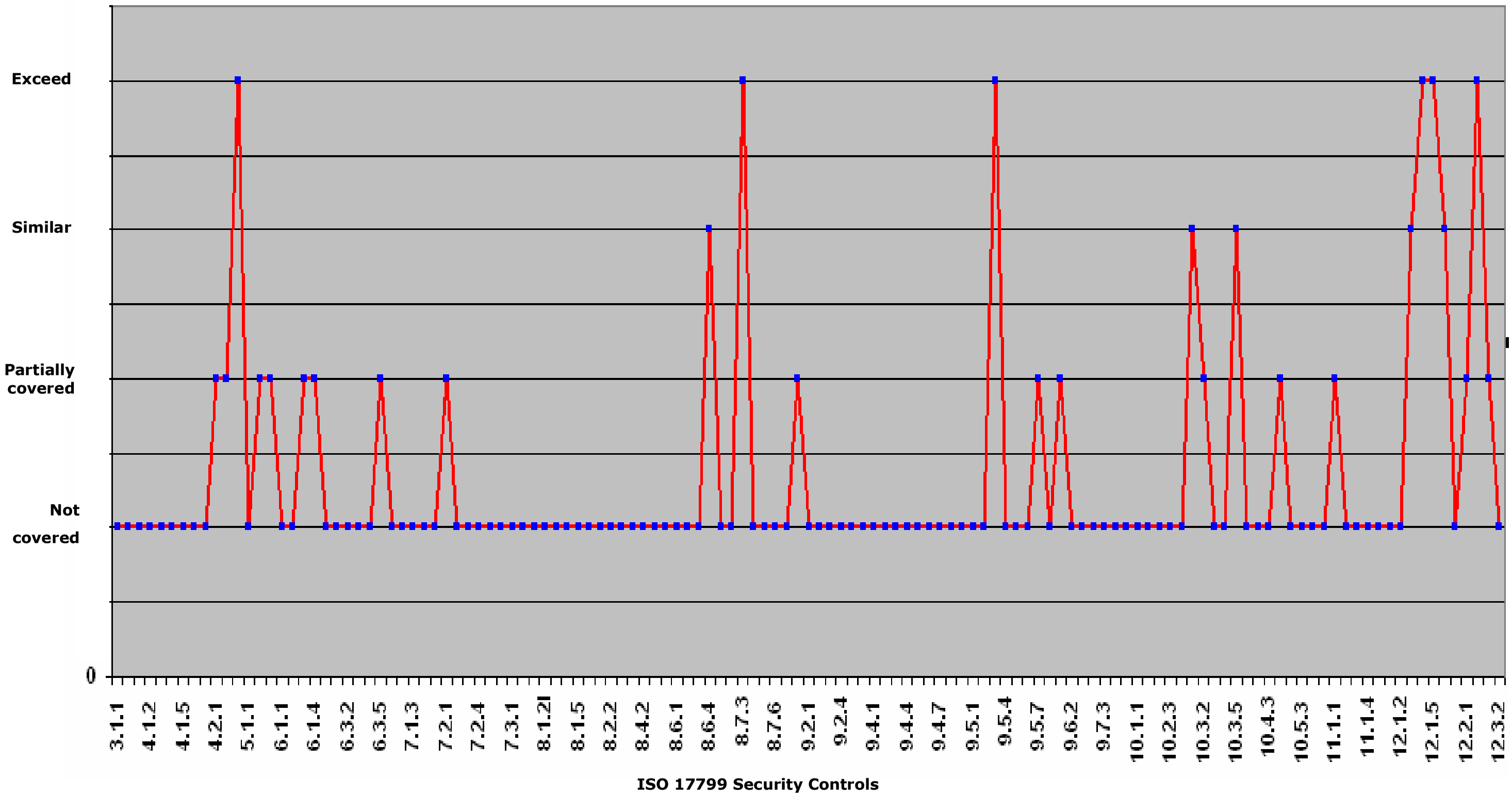


Figure -16- ECTA Standards and ISO 17799 comparison



5.5 ANALYSIS OF THE COMPARISON RESULT

The main objective of this comparative analysis is to deduce how much effort is required by healthcare organizations to meet regulatory compliance requirements when there already exists a well-established Information Security program, which in this case is assumed to be the ISO 17799 security standard. It is shown in the comparison results provided in **Appendix A**, that there are some cases where HIPAA Security, Privacy, Transaction and code set standards, SANHA and ECTA requirements exceed the ISO 17799 requirements. These are regulatory requirements covered in ISO 17799 but entail more requirements for a particular ISO 17799 control. The term Exceed is equally used for regulatory requirements not totally covered by ISO 17799. These are presented in Appendix A following the last ISO 17799 control *12.3.2 Protection of system audit tools*. Both requirements are shown respectively in Table 9, Table 10, Table 11, Table 12, and Table 13 with a brief explanation for each item is provided.

Table -9- Requirements of HIPAA Security Rule not fully present in ISO 17799

HIPAA Security requirement	Explanation
Administrative:(a)(2) Assigned Security Responsibility (required)	HIPAA requires a single person responsible for both information and physical security
Administrative:(a)(3)ii(C) Termination Procedures (addressable)	ISO 17799 has no mention of termination procedures anywhere in the document
Administrative:(a)(4)ii(A) Isolating Healthcare Clearinghouse Functions (required)	Unique requirement of the HIPAA legislation
Administrative:(a)(5)ii(C) Log-in Monitoring (addressable)	ISO 17799 does not have a specific training requirement with respect to log-in monitoring
Administrative:(a)(7)ii(C) Emergency Mode Operation Plan (required)	ISO 17799 does not specifically address security for contingency operations
Physical:(a)(2)(i) Contingency Operations (required)	ISO 17799 does not specifically address physical security for contingency operations
Physical:(a)(2)(ii) Facility Security Plan (required)	Documentation not required by ISO 17799
Physical:(a)(2)(iv) Maintenance Records (addressable)	Documentation not required by ISO 17799

Physical:(a)(2)(iv) Data Backup and storage (addressable)	ISO 17799 does not specifically require data back-up before moving storage units
Technical:(a)(2)(i) Unique User Identification (required)	ISO 17799 allows group user ids in some cases but does not address entity authentication
Technical:(a)(2)(ii) Emergency Access Procedure (required)	ISO 17799 does not specifically address access controls for contingency operations

Source: Borkin, S. 2003. As part of Information Security reading room. SANS Institute 2003

Table -10- Requirements of HIPAA Privacy Rule not fully present in ISO 17799

HIPAA Privacy requirement	**Explanation**
Who is covered by the Privacy Rule?	ISO does not specifically highlight who must ensure compliance.
What information is protected; De-Identified health information	ISO 17799 is for the protection of all types of information.
General principle for uses and disclosures (Basic and required disclosures)	HIPAA privacy rule requires stringent requirements about the circumstances in which health information is used and disclosed.
Permitted uses and disclosures	HIPAA privacy rule permits covered entities to use and disclose health information only as required for the purposes specified in the law.
Authorized uses and disclosures (use of consent)	HIPAA privacy rule requires the patient's authorization before his (her) health information is released unless specified in the legislation.
Administrative requirements	HIPAA privacy rule requires a privacy personnel, procedures for implementation of complaints that are not specifically required in ISO 17799
Notice and other individual rights	Unique requirement of the HIPAA privacy rule legislation
Organizational options(hybrid entity, affiliated covered entity, Organized healthcare arrangement)	Unique requirement of the HIPAA privacy rule legislation
Other provisions: personal representatives and minors	Unique requirement of the HIPAA privacy rule legislation

Table -11- Requirements of HIPAA Transaction and Code Set Rule not fully present in ISO 17799

HIPAA Transaction and Code Set requirement	Explanation
Use of Electronic Transactions standards	Unique requirement of the HIPAA Transaction and Code Set rule
Use of Medical Code Sets standards	Unique requirement of the HIPAA Transaction and Code Set rule
Use of Identifiers standards	Unique requirement of the HIPAA Transaction and Code Set rule

Table -12- Requirements of SANHA not fully present in ISO 17799

SANHA requirement	Explanation
Users to have a full knowledge. Consent of users for disclosure of health information	SANHA provides stringent requirement about the use and disclosure of patient's information.
Participation in decision. Health service without consent. Health service for experimental or research reports disclosures	Unique requirement of the SANHA legislation. It provides rights to patients concerning his (her) information.
Access to health records by a health worker or healthcare provider, duty and procedures to disseminate information by National health department	Unique requirement of the SANHA legislation
Disclosure of health information only if the user provides consent in writing, a court order or any law requires that disclosure, non-disclosure of the information represents a serious threat to public health. Rights of healthcare personnel	Unique requirement of the SANHA legislation. SANHA provides stringent requirement about the use and disclosure of patient's information that are not all specified in ISO 17799.

Table -13- Requirements of ECTA not fully present in ISO 17799

ECTA requirement	Explanation
Admissibility and evidential weight of data messages, Retention, Notarization, Acknowledgement and Certification of data messages	Not specifically covered by ISO 17799
Registration of cryptography providers	ISO 17799 does not specifically require registering cryptography providers
Accreditation, criteria of accreditation of authentication products and services	Unique requirement of the ECTA legislation
Identification, Registration, and Inspection of critical databases	ECTA provides stringent requirements related to protection of critical database which are not specifically covered by ISO 17799
Liability of Service Providers: Hosting, Caching, Mere conduit, Information Location tool	Unique requirement of the ECTA legislation
Appointment of Cyber Inspector and their power to inspect, search, seize, and obtaining warrant	Unique requirement of the ECTA legislation

The results of the comparison are further analyzed and briefly discussed in the next section.

5.5.1 ISO 17799 and HIPAA standards

The HIPAA is only about the protection of one kind of information namely "health information" and ISO 17799 deals with the protection of all types of information.

The HIPAA security standards meet the ISO 17799 controls for 77 (or 55%) of the implementation requirements (quantified as a percentage of 127 ISO 17799 controls). The HIPAA security standards include 19 (or 14%) regulatory requirement for which it has a more stringent requirement than ISO 17799. Table 9 details those requirements and provides more information about various other HIPAA control measures that are not included in the ISO 17799. The ISO 17799 includes 26 (or 18%) controls that are not covered at all by HIPAA security standards; with 18 (or 13%) exceeding the HIPAA security standards requirements. This result demonstrated quite an overlap between the HIPAA

security standards and ISO 17799. This is not surprising because all three categories of HIPAA security standards (administrative, physical and technical) aim at ensuring the protection of the confidentiality, availability and integrity of health information which is exactly the same objective of ISO 17799, on the other hand, which however deals with all types of information.

The HIPAA privacy standards meet the ISO 17799 controls for 5 (or 3%) of the implementation requirements (quantified as a percentage of 127 ISO 17799 controls); with 28 (or 19%) of HIPAA regulatory requirements exceeding ISO 17799. These are explained in Table 10. There are 107 (or 71%) controls of ISO 17799 that are not covered by the HIPAA privacy standards; with 10 (or 7%) of ISO 17799 exceeding the privacy standards requirements. The main reason is because the privacy standards address the use and disclosure of the health information of individuals and control how it is used while the main objective of ISO 17799 is to ensure the security of all types of information. This is a major difference in focus between them.

The HIPAA Transaction and Code Set standards and ISO 17799 meets 1 (or 1%) control requirement; with 20 (or 14%) for which it has a more stringent requirement than ISO 17799. Table 11 details this requirement and provides more information about various other HIPAA Transaction and Code Set control measures that are not included in the ISO 17799. On the other hand, ISO 17799 contains 121 (or 83%) controls that are not covered by the HIPAA Transaction and Code Set standards; with 2 (or 2%) exceeding the HIPAA Transaction and Code Set standards. The raison d'être is because HIPAA Transaction and Code Set standards delves deeply into electronic data interchange which permits providers, carriers, payers and other entities to electronically exchange business data such as eligibility verification, enrollment, claim acceptance and claim status inquiries. ISO 17799 mentions fewer requirements on security of the media in transit in only one subsection, ISO 17799 (8.7 Exchange of information and software).

5.5.2 ISO 17799 and SANHA

The ISO 17799 meets SANHA with 7 (or 5%) control requirement; with 15 (or 11%) of SANHA regulatory requirements that exceed the corresponding requirements in the ISO 17799. This is detailed in Table 12 together with requirements included in SANHA but omitted from ISO 17799. On the other hand, ISO 17799 controls contain 14 (or 10%) exceeding SANHA; with 104 (or 74%)

requirements not covered at all in SANHA implementation regulatory requirements. These controls are not covered in SANHA at all. These results are not surprising because they have different objectives and coverage scope. The scope of ISO 17799 states: "This standard gives recommendations for Information Security Management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings" (ISO 17799); whereas the main objective of SANHA is to provide a framework for a structured, uniform health systems uniting the various elements of the national health system in a common goal to improve universal access to quality health services (SANHA).

5.5.3 ISO 17799 and ECTA

The ISO 17799 controls meet the ECTA for 5 (or 3%) and 99 (or 65%) of ISO 17799 security controls not covered by ECTA implementation regulatory requirements. ECTA contains 32 (or 21%) regulatory requirements that are not covered by ISO 17799, while ISO 17799 exceed 16 (or 11%) of the ECTA regulation requirements. Further requirements of the ECTA that are not covered in the ISO 17799 are expanded on in Table 13. The ISO 17799 specifies controls that should be in place to ensure the security of the information assets while the main focus of ECTA is to provide a framework for the facilitation and regulation of electronic communications and transactions. This is an over-arching difference in focus between the two. The reason is because the ECTA puts more focus on E-commerce issues, including the validity of electronically concluded agreements, the legal validity of electronic data, the admissibility of electronic documents in courts of law and the legal status given to electronic signatures which are not specifically covered in detail in ISO 17799.

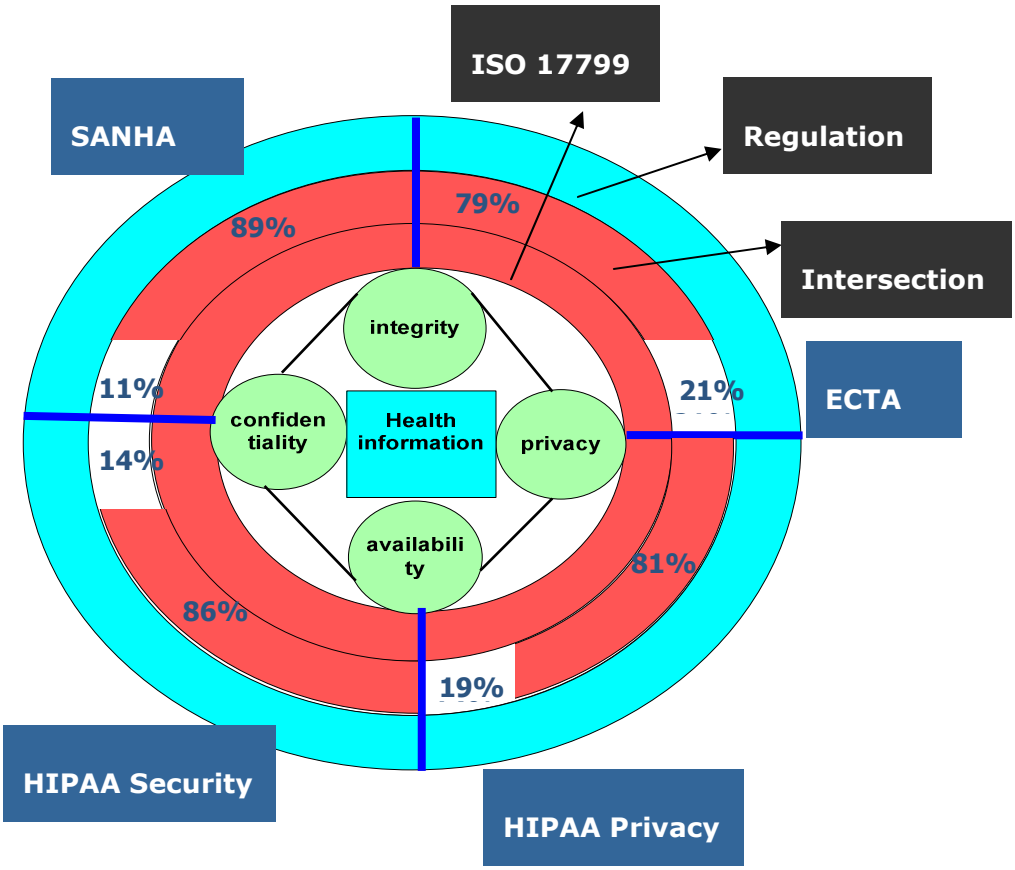
It is evident in all these comparisons, that most of these laws exceed ISO 17799 in one area specifically in *Section 12.1.4 Data protection and privacy of personal information* which requires those who collect, process and disseminate personal information to put in place controls for the protection of such information. This is because ISO 17799 is more security directed ensuring confidentiality, integrity and availability protection while the main objective of the laws investigated in this research is ensuring the privacy protection of the information of the customer. They therefore, delve deeply into disclosures and access to such information. This

further confirms the main objective of this research which requires convergence between the security standards and legal requirements as meeting one does not mean satisfying the other one. It can be inferred that a security and privacy model is needed based on the comparison result.

5.6 SECURITY AND PRIVACY PROTECTION MODEL

It was argued in Section 2.7 of Chapter two that the adequate protection of health information can only be achieved when an ISM standard framework is combined with regulatory requirements. Figure 17, illustrates the Security and Privacy protection model and highlights the three layers that must be in place to ensure the security and privacy of health information. Each of the three layers will be discussed next.

Figure -17- Security and Privacy protection model



In the **First layer**, organizations might use the ISO 17799 as a starting point for the identification of security controls and the regulatory requirements. Arguably,

there is no limitation to using this framework because an organization can choose from other frameworks such as the NIST standards or others. Moreover, because these security standards offer recommendations beyond the defined needs of an organization, they essentially comprise a "reservoir" of controls that compliance managers can tap as the need arises. Layer one contains controls that are unique to the ISM framework ie. Controls not covered in legislation.

The **Second layer** is composed of the intersection of the ISM framework and the regulatory requirements. The use of the proposed compliance model will clearly establish which regulatory requirements are already satisfied by the existing security framework and therefore should not be again dealt with. This layer contains those regulatory requirements exceeding the ISM framework. It is at this layer that management should focus to fulfill the gap of meeting with new regulatory requirements. These requirements are provided in Tables 9, 10, 11, 12, and 13. This layer contains all the controls of the ISO 1799 that are addressed in the legislation but to varying degrees.

The **Third layer** is composed of the unique regulatory requirements which were not addressed in the ISM framework.

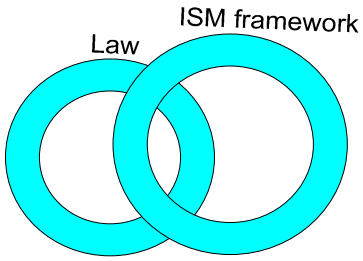
It evident that an organization already compliant with the ISO 17799 will requires fewer efforts to meet these previously mentioned ECTA, SANHA and HIPAA regulations when based on the comparison conducted and reported in Chapter five. The ethos of this proposed compliance model can be summarized as follow:

*In order to ensure **confidentiality**, **availability**, **integrity** and **privacy** of health information, healthcare organizations must implement common controls found in both security standards and regulation requirements plus regulation requirements not covered by the ISM framework add security standard controls exceeding regulatory requirements.*

It is crucial to mention, however, that the implementation of this Security and Privacy protection model must be driven by a risk analysis which determines which security measures are needed in a particular case. For example, the result of a risk analysis might require security measures found in the Layer one (security standard requirements not specifically required in legislation) and/or Layer two (common security measures) and/or Layer three (regulatory requirements specifically required by law).

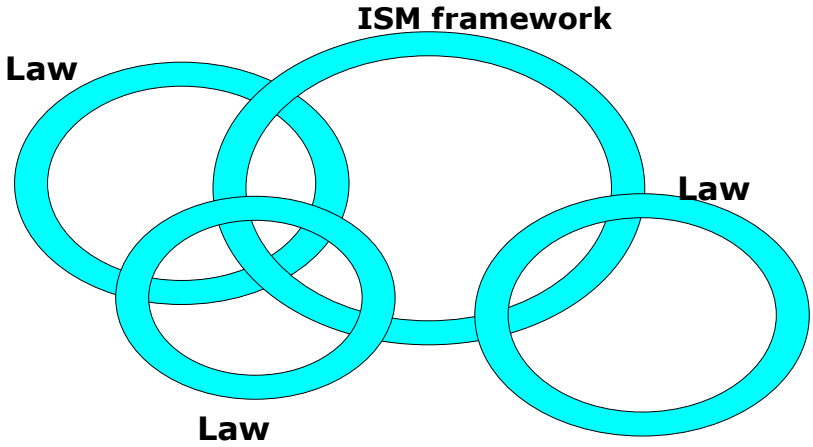
Compliance with new legislation can furthermore be demonstrated by using Set Theory as illustrated in Figure 18.

Figure -18- Compliance Set theory



The relevant regulatory requirements are for simplicity, represented as a single set label law which intersects with the ISM framework. The need to comply with multiple regulations will change this diagram dramatically in reality, to contain differing intersections between the various regulations, with each other and with the ISM framework.

The question that arises is that, is it possible to illustrate compliance with multiple laws with an ISM framework?



Executive management should be aware that there can be overlap between regulations themselves, for example SANHA and ECTA. However, a comparison between those regulations has not been done due to the constraints in scope of this project. Its main focus was limited to the comparison of the individual mentioned regulations with the ISO 17799.

5.7 CONCLUSION

There are a growing number of regulations, currently, that include requirements for healthcare organizations to provide security controls and demonstrate compliance assurance. The challenge encountered by most healthcare organizations is what compliance strategy should be followed to meet these regulatory requirements while ensuring that existing efforts already implemented are maintained (Tuyikeze & Pottas, 2005). There is a need to perform a comparison analysis between those standards and government regulatory requirements which reveal any similarities and differences to achieve this goal. The main objective of this analysis can definitely facilitate management to concentrate only on the missing controls instead of re-inventing the wheel by starting at the beginning in meeting new regulatory requirements.

It emerges clearly from the comparison that health organizations that are ISO 17799 - compliant exceed in both the requirements pertaining to HIPAA Security, Privacy, Transaction and code set standards and SANHA and ECTA regulatory requirements by far. Some effort will be required to ensure compliance with the issues listed in Tables 9, 10, 11, 12 and 13 containing regulatory requirements that South African healthcare organizations must take into account in endeavor to meet the government legal requirements while ensuring that due diligence, in adopting HIPAA standards and ISO 17799 standards, is not neglected.

It can be generalized from this comparison, that some legislation has quite an overlap with an Information Security Management program, such as the ISO 17799 and HIPAA. This confirms that a compliance strategy would serve well to eradicate redundancy while following an ad hoc approach to compliance with various standards and legislations. This provides advantages to the organizations through easy compliance with the new regulatory requirements and entails less effort while increasing the return on investments.

Chapter 5 demonstrates the existence of an overlap between security standards and regulatory requirements. This proves that there is a need for a compliance strategy ensuring the elimination of this redundancy; therefore reducing the complexity and costs associated with compliance to both requirements.

Chapter 6 provides a model for an Information Security management and regulatory compliance. Its main objective is to discuss the major phases of the proposed compliance model.

Chapter 6 A MODEL FOR INFORMATION SECURITY MANAGEMENT AND REGULATORY COMPLIANCE IN THE SOUTH AFRICAN HEALTH SECTOR

The main objective of this **Chapter 6** is to set up a roadmap for Information Security Management and regulatory compliance which ensures that organizations meet privacy regulatory requirements while simultaneously ensuring that best practices for protecting the information of customer are being used concomitantly. This represents the core of this research.

Chapter 7 concludes the research presented in this dissertation.

"…The existence and adequacy of the corporation's compliance program is one of eight factors federal prosecutors consider in deciding whether to even charge a corporation for its wrong-doing under criminal statutes."

U.S. Department of Justice Memorandum, 2003

6.1 INTRODUCTION

Organizations are functioning, globally in a most complex and challenging era of Information Security Management and regulatory compliance requirements. The Information Security and privacy regulatory environment grows more stringent and complicated every day (Teller-Kanzler, 2005). There is inter-trading between companies and they struggle to demonstrate adequate levels of risk-reduction across geographically and functionally diverse business units, each with unique technical and operational challenges. It is no longer enough to manage the security of organization to meet internal standards and policies (Cybertrust, 2004). Additionally, the proliferation of international and nation-specific regulation and standards has become a major concern for executive managers dedicated to demonstrating regulatory compliance. Security incidents, security audits and new regulations are the primary drivers influencing the evolution of Information Security and regulatory compliance according to industry analysts (Bindview, 2005). Business executives and industry analysts, currently, acknowledge that these drivers are interconnected and it is imperative that organizations resolve them through a more holistic approach.

The primary responsibilities of security executives and managers have become overwhelming (Bindview, 2005). They are responsible for securing multiple technologies within a complex and often, global environment. These technologies are constantly changing and new technologies are emerging. Further, they need to build security policies and ensure these policies are understood and followed by employees and contractors. Most importantly, they need to understand the regulations applicable to their business and ensure their organization can demonstrate compliance. Executive managers face an ever-expanding number of critical demands yet they work in an environment where failure is not an option (Vericept Corporation, 2004). Furthermore, a company that experiences a

security breach can suffer significant damages on many levels, including the loss of investor and customer confidence (Unerman & O'Dwyer, 2004). The Executives may be subject to criminal and civil penalties in a case of regulatory compliance failure (Trillium Software, 2004). These pressures can negatively impact the business goals and IT operations of an organization if not appropriately dealt with. Therefore, Executive management are required to carefully inspect the major challenges related to compliance in terms of legal, regulatory and standards.

6.2 CORPORATE COMPLIANCE CHALLENGES

Compliance encompasses behaviors and activities that assure an organization is properly satisfying applicable legal requirements and other standards according to EMC (2005). Organizations must comply with the specific standards or business practices to which they make a commitment to mitigate legal risks and increase investments of stakeholders. These compliance requirements can be external such as, laws and regulations through contracts or industry standards to which the organization subscribes. Additionally, corporate compliance includes meeting internally-defined company policies and other commitments to internal and external stakeholders that go beyond what is legally required. Corporate compliance is with ensuring that the organization is meeting all its compliance commitments. Considering this statement, Organizations are required to conduct their affairs in a particular way which clearly demonstrates evidence of its business conduct (King Report, 2001). This is difficult to accomplish in this increasingly litigated environment with various corporate practice requirements.

BindView (2005) states that while compliance with regulations is a major issue facing businesses today, many IT security executives are confused about what specifically they must do to achieve compliance. The result is that they can easily allocate either too much or too little staff time, money and outside consulting resources, pursuing a seemingly elusive goal. The explosion of legislation regarding the privacy and security of information is having a profound effect on organizations of all sizes and shapes (Kolodgy & Christiansen, 2005). These laws, in combination with less formal standards agreed to among nations and organizations across the world, are driving Executives and Boards of Directors to inspect details previously ignored (netForensics, 2005). The consequences for non compliance according to Unerman & Brendan (2004), can result in penalties, loss of trust of shareholders and increase in cost of compliance. These are discussed in the following scenario.

6.2.1 Consequences of corporate governance failure

The violation of legal or corporate practices requirements can result in serious consequences for a business, its employees, officers or directors – including fines, penalties, loss of revenues, government contractor "blacklisting", business interruption, negative media coverage, reputation damage and loss of trust of shareholders (EMC, 2005). Some apt examples illustrating this statement include the cases of Enron Corp, WorldCom Inc and other organizations that failed to demonstrate good corporate governance practices and these resulted in numerous consequences even to the bankruptcy of the whole organization.

6.2.1.1 Enron, WorldCom, Andersen et al.

Enron grew during the nineties from a relatively-small domestic Texan energy company to become one of the largest US corporations with an array of energy trading and utility operations world-wide (Unerman & O'Dwyer, 2004). At the time of its collapse in 2001, Enron Corporation was listed as the seventh largest company in the United States, with over $100, 000 billion in gross revenues and more than 20,000 employees worldwide (Sloan, 2002). However, in October 2001, it shocked the stock market by announcing accounting 'adjustments' leading to a substantial loss for its third quarter of $618 million and a reduction in its reported net asset value of approximately $1.3 billion (Hill et al, 2001). Further revelations of aggressive earnings management practices, involving a complicated system of off-balance sheet operations, hiding large scale of losses and liabilities were made over the following weeks. Sloan (2002) confirms that Senior Executives at Enron had set up approximately 3500 off-balance sheet partnership, partly owing and benefiting from at least two of them and therefore, causing a clear conflict of interest between the shareholders. Enron Corp, two months later, became the largest bankruptcy case in US history, with estimates of outstanding liabilities ranging up to $55 billion (McLean, 2002). The losses, as a result, claimed so far by public pension funds are approaching $2 billion (News Batch, 2005).

Kenneth Lay, who served the chief executive of Enron for 15 years, was finally indicted in July 2004. Lay was charged with conspiracy to commit securities fraud, four counts of securities fraud, two counts of wire fraud, one count of bank fraud and three counts of making false statements to a bank (Kleinbard, 2005). After collapse of Enron, numerous official enquiries were launched to find out the truth and the company be put in the hands of auditors.

Enron had been audited by Andersen, one of the top five global multinational accounting and auditing businesses at that time (Unerman & O'Dwyer, 2004). Allegations were raised that, in January 2002, following the launching of Security and Exchange Commission (SEC) investigations into accounting practices at Enron, Andersen had systematically destroyed many of its working papers relating to this client (Unerman & O'Dwyer, 2004). In addition, further investigations showed that Andersen had actively played a central role in devising the aggressive earnings management techniques employed by Enron; for example, Andersen generated more fees in 2000 from selling consulting services to Enron ($27 million) than it did from auditing their accounts ($25 million), thereby exposing it to the accusation of conflict of interest that resulted against the auditing profession (McLean, 2002). The consequences of these revelations led to an apparent rapid loss of faith in Andersen, with many clients switching to other large accounting firms. The drawback of this withdrawal of trust quickly resulted in the collapse of their recognition to conduct audits and most of their clients being taken by its competitors (Unerman & O'Dwyer, 2004).

A series of other large companies subsequent to the Enron failure faced allegations of misleading accounting practices and the mismanagement of the interests of shareholders. WorldCom, On 21 June 2002, beat the bankruptcy record set less than eight months earlier by Enron. This new 'largest ever' bankruptcy followed revelations that the Andersen audited company had fraudulently capitalized $3.85 billion of revenue expenditure as capital expenditure, thereby, perpetrating what some called 'the largest accounting fraud in history' (Doward, 2002). A Manhattan federal jury, after some investigations, convicted former WorldCom chief executive, Bernie Ebbers, of criminal charges for masterminding an $11 billion fraud that sent the company into bankruptcy (Kleinbard, 2005). Ebber, the CEO of WorldCom, testified in his own defence, claiming he was unaware that his subordinates were mismanaging the financial accounting books for 18 months (News Batch, 2005). During the trial, his former Chief Financial Officer, Scott Sullivan, confirmed it was Ebbers who instructed him to hide expenses and overstate the revenue beginning, in 2000, so that the company could meet Wall Street expectations. Ebbers faces sentencing of up to 75 years and could spend the rest of his life behind the bars (Kleinbard, 2005).

Among other companies that had similar scenario of compliance failures were: Tyco, PNC Financial Services, Invesys, Xerox, General Electric, IBM, JP Morgan Chase and Global Crossing in the US, Shell and Centrica in the UK and Vivedi in

France (Serwer, 2002). According to Unerman & O'Dwyer (2004), the main reason for the failure of these companies was related to the mismanagement of accounting practices and non-experts auditors resulting in mistrust of shareholders loosing interests in their companies. One commentator claimed generally: "…this is the biggest crisis investors have had since 1929; they don't know who they can trust" (Unerman & O'Dwyer, 2004).

It can be summarized that in most of these corporate governance practices failure, the consequences become apparent such as the loss of trust by the shareholders, bad reputation for the company and stiff penalties for the executive managers (Vericept Corporation, 2004). These organizations failed to demonstrate the major characteristics of good corporate governance such as, transparency, openness and fairness in the way that they manage their organization. Those characteristics were discussed in section 1.1 of chapter 1 and constitute the principal drivers of any organization willing to increase its business value and its return on investment.

Governments around the world have enacted laws and regulations imposing penalties and sanctions with regard to the violations of legal requirements to force organizations to ensure good corporate governance, integrity and accountability of the assets of shareholders.

6.2.1.2 Legislations intervention and their consequences

The governments and regulators have responded to cases such as, Enron, Andersen Consulting and WorldCom with laws like Sarbanes-Oxley that mandate new standards for corporate accountability and transparency and for information management and the privacy of such information (Blair, 2005). The Sarbanes – Oxley Act of 2002 requires more auditing oversight and requires CEOs and CFOs to certify their financial results or suffer severe personal penalties. For example, Section 404 requires each annual report of an issuer to contain an "internal control report", affirming the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. It contains an assessment of the effectiveness of the internal control structure and procedures that must be certified by the public audit firm of the organization. The government of the USA has imposed penalties of a fine up to $500,000 or imprisonment of up to five years as stated by SOX 404 to ensure

that this section is not violated. Table 14 provides examples of the legal offences and the penalties resulting for their violations.

Table -14- Legislation offences and penalties

Law	Offence and penalty
HIPAA privacy rule	Federal penalties of up to $50000 and one year imprisonment can be levied for knowingly obtaining or disclosing personal health information. A stiffer penalty of up to $100,000 and five years imprisonment could result if the misuse is under false pretence; and up to $250,000 and 10 years of imprisonment for obtaining or disclosing protected information with the intent to sell, transfer or use for personal or commercial gain or to cause malicious harm.
HIPAA security rule	Civil penalties include a $100 per person per incident fine with maximums of $25000 per person for each standard within a single year.
ECTA	
Chapter V - *Cryptography Providers*	32(2) A person who contravenes or fails to comply with a provision of this chapter is guilty of an offence and liable, on conviction, to a fine or to imprisonment for a period not exceeding two years.
Chapter VII – *Consumer Protection*	*45(4) A*ny person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1)
Chapter XII – *Cyber inspectors*	84(2) Any person who contravenes subsection (1) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding six months.
Chapter XIII – *Cyber Crime*	89(4) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.
SANHA	
Chapter 2 – *Right and duties of users and healthcare personnel*	17(1) Any person in charge of health establishment, in possession of the health records of a user must set up control measures to prevent any unauthorized access to those records and to the storage facility in which, or system by which, records are kept. Failure to meet this section results in an offence and liable, on conviction, to a fine or to imprisonment for a period not exceeding one year or to both a fine and such imprisonment.

Organizations are spending money to meet these regulatory requirements compliance in order to remain out of legal trouble in response to these penalties imposed by legal and regulation. A possible down-side, however, is that meeting new regulatory demands can have a serious negative impact on cost and time efforts assigned for meeting them if not carefully scrutinized.

6.2.2 The cost of being compliant

The need to comply with multiple regulations has taken effect in most countries worldwide currently. Consequently, this urgent need has led to a dramatic rise in compliance spending (Bindview, 2005). The U.S.A will spend nearly $15.5 billion on compliance-related activities in 2005, according AMR Research (2005); with the total cost for compliance estimated at $80 billion over the next five years. This research further confirms that spending on SOX alone will exceed $6 billion in 2005 with $2.6 billion of this total amount paying internal personnel devoted to compliance, while another $1.7 billion is being spent on consultants and external audits firms (AMR Research, 2005). The increase of regulatory compliance is without exception even in South Africa, as illustrated in the survey conducted by the Strategic Partnership for Business growth in Africa (SBP) between February and June 2004 and who released its main report "Counting the costs of red tape for business in South Africa" in 2005.

During the survey of SBP, a total of 1794 businesses were interviewed, in depth, on the costs of regulation to the South African private sector. The survey covered all the sectors of the economy including manufacturing, mining, construction, trade, agri-business and services. It examined in detail two types of regulatory costs faced by the private sector called; **Efficiency costs** and **Compliance costs** (SBP report, 2005). Efficiency costs rise because regulation may distort market outcomes. If employment is discouraged by inappropriate labour market regulation, for example, then the costs of the resulting unemployment in terms of lost output and incomes is an efficiency cost. The Compliance cost is interesting as it covers the incremental costs incurred by business in the course of complying with regulations. They include the value of time spent by business managers and staff on understanding the rules and applying them; interacting with the authorities to clarify matters arising from; and the payments made for the expertise of professional advisers, such as consultants, lawyers, and accountants (SBP report, 2005). It was discussed in Chapter 5 Section 5.2, that with the increase of numerous legislations which can result in an overlap of security

measures requirements and the time devoted to meet those requirements can be overwhelming if not carefully considered and dealt with to remove these redundancies.

The result of the survey reveal that based on the average recurring Compliance costs per firm of R105 174 and the estimated of 750 000 firms affected, this results that aggregate recurring Compliance costs for the formal sector amounted to R78,9 billion in 2004 – an amount equivalent to 6,52 percent of GDP. The report states that large firms pay the most in absolute terms but regulatory compliance costs are regressive: they weigh more heavily on smaller enterprises because of the lack of sufficient resources dedicated at ensuring compliance. It was revealed in this survey that, in general, South Africa is going through a period of rapid compliance inflation because 76 % of businesses surveyed state that compliance costs have increased in the past two years (SBP report, 2005).

The question is not whether organizations will spend on regulatory compliance because not meeting regulatory requirements is not an option. The consequences of non-compliance and the harsh penalties imposed by regulators means, the likelihood is that organizations will spend and keep the regulators from knocking at their doors. The more pressing question is whether they will spend wisely and effectively, driven by a well established compliance strategy program, rather than by crises. A compliance model is established in Section 6.3, which provides a solution by removing redundancy in the compliance to various regulations and, therefore, presents a method of reducing unnecessary costs.

6.3 A COMPLIANCE MODEL FOR THE SOUTH AFRICAN HEALTH SECTOR

"The strategy for employing the army is not to rely on their not coming, but to depend on us having the means to await them. Do not rely on them not attacking, but depend on us having an unassailable position."

- Sun-Tzu, The Art of War -

While considering this statement, how can an organization ensure that it is in a position to convince its customers that best practices are being used while it is meeting regulatory compliance? The major challenge is to discover a balanced way of meeting compliance using less effort and resources. It is necessary to adopt a unification process, aimed at reducing redundancy, while providing numerous advantages to the organization to solve this problem.

This section provides the description of the compliance model for Information Security Management and Regulatory Compliance in the South African Health Sector which is the principal intention of this project. Please refer to fold-out Figure 20 at the end of this chapter for the graphical representation of the compliance model.

The objective of the compliance model is not to drill down deeply into details of its phases as shown in Figure 20. This is beyond the scope of this research. The idea is to rather to establish a roadmap that Executive managers should follow to meet regulatory compliance while ensuring customers that best practices for Information Security Management are being used. A brief explanation of each phase of the model is provided.

6.3.1 Phase 1 – Identify the scope of compliance

The organization must identify the scope of the compliance, for example which standards, regulations, best practices, etc… are included as part of the compliance effort in the First phase. This research argued that an Information Security Management framework is required together with regulatory requirements. A model for Information Security Management and Regulatory Compliance in the South Africa context would, therefore, use the ISO 17799 as a

base for Information Security Management and would have to incorporate the ECTA and SANHA from a legal perspective. In this research, HIPAA compliance was recommended as a best practice.

6.3.2 Phase 2 – Determine the implementation requirement of ISM framework

After the scope of compliance has been identified, the next step is to determine the implementation requirements of the Information Security Management framework. The ISO 17799 operates using 127 security controls which are grouped into 36 sub-objectives. The main objective of this phase is to ensure that level of the implementation requirement of the ISM is at a level comparable with the regulatory requirements. For example, the 36 sub-objectives of ISO 17799 are not on the level comparable with SANHA security measures requirements.

6.3.3 Phase 3 – Identify the regulatory unit of comparison

A unit in each regulation is identified, which could be used as a point of reference for the comparison with the framework of the ISM implementation requirement chosen for Phase 2. This should be at the level comparable with the ISM framework to ensure that we are comparing "like with like". For example, the 42 HIPAA security measures are on a level comparable with ISO 17799 security controls. This is illustrated in Table 15.

Table -15- Example of ISO 17799 security control in comparison with HIPAA security measure

Standard / Regulation	ISO 17799 Security Control/HIPAA Security measure	Specification
ISO 17799	6.3.5 Disciplinary Process	There should be a formal disciplinary process for employees who have violated organizational security policies and procedures. Such process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures. Additionally, it should ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security.
HIPAA Security Rule	164.308(a)(1)ii(C) Sanction Policy	Sanction must be applied against employees who do not comply with the defined policies and procedures.

The ECTA and SANHA legislations are composed into chapters which are at high level specifications and not worthwhile to be compared to the low level security controls of ISO 17799. It therefore, makes sense to drill down to their specific rule requirements in the process of finding the unit of comparison with ISO 17799 security controls. For example, the ECTA regulation requirement *56.Restrictions on disclosure of information* is on the level comparable with the ISO 17799 control *8.6.4 Security of system documentation* while its main Chapter IX **Protection of critical Database** is not comparable with this control.

6.3.4 Phase 4 - Comparison

Once the implementation requirement of the ISM framework and the unit of comparison for the particular regulation are identified, the next stage is dedicated to their comparison. A graphical representation of the comparison methodology is provided in Figure 19. The steps are numbered and comprise the following actions:

1) List the controls of the ISM framework; these controls constitute the basis to work from.

2) Select the legislation for use during the comparison keeping in mind that there are multiple laws to be used, in this case, SANHA, ECTA and HIPAA rules.

3) Identify regulation requirements of the selected legislation in Step 2.

4) Make a comparison between the regulatory requirement and the identified controls of the ISM selected in Step 1. This comparison occurs only if the two are at a comparable level.

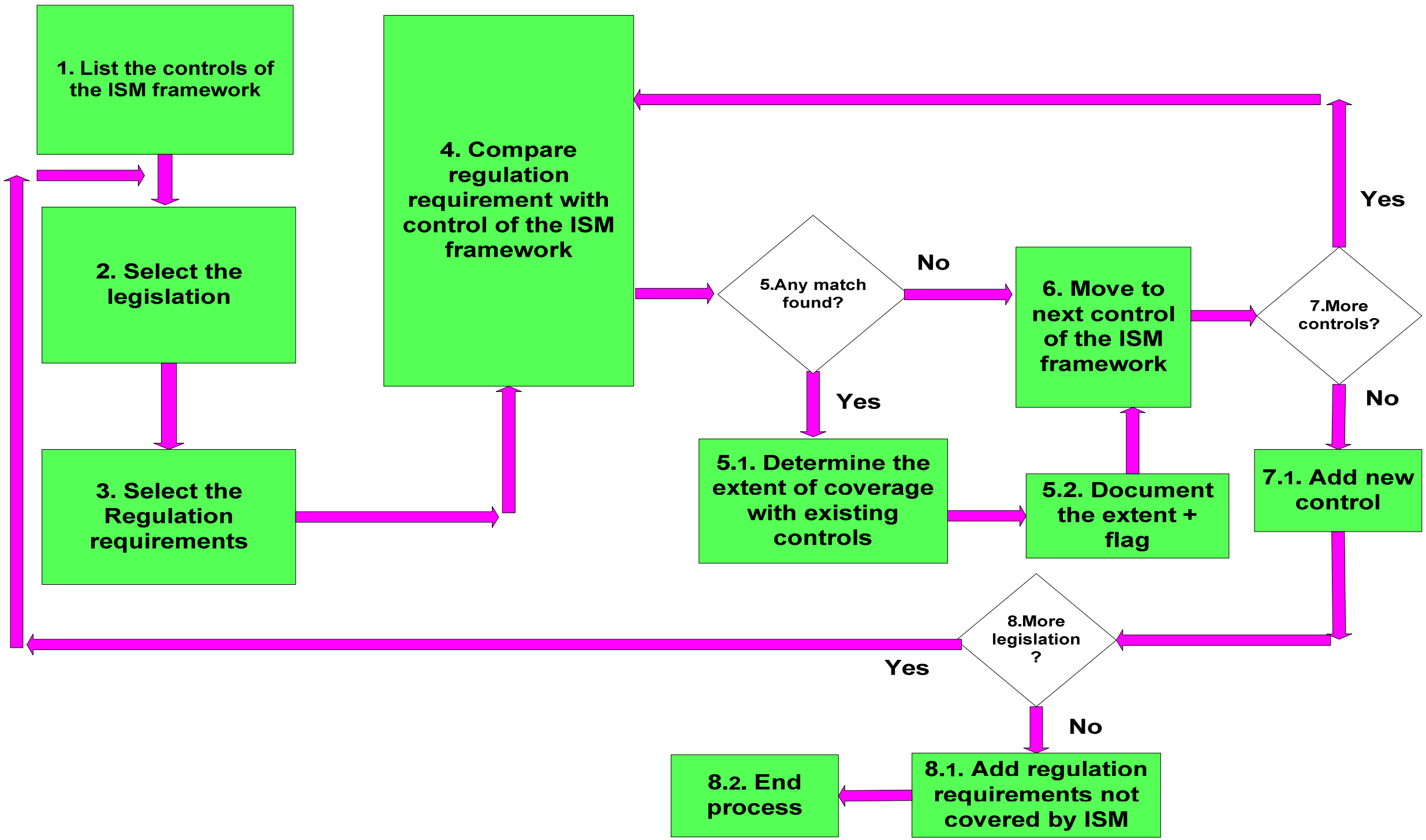
5) Verify that the regulatory requirement and the implementation requirement of the ISM have the same meaning. A match implies an already existing control. Additionally, consideration should be given to the extent that the new regulatory requirement meets with the existing security control (Partially Covered or Exceeding the security control). The coverage is documented and flagged ensuring that the new control security control is not added to the previous comparison. This removes redundant regulatory requirements that might exist between the various legislations.

6) Identify to next control of the ISM framework, and verify if it is the last security control.

7) If the control is not the last one, return to Step 4 and repeat the process; else add the new control if is not flagged as a previously found control.

8) Verify if there is more legislation to comply with; if the answer is "Yes" then restarts the process from Step 2 and make a new comparison; else Add all the regulation requirements not covered at all by the ISM framework plus regulation requirements exceeding the ISM (these were documented in Step 5). The comparison has been successful accomplished.

Figure -19- Comparison methodology (Phase 4 of the Compliance Model)



The output of Phase 4 provides the result produced in the **Appendix A**. The organization should then move to the critical stage of selecting controls that must be implemented.

6.3.5 Phase 5 - Selection of controls

Organizations need a flexible means to identify, introduce, manage and maintain an effective set of security controls in this dynamic regulatory environment. The following proposes an approach that can be followed in identifying and selecting controls meeting regulatory requirements and the best practices commitment of an organization.

6.3.5.1 Prioritized security controls

It was previously mentioned that not meeting regulatory requirement is not an excuse for an organization. Therefore, priority should firstly be given to all mandatory regulatory requirements. It was discussed in Chapter 4 Section 4.5, that HIPAA differentiates between "**Required**" and "**Addressable**" specifications. Required specifications are compulsory ones while Addressable are optional that can be implemented when needed by the organization. A regulatory requirement that is marked "Required" and not found during the comparison must be selected. A good example to illustrate this is shown in the **Appendix A**: *164.308(a)(4)ii(A) Isolating Healthcare Clearinghouse* is a Required specification of HIPAA Security Rule and is not covered by ISO 17799. The organization must ensure that this security measure is added to avoid any legal problems. The same approach should be followed for the ECTA and SANHA regulations. These legislations do not specifically mention compulsory and optional regulatory requirements. They do allude to some requirements that an organization must implement to circumvent any legal difficulties. Michalson (2004) argue that only six of the 14 chapters of ECTA mention a fine or imprisonment for those convicted of an offence under the Act. Therefore, such regulations fall in the category of non-optional requirements because non-compliance can result in committing an offense which could incur a fine or other legal sanction. The regulatory requirements of these chapters were discussed in Section 4.5 of chapter 4. The second category of selection of security controls is composed of best practices and optional regulatory requirements.

6.3.5.2 Best practices security controls and optional regulatory requirements

The selection of security measures to meet optional regulatory specifications and best practices requirements should be driven by a **Risk Analysis** which is a subset of **Risk Management**. World & Shriver (1997) defines Risk Analysis "as a process that involves identifying the threats, which are most likely to have a significantly negative impact on an organization as well as scrutinizing the associated vulnerabilities of an organization to those threats". The main intention of Risk Analysis is to determine which security controls are needed, depending on which risks the organizational information is exposed to. ISO 17799, on the selection of controls, states that "Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occur. Non-monetary factors such as loss of reputation should also be taken into account" (ISO 17999). This can only be accomplished by a Risk Management plan aimed at identifying, assessing, evaluating and implementing risk-reducing security measures.

The National Institute of Standards and Technology SP800-30 (2001) defines Risk Management as a process enabling the achievement of equilibrium between the operational and economic costs associated with protecting organizational assets from the Risks affecting IT, while attempting to achieve their business goals. Therefore, Risk Management essentially focuses on the selection and implementation of assorted and appropriate security controls to effectively manage the IT-related risks of an organization. Humphreys et al. (1998) suggest that the cost of implementing specific types of security controls is more involved with whether they are cost-effective. NIST SP800-30 (2001) even goes further by stating that allocating resources and implementing cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control determining which controls are required and appropriate for their circumstances. This is understandable because it does not make economic sense to apply controls, should their costs exceed the value of the assets they are protecting or the budget that an organization has allocated for security.

The HIPAA Security Rule, to emphasize on the importance of risk analysis and risk management, has imposed them as compulsory to ensure compliance. The required implementation specification 164.308 (a)(1)(ii)(A), for **Risk Analysis**,

states that "Every covered entity **must** conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the *confidentiality*, *integrity*, and *availability* of electronic protected health formation held by the covered entity." Furthermore, the required implementation specification 164.308(a)(1)(ii)(B), for **Risk Management**, requires that "Every covered entity **must** implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the security rule. Both Risk Analysis and Risk Management requirements are marked "**Required**" indicating that they are not optional. It was stated in the responses to public comment in the preamble to the HIPAA Security rule that Risk Analysis and Risk Management are important to covered entities since these processes will "form the foundation upon which an entity's necessary security activities are built" (CMS, 2005).

The COSO (2004) framework further defines the overall process of Risk Management by stating that: "Risk management is a process, effected by a entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of company objectives."

This definition clearly illustrates that Risk Management is a process that is accomplished by the Board of Directors, management and all other personnel in the organization. The Board of Directors is ultimately responsible for ensuring that the risk management practices of their organization are effective and it is necessary that management ensures that various Risk Management strategies are properly implemented and executed within the organization on a daily basis (King Report, 2001). This definition illustrates that Risk Management should be conducted within the Risk Appetite of the organization in order to achieve its objectives. Although, it is possible to reduce the risk to an acceptable level, it can be impossible to eradicate it completely and therefore, some residual risks will remain (Humphrey et.al, 1998).

It can be generalized that Risk Management is critical to organizations committed to reducing risks occurrences to an acceptable level. Thus, it becomes necessary for the Executives Managers to understand what is required of them in terms of Risk Management and Risk Analysis as part of their corporate governance duties to ensure that risks are kept to a minimum level and therefore, guarantee the

stakeholders that their interests are adequately preserved as effectively as possible.

The way that an organization may decide to deal with the risks in reality, will depend on the type of the risks that is currently facing and its available resources. Whitman & Mattord, (2003) suggest that prior to deciding on a particular strategy for dealing with the risk, an organization should conduct a feasibility study with the main intention of answering this question: "What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages of not implementing such control?" The answer will help management makes decision about whether a risk is negligible or should be taken into account.

In addition to selecting controls based on a risk analysis result, Mash (2002) further proposes that by identifying which controls are in place and their effectiveness at reducing the risk, requires an understanding of the controls themselves. For example, the locks on doors reduce the risk of unauthorized access to a building but adding iris scanners could reduce this risk even further. However, the threat may not require this additional risk reduction or its cost might be higher than the value of the assets being protected, in which case, the additional control would be negative and the cost of maintaining the control considered unnecessary expense. Therefore, organizations should carefully consider existing security controls rather than randomly selecting and implementing them.

6.3.6 Phase 6 - Implementation

Once the selection of security controls has been successfully accomplished, the next step is devoted to their implementation. This step focuses, in general, on the formal creation of an Information Security program. ISO/BS 7799-2 highlights that such a program shall include "documented statements of the security policy and control objectives; the scope, procedures and controls of the ISMS; Risk assessment report and risk treatment plan; and documented procedures needed by the organization to ensure the effective planning, operation and control of its Information Security processes".

A compliance program, according to EMC (2005) imposes the responsibility to confirm with documentary evidence that the business complies with laws, regulations and other standards and commitments applicable to that company.

However, a perfect compliance program is of marginal use and will afford little risk protection if its policies and procedures are not implemented and enforced (Westby, 2005).

6.3.7 Phase 7 - Auditing

The next stage, after the implementation stage, should be dedicated to checking and ensuring that implemented security measures meet the commonly agreed or expected standards or values, legal and regulatory requirements and that they are performing their activities in an appropriate, correct and acceptable way. This can be accomplished by conducting an **internal** and **external auditing**.

Langelier & Ingram (2001) generally defines an Information Systems Security audit as "a process that involves providing independent evaluations of an organization's policies, procedures, standards, measures and practices for safeguarding electronic information from loss, damage, unintended disclosure, or denial of availability". This definition clearly highlights that evaluating security measures is one of the main aspects of an audit plan. It is illogical to call external auditors to audit an Information Security Management System without first evaluating and verifying that the security involved in protecting such information is appropriate and adequate. Any failure to comply or to provide auditable records depending on the regulatory requirement can have serious financial and legal consequences. These consequences are in addition to the liabilities caused by compromised data, damaged reputation, loss of trust and the harsh penalties faced by Executive Managers, as described in the case of Enron and other previously discussed cases. Therefore, it becomes necessary to perform an internal audit before the external auditors are summoned. The function of internal auditors is complementary to, but differs from, that of the external auditors. Organizations want to judge their performance against their mission and targets apart from the external check. The internal audit report provides an overview of the various strong and weak points in the effectiveness and efficiency of the organization, for instance, so an improvement program can be developed or existing policies and procedures can be adjusted.

The external auditors, on the other hand are independent of the internal organization unit who conduct an investigation to establish the existence of an equal balance between the security measures and the standards and regulatory requirements that the organization is supposed to ensure compliance against.

(King Report, 2001) confirm that the role of internal and external auditor is different. External auditors have a statutory duty to report their independent opinion on the financial statements to the shareholders of the organization, consider statutory requirements and standards for financial reporting and auditing. This contrasts to the internal audit function, which is a service to the company. It focuses on the internal control framework and reports to the Senior Executive Management and the audit committee (King Report, 2001).

Internal auditing can be considered as a preparatory phase that aims at reducing external audit efforts and helps to achieve external auditing efficiency because most of the tasks are already performed by the insider auditors and only require confirmation with evidence from the external, independent auditors.

The organizational internal audit function should provide a report to intended recipients upon the completion of the audit work. Westby (2005) states that an audit report contains the scope and objectives of the audit, the period of coverage, the nature and extent of the audit work performed and the associated audit standards. The audit report states the findings, conclusions and recommendations concerning the audit work performed and any reservations or qualifications that the auditor has with respect to the audit.

There can be, however, confusion between auditing and monitoring. Monitoring is a current activity and normally involves active, current data. Whitman & Mattord (2003) further confirm that auditing is the process of reviewing the use of a system, and not performance checking. Hensley (2003) states that the difference between monitoring and auditing is that, auditing is primarily "an after-the-fact" and determines if misuse or malfeasance has occurred; whereas monitoring is a current, ongoing activity.

However, Executive Management should realize that a good audit result does not imply an end to the compliance process. There is still the need for regularly checking ensuring that the implemented security operates efficiently as possible. This is accomplished through the reviewing and monitoring process.

6.3.8 Phase 8 - Review and Monitoring

Executive Management should not assume that their duties are completed once the security measures of the organization have been audited, and that the Information Security Systems will continue working perfectly. Executive

managers should realize that being currently secure does assure future security. There is no control system which is entirely effective (ACL, 2005). Furthermore, the pressures of growing workloads and increasing business complexity can make it operationally expedient to circumvent controls. Security measures available in an organization may be overlooked or simply not implemented due to cost, time and efficiency pressures (ACL, 2005). It is necessary that an organization demonstrates that it has implemented the necessary security measures and, that they are operating properly and providing the intended protection for critical information. The ideal solution enables a proactive, ongoing approach to protection, with in-depth reviewing, monitoring, assessment and analysis that correlates to the organizational risk posture, both from internal and external perspective. One major goal of monitoring is to identify problems before external auditors discover disparities in the audit results or they become more serious (Langelier & Ingram, 2001).

Executive Management should furthermore, realize that managing Information Security is a journey not a destination. It is a continuous process. New changes such as new laws requirements and new threats may arise at any time during the course of the business. It is necessary to implement new controls or enhance existing ones to mitigate those new threats and stay compliant with the new regulatory requirements.

The end-result of the auditing and monitoring process must be reported to Executive Management so that precautions can be taken against the problems discovered.

6.3.9 Phase 9 - Reporting

The last step in the Compliance process is Reporting. Once the organization has accomplished the Review and Monitoring process, the information produced should be compiled into reports to alert management to its findings. A well established Reporting system allows a organization to establish whether it has achieved its desired compliance levels and demonstrate to its auditors that it has taken significant steps to demonstrate its compliance efforts.

The reports should be issued in a timely manner allowing management a period in which to take corrective actions before they turn into penalties. They should inform interested parties such as, stakeholders, about current compliance status of the organization.

6.3.10 Phase 10 – Documentation and Awareness

It is necessary to highlight that there are basic requirements that must be performed during the process of a compliance program. These are the **Documentation** and **Awareness** of the implemented corporate compliance program. BS 7799 (1999) generally recommends that the ISMS documentation includes:

a. Documented statements of the security policy and controls objectives;
b. The scope of the ISMS, procedures and controls in support of the ISMS;
c. Risk assessment report;
d. Risk treatment plan;
e. Documented procedures needed by the organization to ensure the effective planning, operation and control of its Information Security processes.

EMC Corporation (2005) argues that "in order to successfully meet a company's compliance obligations, there is a fundamental, ongoing responsibility: *To preserve the business records that demonstrate the company's conduct has satisfied the relevant requirements*". Furthermore, documentation has arguably become a priority for auditors (Bindview, 2005). Proctor (2004) stated that "*Auditors aren't simply going to ask you or not you have got controls anymore. They are going to want to see documentary evidence to that effect and in may instances will want to come on-site to test them*".

Risks can not be managed and organizational assets can not be protected when a security plan is implemented only through documentation and security management software (Westby, 2005). It is evident that a compliance security program must be communicated to all employees from the top management to lower-level employees. Personnel can not be held accountable if they were never aware of what was expected of them. Therefore, it is necessary that the organization has in place mechanisms for training in Information Security related issues to increase security awareness.

6.4 CONCLUSION

The Information Security and privacy regulatory environment, currently, grows more stringent and complicated every day. Organizations are required to ensure compliance with new regulations requirements which complicate the situation. Compliance with regulatory requirement is a mandatory requirement for a

particular organization and ignorance of the legal requirement is not considered an excuse. Such compliance failure can result in heavy consequences such as, the loss of shareholder trust, a bad reputation for the company and stiff penalties for the Executive Managers as illustrated in the case of Enron and other organizations that failed to demonstrate good corporate governance practices. Organizations are required to spend excessively to ensure compliance and avoid such legal troubles. The question is not whether organizations will spend on regulatory compliance; but whether they will spend wisely and effectively, driven by a well-established compliance strategy program rather than by crises.

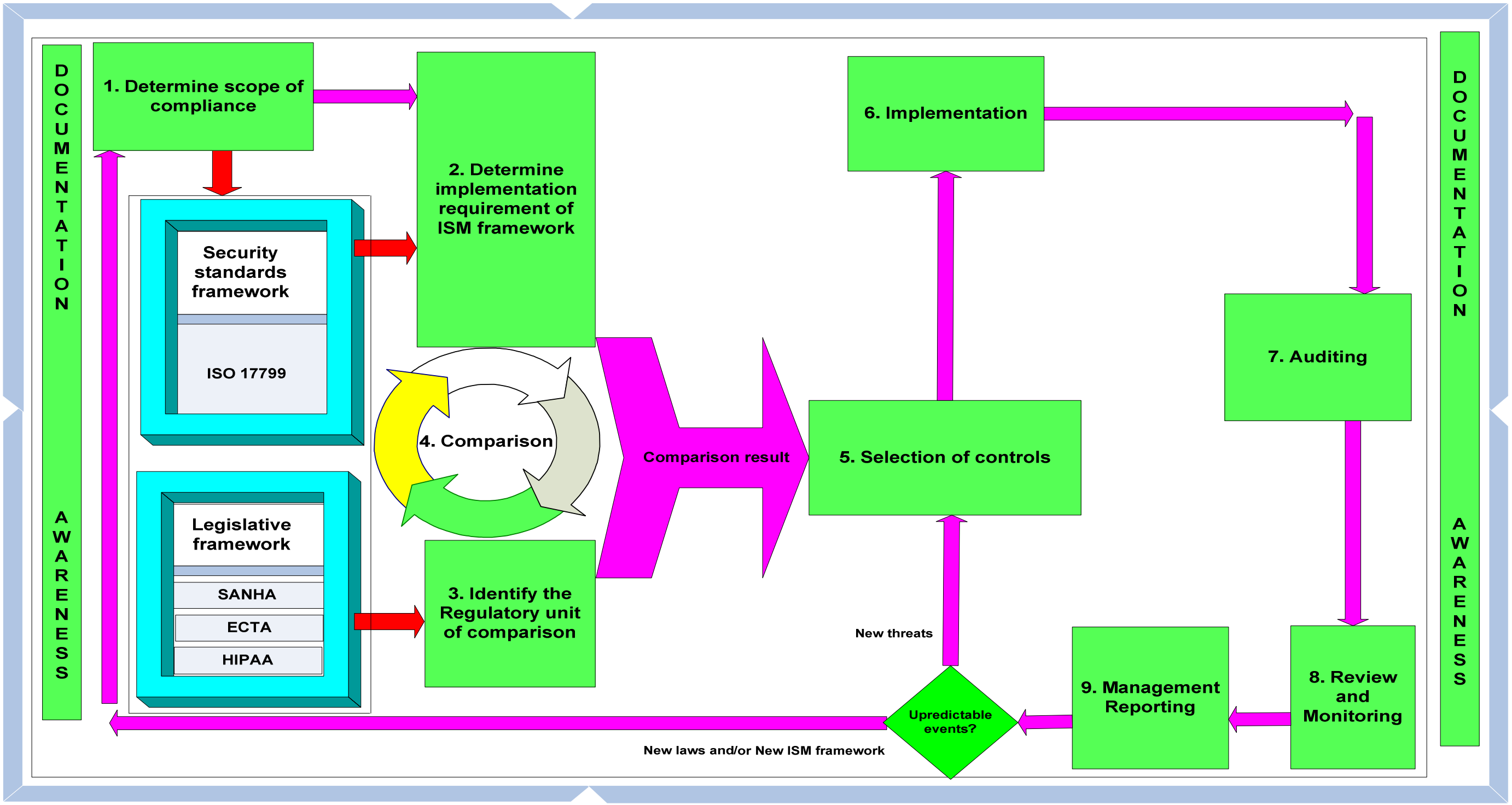
The key solution is to find any overlap that might exist between already implemented controls and these new regulatory requirements. It is obvious that, depending on the legislation, little effort is required to meet new regulation requirements should an organization already has a well-established ISO 17799 compliance program as shown in Figure 17. This proves that a compliance strategy based on a unification process, taking into account both best practices and regulation requirements, will definitively provide remarkable advantages to the organizational compliance efforts. The idea behind the compliance model is to avoid treating each incoming new regulation as a discrete project which can result in unnecessary spending, time and resources devoted to an already implemented security measures. Therefore, such compliance ensures that common elements across regulations and those already covered in an Information Security compliance program are not unnecessarily repeated.

Westby (2005) further proposes that a well-established compliance program must be viewed as an essential responsibility for which all levels of management are accountable; it must not be seen as set of technical requirements emanating from the Chief Information Security Officer or Chief Security Officer, but be considered as a Corporate Compliance Program.

Chapter 6 has established a roadmap that organizations should follow in endeavors to meet both legal and regulatory requirements while ensuring that best practices are being used concomitantly.

Chapter 7 finally concludes the research presented in this dissertation.

Figure -20- A Model for Information Security Management and Regulatory Compliance in the South Africa Health Sector



Chapter 7 CONCLUSION

Chapter 6 provided a compliance model for Information Security Management and regulatory compliance. The compliance model ensures that organizations meet privacy regulatory requirements while, at the same time, ensuring customers that international standards for the protecting information of customers are being used concomitantly. This represents the core of this research project.

This chapter concludes the research presented in this dissertation and discusses the benefits of the compliance model. It suggests some areas suitable for future research.

7.1 INTRODUCTION

Organizations are, currently, functioning in the most complex and challenging era of Information Security Management and regulatory compliance requirements. They are required to ensure compliance with multiple new regulations requirements making such compliance an even more complex issue. In addition, compliance with regulatory requirements is mandatory within an organization and ignorance of the legal requirement is not an excuse. Such compliance failure can result in heavy consequences such as, the loss of shareholders trust, a bad reputation for the company and various stiff penalties for the Executive Managers. Executives and Board members are ultimately accountable for ensuring compliance and face penalties, including fines and jail sentences, for non-compliance.

The problem addressed in this project is which compliance strategy should be followed to meet new regulation requirements while ensuring customers that best practices are being used concomitantly. The greatest challenge that faces Executive Management to ensure a well established corporate compliance program, is how to discover a simple method of meeting these new regulations while spending less money and effort.

This dissertation has demonstrated that the key solution is to discover the overlap that might exist between already implemented controls and these new regulatory requirements. It was illustrated in Section 5.5 of Chapter 5 which provided an analysis of the comparison between ISO 17799 and HIPAA, ECTA and SANHA that depending on the regulation, little effort was needed to meet the regulatory requirements when an organization had already a well-established ISO 17799 compliance program. This proves that a compliance strategy based on a unification process, taking into account both best practices and regulatory requirements, will provide advantages to their compliance efforts.

7.2 BENEFITS OF THE COMPLIANCE MODEL

The implementation of this compliance model provides the following advantages to healthcare organizations:

A. Reduced legal difficulties

There are a growing number of laws relating to the protection of the privacy and security of health information. The implementation of the proposed compliance model will keep an organization legal because it will have ensured due diligence by complying with the relevant legislation requirements. This will, in turn, keep the organizations free when regulatory enforcers come knocking at their doors.

B. Increased trust in business partners and patients

An organization wants to establish the security of the IT systems of its business partners prior to doing business. The implementation of a well-established compliance program will increase trust with other business partners because they are sure that international best practices are being used. In addition, the use of a compliance program will enhance the trust of patients because they are assured that their information is kept secure and private.

C. Reduced audit time

Organizations can save a lot of time and efforts dedicated to auditing process by addressing common elements employed one time for multiple uses. The eradication of redundancy in the auditing process will ensure that no time is wasted on duplicating security controls already implemented.

D. Reduced compliance costs

Conformance with the proposed compliance model is an effective and demonstrable method to ensure that an organization has addressed all the key issues of Information Security, thus reducing losses due to security breaches. This will in turn, reduce the cost for security breaches. Furthermore, the removal of redundancies against the security standards and new regulatory compliance, can save costs that would, otherwise, be devoted to redundant security measures already implemented in the organization.

E. Faster compliance cycle

The implementation of the proposed compliance model will increase the compliance cycle because the organization is building on existing controls already implemented. The compliance with new regulatory requirements will be faster.

F. Unified compliance approach

Conformance with the proposed compliance model ensures a consistent unified approach with the multiple regulatory requirements and security standards rather than the following of disparate compliance approaches.

7.3 CHAPTER OVERVIEW

The aim of this section is to provide the reader with an overview of the work presented in this dissertation.

Chapter 1 – Introduction

Chapter One started by motivating that Information Security Governance has become an important business issue which has escalated to Board level. Executive management and the Board are, currently, responsible and accountable for protecting the security and privacy of the information of their customers. Serious personal consequences, specifically legal, could result from ignoring such Information Security and privacy protection.

This chapter states the problem definition and objectives of this research project.

Chapter 2 – Privacy and Security Concerns Regarding Health Information

Chapter Two highlighted that, although the use of IT in handling medical transactions provides numerous advantages for the healthcare organization and its patients, it equally raises many concerns about the privacy and security of such sensitive information. This chapter illustrated that medical information is used by numerous parties for different purposes and this can result in an increase in vulnerabilities and the various threats to such information proving that there is a need to protect health information. A discussion of various privacy breaches and their consequences were provided.

The chapter concluded by emphasizing the necessity for healthcare organizations to have in place protection mechanisms ensuring the protection of both security and privacy. It was confirmed that the protection of the security of health information can be assured should a reasonable or adequate security standard framework exist; while privacy protection includes various limits of a legal nature

to the collection handling, storage or transmission of personally identifiable or aggregate data collected from individual users.

Chapter 3 – Information Security Standards and Best Practices

Chapter Three described the various international security standards frameworks, government and private guidelines that can be used in ensuring best practices in managing Information Security. The ISO 17799, the mostly widely used International Security Management standard was examined. Its advantages and critics were discussed. It was proposed that Executive Managers should consider using additional existing standards to complement the ISO 17799 and fill any exposed gaps to overcome some of those criticisms. Such convergences become a necessity especially in the healthcare environment where healthcare Information Security standards provide for more stringent solutions in the protection of medical information.

The implementation of proper Information Security Management practices, alone, does not necessarily ensure regulatory compliance and vice versa. Healthcare Executive management must be alert to reduce the losses from the legal action. They must understand the current legal environment, stay current with new laws and regulations and watch for new issues as they emerge.

Chapter 4 – Legal and Regulatory Requirements Pertaining to Privacy and Data Protection

Chapter Four provided a discussion of data and privacy protection on international and national regulatory requirements. This chapter focused on privacy protection in the Republic of South Africa and specifically in the health sector to contextualize with the main objective of this research.

The challenge encountered by most organizations is which compliance strategy they should follow to meet these new regulations while ensuring that existing measures are maintained with the growing number of regulations that require healthcare organizations to demonstrate compliance. Therefore, a comparative analysis of compliance requirements is required which for this project was based on ISO 17799, HIPAA, SANHA and ECTA.

Chapter 5 – Comparison between ISO 17799, HIPAA, SANHA and ECTA

Chapter Five was dedicated to the comparison between an Information Security Management standard (ISO 17799) against the laws applicable to typical South African healthcare organizations. These are not the only applicable laws in the SA context but were selected for the scope of this research project. The analysis of the comparison result illustrated that some legislation has quite an overlap with an Information Security Management program. This confirmed that a compliance strategy would serve to eradicate redundancy while following an ad hoc approach to compliance with the various standards and legislations. This can provide advantages to the organization by easily comply with new regulatory requirements and spend less effort while increasing the return on investment.

This chapter concluded by emphasizing the need for a framework which ensures full compliance with regulatory requirements while ensuring patients that best practices for Information Security management are being used concomitantly to ensure the privacy and security of medical information.

Chapter 6 – A Model for Information Security Management and Regulatory Compliance in the South African Health Sector

This chapter used the result of the comparison analysis and built a model for Information Security Management and regulatory compliance. Its main intention was to establish a roadmap for organizations to follow in their endeavors to meet security standards and regulatory requirements. The phases that constitute this compliance model were discussed. The concept behind this compliance model is to avoid treating each new incoming regulation as a discrete project which can result in unnecessary spending, time and resources which are devoted to already implemented security measures. Therefore, such compliance ensures that common elements across regulations and those already covered in an Information Security Compliance program are not unnecessarily repeated. The compliance program is viewed as an essential responsibility for which all levels of management are accountable and must not be seen as set of technical requirements emanating from the Chief Information Security Officer or Chief Security Officer but must be considered as a corporate compliance program.

Chapter 7 – Conclusion

The research is concluded in this chapter. The benefits of the proposed compliance model are discussed. Future research directions are discussed in the following section.

7.4 FUTURE RESEARCH

The International Information Security Management framework (ISO 17799) provides requirements structure used to identify controls, but it contains insufficient details to enable their implementation. Regulatory requirements are typically written for what you must do, and not how to do it. This project has provided a roadmap for organizations to follow to ensure the compliance of security standard and regulatory requirements. Chapter Six has touched upon on the phases that constitute the proposed compliance model. Possible directions for future research include a detailed practical implementation for an **automated compliance solution** of this proposed model. The use of technology to automate and consolidate many manual activities will significantly reduce the time and costs spent on manually managing the many processes related to meeting compliance with the multiple regulations.

Organizations are required to follow a more holistic approach in ensuring compliance to successfully implement this compliance solution. Thus, technologies such as **Continuous Auditing, Monitoring** and **Reporting** will be of the greatest use in achieving an automated compliance solution.

Woodroof & Searcy (2001) define Continuous Auditing as "*an assurance service where the time between the occurrence of events underlying a particular subject matter of a client and the issuance of an auditor's opinion on the fairness of the client's representation of the subject matter is eliminated*". Miklos et.al (2002) argue that while many people believe that a well-performed traditional audit could have detected some of the operational problems of Enron, a well-performed Continuous Audit would have exposed them much sooner. A Continuous Audit would have provided an assurance of processes that are not necessarily part of the eventual financial reporting and an assurance focus that is closer to secondary supervision than an after-the-fact archival review (Miklos et.al, 2002).

On the other hand, a Continuous Monitoring process should further provide the ability to observe the performance of one or many processes, systems or types of

data and report any fluctuations in a timely manner (ISACA, 2002). Continuous Monitoring can be defined as the internal continuous provision of key metrics or other information enabling the early identification of issues that may affect corporate performance (Nehmer, 2003).

The main goal of Continuous Reporting is, according to Williams (2002), to develop reporting systems within a company, whereby management by exception enables Boards of Directors and others to gain a continuous assurance on corporate performance and therefore, enable to better discharge their governance responsibilities in a timely manner.

One aspect that has been raised, but not discussed, is that of providing a structure for the regulatory requirements which were not taken into account during the comparison reported in Chapter Five. These regulatory requirements are not specifically security and privacy related issues but healthcare organizations must meet those requirements because they are part of regulatory compliance. For example, Chapter 2 (Rights and duties of users and Health care personnel) of SANHA, Section 5 requires that *"A health care provider, health worker or health establishment may not refuse a person emergency medical treatment".*

7.5 CONCLUSION

This chapter concludes this dissertation and illustrates that all of the objectives established at the beginning of this research project were accomplished. An overview of the information covered in the various chapters of this dissertation was provided and future research directions suggested. The benefits of the proposed compliance model were discussed.

The managing of Information Security in information systems has reached the point where sufficient but dispersed knowledge exists in various domains (Denis, 2003). Some of the areas supporting the Information Security program may be required by either law or regulations whereas others may be considered best practices.

Compliance with SANHA and ECTA is a regulatory requirement for South African healthcare organizations and ignorance of the legal requirement is not an excuse. Any ignorance of legal requirements can result in heavy punishment and the loss of organizational credibility. The managers of South African healthcare

organization must consider that being compliant with all legal requirements does not guarantee the privacy and security protection of health information and vice versa. They should adopt international security standards as part of the Information Security Management to ensure that best practices are used in addition to meeting the regulatory requirements. This statement is used as a premise for this research and it is proposed that a compliance strategy should use an Information Security Management framework as a point of reference to collate further requirements posed by regulations. This is particularly important in the health sector in terms of the security and privacy of health information. The use of an internationally accepted standard, such as the ISO 17799, will further enhance the desired level of security. This can help reduce the security and privacy risks to a minimum level while minimizing the redundancy in the approach to complying with relevant legislations. Legislations have a profound impact on organizations through non-compliance fines, penalties, resulting bad publicity and damaged reputation and provide the motivation to help improve the privacy and security of health information.

Security and Privacy of health information can only be assured if Security standards and Legislations complement each other in protecting such critical information.

References

Accenture, 2004. *Security and Privacy Compliance* [online]. Available on the internet:
http://www.accenture.com/xdoc/en/services/secsol/insights/compliance.pdf.
Sited 15 October 2005

ACL, 2005. Continuous Controls Monitoring. ACL Services Ltd

Allen, A. (1995). Privacy in health care. In: Reich WT, ed. Encyclopedia of Bioethics. (Vol.4). New York, NY: Macmillan. 1995:2064-2073.

AMR Research, 2005. Spending in an age of compliance. Executive summary, pages 1-2.

ANDERSON, R. 1996. *Personal Medical Information Security, Engineering, and Ethics*. Proceedings of Personal Information Workshop. Cambridge, UK, June 21-22, 1996.

Anderson, D. 2005. *HIPAA security and compliance* [online]. Available on the internet: http://www.tdan.com/i033ht04.htm (Sited 07 July 2005).

Ashton, G., 2002. *BS7799 / ISO-IEC-17799 Benefits in the Real World* [online]. Available on the internet: http://www.lrqa.co.uk/downloads/public/lrqa-publications/infosec-2005-lrqa-presentation.pps. Sited 25 March 2005

Barnard, L., von Solms, R., 1998. A formalized approach to the effective selection and evaluation of Information Security controls. Information Security Small Systems Security & Information Security Management (2) pp 70-85. Vienna – Budapest, 2 September 1998.

Bassett, 2003. *Healthcare in South Africa* [online]. Available on the internet: http://www.medhunters.com/articles/healthcareInSouthAfrica.html. Sited 08 March 2005.

Baumrucker, T. ISO 17799 security standards [online]. Available on the internet: http://www.callisma.com/. Sited 10 March 2005

Bisson, J., Saint-Germain, R. 2003. *The BS 7799 / ISO 17799 Standard For a better approach to Information Security* [online]. Available on the internet: http://www.callio.com/files/wp_iso_en.pdf. Sited 24 September 2005

Bindview, 2005. *Finding the Compliance "Sweet Spot": Demonstrating Compliance, Reducing Complexity, and Lowering Costs* [online]. Available on the internet: www.bindview.com. Sited on 15 September 2005.

Blair, J. *AN OVERVIEW OF HEALTHCARE INFORMATION STANDARDS* [online]. Available on the internet: http://im.med.up.pt/standards/cache/overview.htm. Sited 07 March 2005

Borkin, S. 2003. *The HIPAA Final Security Standards and ISO/IEC 17799*. SANS Institute 2003 [online]. Available on the internet: http://www.sans.org/rr/whitepapers/standards/1193.php. Sited 10 March 2005.

Briggs, L. 2000. *A National Approach to Electronic Health Records*. Proceedings of the Electronic Health Records Conference, 29 May – 1 June 2000.

Brewer,C. 2005. *The Truth Will Keep You Free: Analytics, BI, and Compliance*. [online]. Available on the internet: http://www.itcinstitute.com/display.aspx?id=509. Sited 29 May 2005

Callio Technologies, 2001. *The Callio Technologies ISO17799 / BS7799 solution* [online]. Available on the internet: http://www.callio.com/bs7799/id,69. Sited 25 May 2005

Caroline, N. 2004. *A Comparative Analysis of Zimbabwean and South African Data Protection Systems*. Journal of Information, Law and Technology (JILT) [online]. Available on the internet: http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/ncube/. Sited 17 June 2005

Carlson, T.2001. *Information Security Management: Understanding ISO 17799* [online]. Available on the Internet: http://www.ins.com/downloads/whitepapers/ins_white_paper_info_security_iso_17799_1101.pdf. Sited on 14 June 2005

Centers for Medicare & Medicaid Services (CMMS), 1996. *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)* [online]. Available on the internet: http://www.cms.hhs.gov/hipaa. Sited 01 April 2005.

CNN Interactive, 1996. *Yeltsin Had Heart Attack During Russian Elections*. September 21, 1996 [online]. Available on the internet at: www.cnn.com or at: www.nap.edu/readingroom/books/ftr/. Sited 01 July 2005

COBIT, 2000. *Control Objectives for Information and related Technologies.3rd ed.USA:* IT Governance Institute.

Collier, G. (1995) "Information Privacy" in *Information Management & Computer Security*, Vol 03 Issue 1, ISSN 0968-5227.

Computer-based Patient Records Institute (CPRI) Toolkit, 1995. *Managing Information Security in Heath Care* [online]. Available on the internet: http://www.himss.org/CPRIToolkit/html/3.6.html Sited 10 March 2005.

Conradie, N., Hoekstra, A. 2002. COBIT*, ITIL and ISO 17799 How to use them in conjunction* [online]. Available on the internet: http://www.cccure.org/Documents/COBIT/COBIT_ITIL_and_BS7799.pdf. Sited 20 April 2005

Constitution of the Republic of South Africa (1996). Act 108 of 1996, Chapter 2, Section 14 and 32" [online]. Available on the internet: http://www.polity.org.za/govdocs/constitution/saconst02.html#14. Sited 16 September 2005

Corporate Governance Task Force. (2004, April). *Information Security Governance: A Call To Action*. Available from: http://www. Cyberpartnership.org/InfoSecGov4 04.pdf. Sited 03 November 2005.

Council Medical Schemes, 2002. *Draft Recommendations of the Committee on Standardization of Data and billing Practices. Research and Monitoring.*

Council of Europe Treaty Office (1981) "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no.: 108", Strasbourg, January 28, 1981 [online]. Available on the internet: http://conventions.coe.int/treaty/EN/cadreprincipal.htm. Sited 15 March 2005

COSO, 2004. Enterprise Risk Management – Integrated Framework, Vol 1 and Vol 2 [online]. Available on the internet: http://www.coso.org. Sited on 15 September 2005.

Cybertrust, 2004. Risk Commander 2.0: Enterprise-level compliance and vulnerability management. July, 2004 [online]. Available on the internet: http://www.trusecure.com. Sited on 20 September 2005.

Dan Geer. 2005. *Governing for Enterprise Security: Be Aware and Understand* [online]. Available on the internet: http://www.cert.org/features/green/ges-aware.html. Sited 21 June 2005

Dash, J. 2000. Health-care industry looks at security risks: Data theft at cancer institute highlights concerns. ComputerWorld. August 14, 2000 [Online] Available on the internet at:
http://www.computerworld.com/industrytopics/manufacturing/story/0,10801,48493,00.html

Denis, T. 2003. *An integral framework for information systems security management*. Computers & Security, Elsevier Science. Vol 22 (4), pp. 337-360.

Department of Health and Human Services (DHHS), 2000. *Standards for Privacy of Individually Identifiable Health Information*. Final Rule 45 CFR Parts 160 and 164. Federal Register: December 28, 2000 (Vol 65, Number 250).

DICT, 1992. The *American Heritage Dictionary of the English Language, Third Edition*. Houghton Mifflin Company. Electronic version licensed from InfoSoft International, Inc.

Dobson, J., Samarati, P., Jajodia, S., Thuraisingham, B. 1995. Security and Privacy issues for the World Wide Web: Panel Discussion.

Doward, J. 2002. Day the WorldCom world. The Observer (London) 2002 June 30

Electronic Communication Transaction Act (ECTA) (25 0f 2002). Vol.446 Government Gazette, Cape Town, 02 August 2002.

Electronic Privacy Information Center (EPIC) and Privacy International. Privacy and Human Rights Report (2002). *'An International Survey of Privacy Laws and Developments,' United States of America* [online]. Available on the internet: http://www.privacyinternational.org. Sited 20 February 2005.

Eloff, M., von Solms, B. 2000. *Information Security management: a hierarchical framework for various approaches*. Computers & Security, Elsevier Science. Volume 19 (3), pp. B1-B21

Eloff, M., von Solms, S. 2000. *Information Security Management: an approach to combine process certification and product evaluation*. Computer & Security vol (19) 8, Elsevier.

EMC Corporation, 2005. *The External Charter: Improving Corporate Governance through Compliance and Assured Records Management*. April, 2005. Cohasset Associates, Inc.

Entrust. 2004. Information Security Governance (ISG): An Essential Element of Corporate Governance [online]. Available on the internet: http://itresearch. forbes.com/detail/RES/1082396487 702.html. Sited 08 August 2005

ERNST & YOUNG, 2004. Global Information Security Survey. [online]. Available on the internet at: http://www.ey.com/global/download.nsf/International/2004_Global_Information_Security_Survey/$file/2004_Global_Information_Security_Survey_2004.pdf. Sited 12 August 2005

EthicSA, 2000. *Chris Hani Baragwanath Hospital Ethics Audit* [online]. Available on the internet: http://www.ethicsa.org/article.php?story=20030919084251975. Sited 14 February 2005.

Finextra news, 2005. *U.S Companies want companies fined for security breaches.* July, 08, 2005 [online] available on the internet: http://www.finextra.com/fullstory.asp?id=13952. Sited 14 September 2005

Fitzmaurice .J.M, 1998. *A new twist in US healthcare data standards development: adoption of electronic healthcare transactions standards for administrative simplification*. International Journal of Medical Informatics (48), pp 19-28. Elsevier Science Ltd.

Flaherty, D. 1989. *Protecting the Privacy in Surveillance Societies*. University of Carolina Press.

Gerber, M., & von Solms, R. 2001. From risk analysis to security requirements. Computers and Security, 20 (7), 577–584.

GOSTIN, L.J.D. 1997. *Annals of Internal Medicine, Part 2*. October 15, 1997. (127), pp683-690 [online]. Available on the internet at: http://www.acponline.org/journals/annals/supplement/protect.htm. Sited 07 May 2005

Hancock, B. 1999. *Healthcare and Network Security: Protecting Patient Privacy*. Network-1 Security Solutions, Inc., Waltham, MA, USA, October 1999.

Halliday, J., von Solms,R. 1997. *Effective Information Security policies.* In: von Solms R, editor. Information Technology on the move, Port Elizabeth Technikon, 1997, pp 12-20.

HARRIS, L. and Associates. 1995. "*Equifax-Harris Mid-Decade Consumer Privacy Survey, Study No. 953012*". New York. In *For the Record* [online]. Available on the Internet: www.nap.edu/readingroom/books/ftr/. (Sited 14 May 2005)

Health Human Services, 2003. *Administrative Simplification in the Health Sector* [online]. Available on the internet: http://aspe.os.dhhs.gov/admnsimp/index.shtml (Sited 28 February 2005).

Health Professions Council of South Africa (HPCSA), 2002. *Guidelines for good practice in medicine, Dentistry and the Medical Sciences, Confidentiality: Protecting and Providing Information*. Pretoria July 2002.

Hensley, M. 2003. *Monitoring Training for Area Agencies on Aging Basic Fundamental and New Requirements* [online]. Available on the internet: http://www.dhhs.state.nc.us/aging/monitor/monitoringtraining.ppt**.** Sited 02 May 2005. Sited 01 May 2005

Herold, R. 2001. *The practical guide to assuring compliance* [online]. Available on the internet: http://download.netiq.com/Library/eBooks/Practical/Chapter1.pdf Sited 26 April 2005.

HHS, 2001. *U.S Department of Health and Human Services (HHS) Fact Sheet.* May 9, 2001.

HIV/AIDS Law and Human Rights Update, 2004. *AIDS Law Project, Centre of Applied Legal Studies*, University of Witwatersrand, Edition 2, July 20, 2004 [online] available at the internet: http://dedi20a.your-server.co.za/alp/images/upload/20040721_Newslette2.pdf. Sited 10 July 2005

Hill, A., McNulty, S., Wine, E. 2001. *A chaotic collapse*. The Financial Times London. 2001 November 30.

HIV / AIDS MINISTRIES NETWORK, 1995. Girl, 13, Sentenced in an AIDS Hoax. New York Times, April 21, 1995. In *FOCUS PAPER No 28* [online] available at the internet: http://gbgm-umc.org/resources/hivfocus/focus028.html. Sited 26 August 2005

HIPAA Administrative Simplification – Security Final Rule, 2003. Center of Medical & Medicare Services [online]. Available on the internet: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp. Sited 17 August 2005

HIPAA Administrative Simplification – Privacy Final Rule, 2002. Center of Medical & Medicare Services [online]. Available on the internet: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/privacy/default.asp. Sited 16 August 2005

HIPAA Administrative Simplification – Transaction and Code Set Rule, 2000. Center of Medical & Medicare Services [online]. Available on the internet: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/default.asp. Sited 16 August 2005

Humphreys, T., 2005. *The New edition of ISO/IEC 17799 Code of practice for Information Security Managemen*t. Vienna, 18 April 2005 [online]. Available on the internet: http://www.cccure.org/Documents/ISO17799/newstandard.png

Humphreys, T., 2005. *Frequently Asked Questions on Information Security Management System.* May 2005. ISMS International User Group, 2003-2005.

ISACA, 2005. *New COBIT version coming* [online]. Available on the internet: www.isaca.org/cobit.htm. Sited 01 March 2005

ISACA, 2002. *Continuous Auditing: Is it Fantasy or Reality?*. Information Systems Control Journal, vol 5, 2002.

ISMS International User Group, 2005. *The New edition of ISO/IEC 17799 Code of practice for Information Security Management.* Vienna, 18 April 2005. [online] Available on the internet: http://www.cccure.org/Documents/ISO17799/newstandard.png. Sited 05 February 2005

ISO17799 SOUTH AFRICAN STANDARD, 2000, *SABS ISO/IEC 17799, Information Technology - Code of practice for Information Security management.* SABS edition 1/ISO/IEC edition 2000. Pretoria: South African Bureau of Standards.

ISO/DIS 22857, Geneva, 2003. *Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information* [online]. Available on the internet: http://www.cihi.ca/cihiweb/en/downloads/event_partner_may03_iso22857_e.pdf. Sited 01 April 2005

ISO IEC 15408, International Organization for Standardization (ISO), *Evaluation Criteria for Information Technology Security*, Switzerland, 1999.

ISO TC 215. ISO/TC. *Health Informatics* [online]. Available on the internet: http://isotc.iso.ch/livelink/livelink?func=ll&objId=529136&objAction=browse&sort=nameStandards specific information. Sited 01 February 2005

ISO/IEC 15408. *International Organization for Standardization (ISO), Evaluation Criteria for Information Technology Security.* Switzerland, 1999

IT Governance Institute (ITGI). [online] Available on the internet: www.itgi.org. Sited 06 June 2005

IT Governance Institute, 2001. *Board and Briefing on IT Governance ITGI*, USA.

itGovernace, 2005. *ISO/IEC 17799:2005 Plus FDIS ISO/IEC 27001* [online] Available at the internet: http://www.itgovernancesales.co.uk/catalog_product.aspx?prod_id=127 Sited 10 June 2005

IT Governance Institute, 2004. *COBIT Mapping: Overview of International IT Guidance* [online]. Available on the internet: http://www.cccure.org/Documents/COBIT/COBIT_Mapping_Paper_6jan04.pdf

Janczewski, L. Keng, B. 1998. *Privacy protection in hyper-media health information systems from law point of view*. In Proceedings of Joint IFIP TC 6 and TC 11 Working Conference on Information Security small systems security & Information Security management. Vienna-Budapest , 2 september 1998.

Kahn, R., Blair,T. 2005. Understanding the Impact of Today's Legal and Regulatory Requirements on IT. Special Report: The Legislating of IT [online]. Available on the internet: www.kahnConsultingInc.com. Sited 10 November 2005.

King Report. (2001). *The King Report on Corporate Governance for South Africa* [online]. Available on the internet: http://www.iodsa.co.za/IoD%20Draft% 20King%20Report.pdf.

Klein, G., 2002. S*tandardization of health informatics results and challenges.* Yearbook for Medical Informatics Centre for Health Telematics Karolisnska Institute Stockholm, Sweden, pp(103-114).

Kleinbard, D. 2005. *The Hard Times They Are Changin'. A Securities Fraud And Corporate Governance Quarterly* [online]. Available on the internet: www.blbglaw.com/advocate/adv2005q1.pdf. Sited on 17 July 2005

Klinck, E. 2000. *Health Data Confidentiality and Privacy: Standards* Human Rights, Law and Ethics Unit, SAMA. Document based in part on the document generated by the Privacy and Confidentiality Subcommittee of the Committee on Standardization of Data and Billing Practices.

Kolodgy, C., Christiansen, C. 2005. *Using Security Compliance Software to Improve Business Efficiency and Reduce Costs*. June, 2005 [online]. Available on the internet: www.bindview.com. Sited on 22 August 2005.

KPMG, 2001. *A new covenant with stakeholders: Managing privacy as a Competitive Advantage*. KPMG's Assurance & Advisory Services Center.

Langelier, C., Ingram, J. 2001. *National State Auditors Association and the U.S. General Accounting Office: Management Planning Guide Information System Security Auditing* [online]. Available on the internet: www.gao.gov. Sited 01 May 2005

Lawrence, W. 2002. *Standard Practice: ISO 17799 aims to provide best practices for security, but leaves many yearnings for more* [online]. Available on the internet: http://infosecuritymag.techtarget.com/2002/mar/iso17799.shtml

LINCOLN, T.L., ESSIN, D. *The Computer-Based Patient Record: Issues of Organisation*, Security and Confidentiality in IFIP Transactions A-6 Database Security ,V*.*

Lineman, 2005. *InfoSec Synergies: Aligning Standards Improves Security* [online]. Available on the internet: http://www.itcinstitute.com/display.aspx?ID=171

Luck, J. 2000. *Privacy, Security and Confidentiality.* Health Informatics Journal pp 1-11.

Martin, E. (2000). *Public opinion changes during two censuses*. Paper presented at the Decennial Census Advisory Committee, September 21, 2000.

Mash, S. 2002. *Risk Assessment for Dummies*. Computer Fraud & Security, Vol.2002, No.12, pp.11-13, 2002

Mayer, T.S. 2002. *Privacy and Confidentiality Research and the U.S. Census Bureau Recommendations Based on a Review of the Literature*. February 7, 2002. Statistical Research Division U.S. Bureau of the Census. Washington D.C.

McLean, B. 2002. *Monster mess: the Enron fallout has just begun*. Fortune European Edition 2002 March 11:52

Medical Records, 1999. *Enhancing Privacy, Preserving the Common Good in The Hastings Center Report*, March-April 1999, pp. 14-23 [online]. Available on the internet: http://www.gwu.edu/~ccps/etzioni/A265.html

Meyer, S. 2001. *What is means for Privacy and Security* [online]. Available on the Internet: http://www.giac.org/certified_professionals/practicals/gsec/0609.php

Michalson, L. 2004. *Guide to ECT Act*. *IT Law Insight* [online]. Available on the internet:http://www.salaw.co.za/docs/Michalsons%20Infosheet%20-%20Guide%20to%20the%20ECT%20Act.pdf

Moulton, R., Coles, R. (2003). *Applying Information Security governance*. Computers & Security, Elsevier Science. Vol 22 (7), pp. 580-584

Munk,K. 98. *Traditional healers and HIV/AIDS in Kwazulu-Natal: an interim report" AIDS Analysis Africa*. South African Edition page 7.

National Institute of Standards and Technology (2001, October). NIST Special Publication 800-30: *Risk Management Guide for Information Technology Systems*.

National Research Council (NRC), 1997. Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure. *For the Record: Protecting Electronic Health Information*. National Academy Press. Washington DC.1997. [online] Available on the Internet: http://books.nap.edu/catalog/5595.html

Neethling, J., Potgieter, J. (1996). *Neethling's Law of Personality. Recognition of the Right to Privacy* [online]. Available on the internet: wwwserver.law.wits.ac.za/salc/issue/ip24-03.pdf

NetForensics, 2005. *Achieving Regulatory Compliance through Security-Information Management* [online]. Available on the internet: www.netForensics.com. Sited on 10 July 2005.

Nehmer, R. 2003. *Continuous Audit: Taking the plunge*. ISACA, vol 1, 2003.

News Batch, 2004. *What is the present status of the principals in the 2001 corporate governance scandals?* August, 2004 [online]. Available on the internet: http://www.newsbatch.com/corp.htm. Sited on 14 April 2005

NEMA, 2001. *Security and Privacy: An Introduction to HIPAA*. The Privacy and Security Committee Medical Imaging Informatics Section. February 14, 2001.

NIST, 800-66. *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. NIST Special Publication 800-66. U.S. Government Printing Office, Washington [online]. Available on the internet: http://csrc.nist.gov/publications/drafts/DRAFT-sp800-66.pdf

NIST, 1901. *National Institute of Standards and Technology publications.* [online] Available on the internet: http://csrc.nist.gov/publications/nistpubs/ index.html.

Nozizwe, M. 2004. *Speech on the Traditional Health Practitioners Bill by the Deputy Minister of Health Mrs Nozizwe Madlala-Routledge*. South African Government Information

Oberholzer, H. 2001. *A privacy protection model to support personal privacy in relational database*. Published master's thesis. Rand Afrikaans University, Johannesburg, South Africa.

OECD: "*Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*" [online] Available on the internet: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM (Sited 07 July 2005).

Office of Technology Assessment (OTA), 1993. *Protecting privacy in computerized medical information*. Washington DC: US Congress, OTA TCT-576.

OLIVIER, M.S., THURAISINGHAM, B., JAJODIA, S., SAMARATI, P., DOBSON, J. *Security and Privacy Issues for the World Wide Web: Panel Discussion*.

Open Democracy Bill No 67, 1998 of the Republic of South Africa. [online] Available on the internet: http://www.parliament.gov.za/bills/1998/b67-98.pdf

Oppliger, R. 1996. *Authentication systems for secure networks*. Artech House.

Piller, C. 1993. *Privacy in peril.* Macworld v10 n7 [online]. Available on the internet: http://newfirstsearch.oclc.org/ (Sited 10 July 2005).

Posthumus, S., von Solms, R. 2005. *IT oversight: an important function of Corporate Governance*. Computer Fraud & Security. June 2005.

Powe, L. CSC Press Releases: *Technology could ease stress of nursing shortage* [online]. Available on the Internet: http://za.country.csc.com/en/ne/pr/680.shtml (Sited 20 February 2005).

Privitelli, E. 2004. *Interview with Eugenio Privitelli* [online]. Available on the internet http://www.miamalta.org/MagSpring03Page08.htm

Promotion of Access to Information Act (PAIA), 2000. Government Gazette, 2000

Rasmussen, M. 2005. *Revised ISO 17799 Boosts Information Security Management Relevance* [online]. Available on the internet: http://www.csoonline.com/analyst/report3730.html.

Rezaee, Z., Elam, R., Sharbatonghlie, A. (2002). *Continuous Auditing: the audit of the future*. Managerial Auditing Journal, 16(3), 150-158.

ROEMER, M. 1991. *National Health Systems of the World*. (vol.1: The Countries). Oxford, Oxford University Press.

Romanow Report & Informatics, 2002. *Final Report: Building on Values: The Future of Healthcare in Canada*. Information, Evidence and Ideas pp (75-95).

Sadan, B. (2001). *Patient data confidentiality and patient rights*. International journal of Medical Informatics (62), pp 41-49. Elsevier Science Ltd.

Saliba, R., Saint-Germain, R. 2004. *Callio Secure 17799: A tool for implementing the ISO 17799 / BS 7799 standard* [online]. Available on the internet: http://www.callio.com/expertise/files/EN/wp_secura_en.pdf

Sarah, D. 2003. *Information Security standards are quite a bit less than that—and that needs to change* [online]. Available on the internet: http://www.csoonline.com/read/030103/lite.html

SBP report, 2005. *Counting the costs of red tape for business in South Africa.* Main Report – Strategic partnership for business growth in South Africa. Johannesburg June 2005 [online]. Available on the internet: www.sbp.org.za

Schwartz, M. 2005. *InfoSec Synergies: Aligning Standards Improves Security* [online]. Available on the internet: http://www.itcinstitute.com/display.aspx?ID=171. Sited on 22 July 2005

Serwer, A. 2002. *Dirty rotten numbers*. Fortune European Edition 2002 February

Sloan, A. 2002*. Enron's failed power play*. Newsweek 2002 January 21:34–9

SIMONS, B. *The Need for Improved Privacy and Security of Medical Databases* [online] available at the internet: http://www.acm.org/usacm/privacy/simons_medical.html. Sited on 12 July 2005

SITA Act 38 of 2002 section 6 [online]. Available on the Internet: http://www.sita.co.za. Sited on 2 March 2005.

Smith, E., Eloff, J.H.P. 1999. *Security in health-care information systems – current trends*. International Journal of Medical Informatics, vol 54 pp 39-54. Elsevier Science Ltd.

Smith, C.2004. *SANS Institute- GIAC Security Essentials Certification (GSEC) Cross Walking Security requirements* [online]. Available on the internet: http://www.sans.org/rr/whitepapers/country/1463.php. Sited 14 March 2005.

South African National Health Act (SANHA) (61 of 2003). Vol.469. Government Gazette, Cape Town 23 Jully 2004.

South African Health Review 1998 Technical Report, 1997. *Measuring quality of care in South African Clinics and Hospitals (chapter 14).* Health Systems Trust.

South African Law Commission (SALC), 2003. *An Investigation of Privacy and Data Protection in South Africa* [online]. Available on the internet: http://wwwserver.law.wits.ac.za/salc/salc.html. Sited on 26 June 2005

South African National Health Act (SANHA) (61 of 2003). Vol.469. Government Gazette, Cape Town 23 July 2004.

Sun Tzu, 1910. The Art of war by Sun Tzu. A Puppet Press Classic.

Swindom, G., 2004. *HIPAA Final Security Rule Information Security Reference Guide.* Sygate Technologies, Inc.

Teller-Kanzler, J. 2005. *Are you self-assessing your Information Security & privacy environment?.* July, 2005 [online]. Available on the internet: www.secureinfo.com. Sited on 10 September 2005.

Traditional Health Bill. (No 24751). Government Gazette 14 April 2003 [online]. Available on the internet: http://www.polity.org.za/pdf/TradHealPracB66A.pdf

Tuyikeze, T., Pottas, D. (2005).*Information Security Management and Regulatory Compliance in the South African Health Sector*. Proceedings of the 5th Annual Information Security South Africa Conference, 29-01 July 2005, Sandton, South Africa, pp. 3-12.

Trillium Software, 2004. Corporate Governance and Compliance: Could Data Quality Be your Downfall? [online]. Available on the internet: http://www.trilliumsoftware.com/success/dqic.pdf.

Unerman, J., O'Dwyer, B. 2004. *Enron, WolrdCom, Andersen et all.: a challenge to modernity*. Critical Perspectives on Accounting (15), pp 971-993. Elsevier Science Ltd [online]. Available on the internet: www.elsevier.com/locate/cpa. Sited on 05 September 2005.

URAC, 2004. *Comparison between ISO 17799 and HIPAA Security Ru*le [online]. Available on the internet: http://www.urac.org/sworkgroup_junemeeting.asp

U.S. Department of Justice Memorandum, 2003. Principles of Federal Prosecution of Business Organizations. January 2003 [online]. Available on the internet: www.cohasset.com/papers/doj_business_prosecution_Principles.pdf. Sited on 21 September 2005.

U.S Senate, 1997. *Testimony before the Committee on Labor and Human Resources*. October, 28, 1997.

Vericept Corporation, 2004. Preventing Identity Theft and Loss of Intellectual Property: The Importance of Information Security in Internal Controls and Corporate Governance [online]. Available on the internet: http://www.vericept.com/Downloads/WhitePapers/Vericept_Fraud_IdentityTheft_WP.pdf.

Von Solms, B. 2001. *Corporate Governance and Information Security*. Computers & Security, Elsevier Science. Vol 20 , pp. 215-218

Von Solms, B., von Solms, R. 2005. *From Information Security to business security?* Computers & Security. 14 May 2005, Elsevier Science. pp. 1-3

Von Solms, B.2005*. Information Security governance: COBIT or ISO 17799 or both?.* Computers & Security, Elsevier Science. Volume 24, pp. 99-104.

Von Solms, R.1998*. The evaluation and certification of Information Security against BS7799.* Computers & Security, MCB University Press, pp. 72-77.

Von Solms, R.1998*. Information Security Management (1) : Why Information Security is so important.* Computers & Security, MCB University Press, pp. 174-177.

Von Solms, R.1999*. Information Security Management: Why standards are so important.* Computers & Security, MCB University Press, pp. 50-57.

Wallhoff, J. 2005. *How ITIL can be combined with ISO 17799 and COBIT*. [online]. Available on the internet: http://www.isaca.dk/information/ITILCOBIT17799.pdf Sited on 25 May 2005.

Williams, P.2002. *Continuous Auditing and Reporting – The Fourth World Symposium.* Information Systems Control Journal, Vol5, 2002.

Workgroup for Electronic Data Interchange (WEDI) [online]. Available on the internet: (http://www.wedi.org). Sited on 10 June 2005.

Westby, J. 2005. Roadmap to an Enterprise Security Program. American Bar Association Privacy & Computer Crime Committee Section of Science & Technology Law. ABA 2005 [online]. Available on the internet: www.ababooks.org Sited on 02 March 2005.

Whitman, M. E., & Mattford, H. J. (2003). *Principles of information security*. (pp: 19 – 195). Course Technology.

WHO Center of Health Development. *Planning for cost-effective traditional medicines in the new century* [online]. Available on the internet: http://www.who.or.jp/tm/research/bkg/3_definitions.html. Sited on 15 September 2005.

Wold, G. H., & Shriver, R. F. (Eds.). 1997. Risk analysis techniques. Available from: http://www.drj.com/new2dr/w3 030.htm: Systems Support, inc.

Woodroof, J., Searcy,D. 2001. Continuous Audit: Model development and implementation within a debt covenant compliance domain.

Yun Sik Kwak, 2004. *Current ISO/TC 215, Health Informatics Standardization Activity* [online]. Available on the internet: http://www.iso.org/iso/en/domai_ns/WSC-MedTech/pdf/Abstract%20Yun%20Sik%20Kwak.pdf. Sited on 24 May 2005

Zhang, L., Ahn, G, Chu.B (2002). *A Role-Based Delegation Framework for Healthcare Information Systems*. Proceedings of the seventh ACM symposium on Access control models and Technology (SACMAT), pages 153-162. Chantilly, VA, May 3-4, 2001.

Appendix A

COMPARISON BETWEEN ISO 17799, HIPAA, SANHA AND ECTA

ISO 17799 Security Standard	HIPAA_SSMp	HIPAA_SSEq	HIPAA_PSMp	HIPAA_PSEq	HIPAA_TCSMp	HIPAA_TCSEq	SANHA_Mp	SANHA_Eq	ECTA_Mp	ECTA_Eq
1. Introduction										
2. Terms and Definitions										
2.1 Information Security	164.304Definitions									
2.2 Risk assessment	164.308(a)(1)(ii)(a)Risk Analysis									
2.3 Risk Management	164.308(a)(1)(ii)(b)Risk Management									
3. Security Policy										
3.1 Information Security Policy										
3.1.1 Information Security policy document	164.316(a)Policies and Procedures. 164.316(b)Policies Documentations	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
3.1.2 Review and Evaluation	164.306(e) Maintenance. 164.308(a)(8)Evaluation. 164.316(b)(2)(iii)Updates	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
4. Organizational Security										
4.1 Information Security Infrastructure										
4.1.1 Management Information Security forum	164.308(a)(2)Assigned Security Responsibility	>	Not covered	#	Not covered	#	Not covered	#	Not covered	#
4.1.2 Information Security co-ordination	164.308(a)(2)Assigned Security Responsibility	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#

4.1.3 Allocation of Information Security responsibilities	164.308(a)(2)Assigned Security Responsibility	>	164.530(a)Privacy Officer	<	Not covered	#	12(g)The rights and duties of users and healthcare providers	<	Not covered	#
4.1.4 Authorization process for information processing facilities	164.308(a)(1)(I)(b)Security management process	~	Not covered	#	Not covered	#	12.Duty to disseminate information	<	Not covered	#
4.1.5 Specialist Information Security advise	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
4.1.6 Co-operation between organizations	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
4.1.7 Independent review of information security	164.308(a)(8)Evaluation	~	Not covered		Not covered	#	Not covered	#	Not covered	#
4.2 Security of Third Party Access										
4.2.1 Identification of risks from third party access	164.308(a)(1)(ii)(a)Risk analysis	~	160.103;164.502(e); 164.504(e);164.532(d)(e) Business Associates	<	Transaction and code sets standards	<	Not covered	#	VI. Authentication Service Providers	<
4.2.2 Security requirements in third party contracts	164.308(b)(1)Written Contract or Other Arrangement. 164.308(b)(1)Business associate contracts and other arrangement	<	160.103;164.502(e); 164.504(e);164.532(d)(e) Business Associates. 164.510(a)Facility Directories	<	Transaction and code sets standards	<	Not covered	#	29(3)Registration of cryptography providers	<
4.3 Outsourcing										
4.3.1 Security requirements in outsourcing contracts	164.308(b)(1)Business associate contracts and other arrangement	~	160.103;164.502(e); 164.504(e);164.532(d)(e) Business Associates	~	Not covered	#	Not covered	#	VI. Authentication Service Providers	>
5. Asset Classification and Control										
5.1 Accountability for Assets										
5.1.1 Inventory of assets	164.308(a)(7)(ii)(e)Applications and data criticality analysis	~	160.103;164.104;164;501.16 4.514(a)(e)What is covered?	<	Not covered	#	Not covered	#	Not covered	#
5.2 Information Classification										
5.2.1 Classification guidelines	164.308(a)(7)(ii)(e)Applications and data criticality analysis	<	Not covered	#	Not covered	#	13.Obligation to keep records. 14(1)(2)Confidentiality	<	53.Identification of critical database	<

5.2.2 Information labeling and handling	164.308(a)(7)(ii)(e)Applications and data criticality analysis	~	Not covered	#	Not covered	#	14(1)(2)Confidentilaity	<	55.Management of critical database	<
6. Personnel Security										
6.1 Security in Job Definition and Resourcing										
6.1.1 Including security in job responsibilities	164.308(a)(3)Authorization and/or Supervision	<	160.102;164.103;164;501.164.104;164.500(2)(3)Transmitting health info electronically in connection with standard transactions	~	Not covered	#	Not covered	#	86Unauthorized access to, interception or interference with data	~
6.1.2 Personnel screening and policy	164.308(a)(3)(i)Workforce security	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
6.1.3 Confidentiality agreements	164.308(a)(3)(i)Workforce Security. 164.314(a)(1)Business associate contracts or other arrangements. 164.308(b)Risk management	~	Not covered	#	Not covered	#	14(1)(2)Confidentiality	<	32(1)(2)Application of Chapter and offences. 35.Accreditaion	<
6.1.4 Terms and conditions of employment	164.308(a)(1)(ii)(c)Sanction Policy	<	160.308 & 160.310 & 160.312.C.Penalties	<	Not covered	#	17(1) Protection of health records	~	29(2)Register of cryptography provider. 30Registration with department	<
6.2 User Training										
6.2.1 Information Security education and training	164.308(a)(5)ii(a)Security Reminders. 164.308(a)(5)ii(b) Protection from malicious software	<	164.5309(b) Training	~	Not covered	#	Not covered	#	Not covered	#
6.3 Responding to Security Incidents and Malfunctions										
6.3.1 Reporting security incidents	164.308(a)(6)Response and Reporting	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
6.3.2 Reporting security weaknesses	164.308(a)(1)(ii)(D)Information system activity review. 164.308(a)(6)(ii)Response and reporting	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
6.3.3 Reporting software malfunctions	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#

6.3.4 Learning from incidents	164.308(a)(6)(ii)Response and reporting. 164.308(a)(1)(ii)(b) Risk management	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
6.3.5 Disciplinary process	164.308(a)(1)(ii)(c)Sanction Policy	~	Not covered	#	Not covered	#	12(f) Procedures for laying complaints. 18.Laying of complaints	<	32(1)(2)Application of Chapter and offences. 89Penalties	<
7. Physical and Environmental Security										
7.1 Secure Areas										
7.1.1 Physical security perimeter	164.310(a)(1)Facility access controls	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.1.2 Physical entry controls	164.310(a)(1)Access Control and Validation Procedures. 164.310(a)(2)(ii)Facility security plan. 164.310(a)(2)(iii)Access control and validation procedures	~	Not covered	#	Not covered	#	17(1)(2)Protection of health records	<	Not covered	#
7.1.3 Securing offices, rooms and facilities	164.310(a)(1)Access Control and Validation Procedures. 164.310(a)(2)(ii)Facility security plan.164.310(a)(2)(iii)Access control and validation procedures.164.310(b)Workstation use. 164.310(c)Workstation security	~	Not covered		Not covered	#	17(1)(2)Protection of health records	<	Not covered	#
7.1.4 Working in secure areas	164.310(a)(1)Facility access controls. 164.310(a)(2)(ii)Facility security plan. 164.310(a)(2)(iii) Access control and validation procedures.164.310(b)Workstation use. 164.310(c)Workstation security	~	Not covered	#	Not covered	#	15(1)Access to health records. 16(1)Access to health records by healthcare provider	<	Not covered	#

7.1.5 Isolated delivery and loading areas	164.310(a)(1)Facility access controls.164.310(a)(2)(ii)Facility security plan. 164.310(a)(2)(iii) Access control and validation procedures	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.2 Equipment Security										
7.2.1 Equipment sitting and protection	164.310(b)Workstation Use 164.310(c)Workstation Security. 164.310(a)(2)(ii)Facility security plan.	<	Not covered	#	Not covered	#	Not covered	#	87.Computer related extortion, fraud and forgery	<
7.2.2 Power supplies	164.310(a)(2)(ii)Facility security plan	>	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.2.3 Cabling security	164.310(a)(2)(ii)Facility security plan	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.2.4 Equipment maintenance	164.310(a)(2)(ii)Facility security plan.164.310(a)(2)(iii)Access control and validation procedures. 164.310(a)(1)Facility access controls. 164.310(d)(2)(iii)Device and media controls. 164.310(d)(2)(iv) Data backup and storage	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.2.5 Security of equipment off-premises	164.310(a)(2)(ii)Facility security plan. 164.310(d)(2)(iii) Accountability	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.2.6 Secure disposal or re-use of equipment	164.310(d)(2)Media Re-use. 164.310(a)(2)(ii)Facility security plan.	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.3 General Controls										
7.3.1 Clear desk and clear screen policy	164.310(b)Workstation use. 164.310(c)Workstation Security.	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
7.3.2 Removal of property	164.310(d)(2)(iii)	~	Not covered	#	Not	#	Not covered	#	Not covered	#

	Accountability				covered					
8. Communications and Operations Management										
8.1 Operational Procedures and Responsibilities										
8.1.1 Documented operating procedures	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.1.2 Operational change control	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.1.3 Incident management procedures	164.308(a)(6)Security incident procedures	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.1.4 Segregation of duties	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.1.5 Separation of development and operational facilities	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.1.6 External facilities management	164.308(b)(1)Business associate contracts and other arrangement. 164.314(a) Business associate contracts and other arrangement	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.2 System Planning and Acceptance										
8.2.1 Capacity planning	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.2.2 System acceptance	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.3 Protection against malicious software										
8.3.1 Controls against malicious software	164.308(a)(5)(ii)(b)Protection Against Malicious Software. 164.312(a)(1)Access control	~	Not covered		Not covered	#	Not covered	#	Not covered	#
8.4 Housekeeping										
8.4.1 Information back-up	164.308(a)(7)(ii)(a)Data Backup and Storage. 164.310(d)(2)(iv) Data backup and storage	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#

8.4.2 Operator logs	164.312(b)Audit Controls. 164.310(a)(1)(ii)(d)Testing and revision procedures	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.4.3 Fault logging	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.5 Network Management										
8.5.1 Network controls	164.312(a)(1)Access control	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.6 Media Handling and Security										
8.6.1 Management of removable computer media	164.310(d)Device and Media Controls	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.6.2 Disposal of media	164.310(d)(2)(i)Disposal of media. 164.310(d)(2)(iii) Accountability	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.6.3 Information handling procedures	164.312(c)(2)Mechanisms to authenticate electronic protected health information. 164.310(d)(1) Device and Media controls. 164.310(a)Facility access controls. 164.310(a)(2)(iii) Access control and validation procedures. 164.310(d)(2)(iii) Accountability	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.6.4 Security of system documentation	Not covered	#	Not covered	#	Not covered	#	Not covered	#	56.Restrictions on disclosure of information	<
8.7 Exchanges of Information and Software										
8.7.1 Information and software exchange agreements	164.301(b)(1)Business associate contracts and other arrangements	~	Not covered	#	Transaction and code sets standards	>	Not covered	~	Not covered	#
8.7.2 Security of media in transit	164.310(d)(1) Device and media controls	<	160.102;160.103;164.104;164;500. A.3Transmitting information in the required "standard format"	<	Transaction and code sets standards	~	17(1)(2)(h)Protection of health records	<	Not covered	#

8.7.3 Electronic commerce security	164.312(e) Transmission security	~	Not covered	#	Transaction and code sets standards	>	Not covered	~	VII. Consumer Protection. 43Information to be provided. 45Unsolicited goods, services or communications	>
8.7.4 Security of electronic mail	164.312(a)(1)Access control. 164.312(e)(1)Transmission security	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.7.5 Security of electronic office systems	164.310(b)Workstation use. 164.310(a)(1)Facility access controls. 164.312(a)(1) Access control	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
8.7.6 Publicly available systems	164.312(a)(1)Access control. 164.312(c)Integrity. 164.312(d)Person or entity authentication. 164.312(e) Transmission security	~	Not covered	#	Not covered	#	17(1)(2)Protection of health records	<	Not covered	#
8.7.7 Other forms of information exchange	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9. Access Control										
9.1 Business Requirement for Access Control										
9.1.1 Access control policy	164.308(a)(3)(i)Workforce Security. 164.312(a)(1) Access control.	>	160.103;160.501;164.514;164.514(a)(e). B. What is covered? 164.524Right to Inspect and Copy. 164.502(a)B. Permitted Uses and Disclosures. 164.502(b) 164.514(d) Minimum Necessary	>	Not covered	#	12.Duty to disseminate information. 14(1)(2)Confidentiality 15(1)Access to health records. 16Access to health records by healthcare provider	~	55(1)(2)Management of critical database. 56Restriction on the disclosure of information	<
9.2 User Access Management										
9.2.1 User registration	164.308(a)(4)(i)Access Establishment and Modification 164.308(a)(3)(ii)(c)Workforce clearance procedures 164.308(a)(3)Access Authorization 164.308(a)(3) Termination Procedures 164.312(a)(2)(i) Unique	~	164.524Right to Inspect and Copy. 164.526Right to Amend	<	Not covered	#	12.Duty to disseminate information. 17(1)(2)Protection of health records	~	Not covered	#

	User Identification									
9.2.2 Privilege management	164.308(a)(3)Access Authorization. 164(308)(a)(4) Access Establishment and Modification	<	164.524 Right to inspect and copy 164.502(b);164.514(d) Minimum Necessary. 164.502(a) 164.508 Revocation of authorization	~	Not covered	#	12.Duty to disseminate information.	<	Not covered	#
9.2.3 User password management	164.308(a)(5)(ii)(d)Password Management	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.2.4 Review of user access rights	164.308(a)(4)(ii)(c)Access establishment and modification	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.3 User Responsibilities										
9.3.1 Password use	164.308(a)(5)(ii)(d)Password Management	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.3.2 Unattended user equipment	164.310(b)Workstation Use. 164.310(c) Workstation security 164.312(a)(2)(iii)Automatic logoff	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4 Network Access Control										
9.4.1 Policy on use of network services	164.312(a)(1)Access control. 164.312(d)(2)Transmission security. 164.308(a)(4)(ii)(b) Access authorization	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4.2 Enforced path	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4.3 User authentication for external connections	164.312(d)Person or Entity Authentication	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4.4 Node authentication	164.312(d)Person or Entity Authentication.	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#

9.4.5 Remote diagnostic port protection	164.312(a)(1)Access control. 164.312(a)(2)(i)Unique user authentication. 164.312(d) Person or Entity authentication	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4.6 Segregation in networks	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4.7 Network connection control	164.312(e)(1)Transmission security	~	Not covered	#	Not covered	#	Not covered	#	Not covered	
9.4.8 Network routing control	164.312(a)(1)Access control	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.4.9 Security of network services	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.5 Operating System Access Control										
9.5.1 Automatic terminal identification	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.5.2 Terminal log-on procedures	164.308(a)(5)(ii)(d)Password Management	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.5.3 User identification and authentication	164.312(a)(2)(i)Unique User Identification	>	Not covered	#	Not covered	#	Not covered	#	VI. Authentication Service Providers	>
9.5.4 Password management system	164.308(a)(5)(ii)(d)Password Management	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.5.5 User of system utilities	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.5.6 Duress alarm to safeguard users	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.5.7 Terminal time-out	164.312(a)(2)(iii)Automatic Logoff	~	Not covered	#	Not covered	#	Not covered	#	31(1)(2)Restrictions on disclosure of information	<
9.5.8 Limitation of connection time	164.312(a)(2)(iii)Automatic Logoff	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.6 Application Access Control										
9.6.1 Information access restriction	164.312(a)(1)Access control. 164.308(a)(4)(ii)(b)Access authorization. 164.308(a)(4)(ii)(c) Access authorization and	~	Not covered	#	Not covered	#	12(d) Procedures for access to health services	~	31(1)(2)Restrictions on disclosure of information	<

	modification									
9.6.2 Sensitive system isolation	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.7 Monitoring System Access and Use										
9.7.1 Event logging	164.312(b)Audit Controls	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.7.2 Monitoring system use	164.308(a)(1)(ii)(d)Information Security Activity Review. 164.308(a)(5)(ii)(c)Log-in monitoring	>	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.7.3 Clock synchronization	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.8 Mobile Computing and Teleworking										
9.8.1 Mobile computing	164.312(a)(1)Access control. 164.308(a)(1)(i)Security management process. 164.308(a)(5)(i)Security awareness and training. 164.310(b)Workstation use. 164.310(c)Workstation security. 164.312(e)(1)Transmission security	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
9.8.2Teleworking	164.312(a)(1)Access control. 164.308(a)(1)(i)Security management process. 164.308(a)(5)(i)Security awareness and training. 164.310(b)Workstation use. 164.310(c)Workstation security. 164.312(e)(1) Transmission security	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10. Systems Development and Maintenance										

10.1 Security Requirements of Systems										
10.1.1 Security requirements analysis and specification	164.308(a)(1)(i)Security management process. 168.308(a)(1)(ii)(c)Sanction policy.168.308(a)(1)(ii)(b)Risk management	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.2 Security in Application Systems										
10.2.1 Input data validation	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.2.2 Control of internal processing	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.2.3 Message authentication	164.312(c)(1)Integrity. 164.312(d)(2) Integrity controls. Encryption	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.2.4 Output data validation	164.312(c)(2)Mechanisms to authenticate electronic protected health information.	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.3 Cryptographic Controls										
10.3.1 Policy on the use of cryptographic controls	164.308(a)(1)(i)Security management process. 168.308(a)(1)(ii)(a)Risk analysis	<	Not covered	#	Not covered	#	Not covered	#	V.Crytography providers: 31. Restriction of disclosure of information	~
10.3.2 Encryption	164.312(a)(2)(iv)Encryption and Decryption. 164.312(e)(2)(ii) Encryption	<	Not covered	#	Not covered	#	Not covered	#	VI. Authentication Service Providers. 32. Application of Chapter and Offences	<
10.3.3 Digital signatures	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.3.4 Non-repudiation services	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.3.5 Key management	164.312(a)(2)(iv)Encryption and Decryption.	~	Not covered	#	Not covered	#	Not covered	#	V.Cryptography providers: 31. Restriction of disclosure of information	~
10.4 Security of System Files										
10.4.1 Control of operational software	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	17.(2)(J)(i)Protection of health records	<	Not covered	#

10.4.2 Protection of system test data	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.4.3 Access control to program source library	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	17.(2)(J)(ii)Protection of health records	<	Not covered	#
10.5 Security in Development and Support Processes										
10.5.1 Change control procedures	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.5.2 Technical review of operating system changes	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.5.3 Restrictions on changes to software packages	164.312(c)(1)Integrity	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.5.4 Covert channels and Trojan code	134.308(a)(5)(ii)(b)Protection from malicious software	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#
10.5.5 Outsourced software development	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
11. Business Continuity Management										
11.1 Aspects of Business Continuity Management										
11.1.1 Business continuity management process	164.308(a)(7)(i)Contingency Plan. 164.310(a)(2)(i)Contingency operations. 164.312(a)(2)(ii) Emergency access procedure	<	Not covered	#	Not covered	#	Not covered	#	55(d)(e)Management of critical database	<
11.1.2 Business continuity and impact analysis	164.308(a)(7)(ii)(e)Applications and Data Criticality Analysis	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#
11.1 3 Writing and implementing continuity plans	164.308(a)(7)(ii)(a)Data backup Plan. 164.308(a)(7)(ii)(b)Disaster recovery plan. 164.308(a)(7)(ii)(c)Emergency mode operation. 164.308(a)(7)(ii)(d)Testing and revision procedure. 164.310(a)(2)(ii)Facility security plan.	~	Not covered	#	Not covered	#	Not covered	#	Not covered	#

	164.312(a)(2)(ii)Emergency access procedures.									
11.1.4 Business continuity planning framework	164.308(a)(7)(ii)(d)Testing and revision procedure.	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#
11.1.5 Testing, maintaining and reassessing business continuity plans	164.308(a)(7)Testing and Revision Procedures	<	Not covered	#	Not covered	#	Not covered	#	Not covered	#
12. Compliance										
12.1 Compliance with Legal Requirements										
12.1.1 Identification of applicable legislation	Not covered	#	164.530(b) Safeguards	<	Not covered	#	Not covered	#	Not covered	#
12.1.2 Intellectual property rights (IPR)	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
12.1.3 Safeguarding of organizational records	164.316(b)(1) Policies and procedures documentations	~	160.103; 164.501; 164.514(a) What is covered?	<	Not covered	#	13.Obligation to keep record. 17.(1)(2)Protection of health records. 11.Health services for experimental or research purposes. 12(d)Procedures for access to the health services	>	IX. Protection of critical databases. 31(1)(2)Restrictions on disclosure of information. VIII. Protection of personal information	~

12.1. 4 Data protection and privacy of personal information	164.306(a) Security standards: General requirements. 164.308(a)(2)Assigned security responsibility	~	164.501; 164.502(g) Who may exercise privacy right? 164.524 Right to inspect and copy. 164.526 Right to amend.164.502(a) Permitted Uses and Disclosures .160.102;160.103;164.104;164;500Who is covered?164.502(b);164.514(d) Minimum Necessary 164.502(a)(b) Permissive and Mandatory 164.502(a)Incidental Use and Disclosure 160.103;164.502(e); 164.504(e); 164.532(d)(e) Business Associates 164.502(a);164.508 Authorization. 164.512(f) Law Enforcement. 164.5129(a)Required by Law	>	Transaction and code sets standards	>	14.(1)Confidentiality. 7.Consent of User. 13.Obligation to keep records. 12.Duty to disseminate information. 15.(1) Access to health records. 16.(1)(2) Access to health records by healthcare provider. 17.(1) (2)Protection of health records. 18.Laying of complaints. 11.Health services for experimental or research purposes	>	VIII. Protection of Personal Information: 50.Scope of personal information. 51. Principles for electronically collecting personal information. 88.Attempt, and aiding and abetting. 89. Penalties. 31(1)(2)Restrictions on disclosure of information. 32(1)(2)Application of Chapter and offences	>
12.1.5 Prevention of misuse of information processing facilities	164.310(a)(1)Facility access control. 164.310(b)Workstation use. 164.308(a)(3)Workforce security	~	Not covered	#	Not covered	#	17.(1) (2)(i)Protection of health records.	~	XIII. Cyber Crime	>
12.1.6 Regulation of cryptographic controls	Not covered	#	Not covered	#	Not covered	#	Not covered	#	V. Cryptography providers: 31. Restriction of disclosure of information	~
12.1.7 Collection of evidence	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
12.2 Reviews of Security Policy and Technical Compliance										
12.2.1 Compliance with Security Policy	164.308(a)(8)Evaluation	~	160.308; 160.310; 160.312 Compliance Reviews	~	Not covered	#	Not covered	#	57.Right of inspection	<
12.2.2 Technical compliance checking	164.308(a)(8)Evaluation	~	160.308; 160.310; 160.312 Compliance Reviews	<	Not covered	#	Not covered	#	XII. Cyber Inspectors 81.Power of cyber inspectors 82.Power to inspect search and seize. 83. Obtaining warrant. 84. Preservation of confidentiality	>

12.3 System Audit Considerations										
12.3.1 System audit controls	164.308(a)(8)Evaluation	~	Not covered	#	Not covered	#	Not covered	#	57.Right of inspection. 58Non compliance with chapter	<
12.3.2 Protection of system audit tools	Not covered	#	Not covered	#	Not covered	#	Not covered	#	Not covered	#
Regulation requirements not covered in ISO17799 standard										
New security measure	164.308(a)(4)ii(A) Isolating Healthcare Clearinghouse	>	160.102;160.103; 164.104; 160.500 Who is covered?	>	X2N837HealthcareClaim	>	14.Confidentiality of health records	>	29. Register of cryptography providers.	>
New security measure	164.310(a)(2)(ii) Emergency Access Procedures	>	164.501;164.506;164.520(c); 164.522 Treatment, Payment, and Healthcare Operations; General rule for use and disclosure; consent; Right to request restrictions; Limited data set	>	X12N 835 - Healthcare Claim Payment/Advice	>	6.User to have a full knowledge	>	30. Registration with Department.	>
New security measure	164.308(a)(6) Security Incident Procedures	>	164.510(a) Facility Directories	>	X12N 835 - Healthcare Claim Payment/Advice	>	7.Consent of user	>	32. Application of Chapter and Offences	>
New security measure	164.308(a)(7)(ii)(C) Emergency Mode Operation Plan	>	164.5109(b); 165.522 Disclosure to those Involved in Providing Care(Next of Kin)	>	X12N 820 - Payroll Deducted and Other Group Premium Payment for Insurance Products	>	8.Participation in decisions	>	34. Appointment of Accreditation Authority and other officers	>
New security measure	164.308(b)(1) Business Associate Contracts and Other Arrangements	>	164.501; 164.508(a)(3) Marketing	>	X12N 278 - Healthcare Services Request for Review and	>	9.Health service without consent	>	35. Accreditation to be voluntary	>

					Response					
New security measure	164.310(a)(2)(ii) Facility Security Plan	>	164.501;164.514(f); 164.522 Fundraising	>	X12N 276 - Healthcare Claim Status Request	>	10.Discharge reports	>	36. Powers and duties of Accreditation Authority	>
New security measure	164.310(a)(2)(i) Contingency Operations	>	164.512(j) Avertising a serious Threat to Health or Safety	>	X12N 277 - Healthcare Claim Status Response	>	11.Health services for experimental or research purposes	>	37. Accreditation of Authentication products and services	>
New security measure	164.310.(a)(3)ii (c) Termination Procedures	>	164.512(d)Health oversight Activities	>	X12N 270 - Healthcare Claim Eligibility Inquiry	>	12.Duty of disseminate information	>	38. Criteria for accreditation	>
New security measure	164.310(a)(2)(iv) Maintenance Records	>	164.512(e) Judicial and Administrative Proceedings	>	X12N 271 - Healthcare Claim Eligibility Response	>	13.Obligation to keep records	>	39. Revocation or termination of accreditation	>
New security measure	164.310(a)(5)ii (c)Log-In Monitoring	>	164.512(b); 164.514(e) Public Health Activities.	>	X12N 148 - Report of Injury or Illness	>	17.Protection of health records	>	40. Accreditation of foreign products and services	>
New security measure	164.310(e)(1) Transmission Security	>	164.512(c) Victims of Abuse, Neglect, or Domestic Violence	>	X12N 186 - Life and Annuity Lab Report	>	18.Laying of complaints	>	41. Accreditation regulations	>
New security measure	164.310.(a)(2)(i) Unique User Authentication	>	164.512(i) Workers' Compensation	>	X12N 275 - Patient Information	>	20.Rights of healthcare personnel	>	43. Information to be provided	>
New security measure	164.310.(a)(2)(iv) Data Back-up and storage	>	164.500; 164.520 Notice	>	ICD_9_CM _Diagnosis & Inpatient Procedures	>	19.Duties of users	>	44. Cooling-off period	>

New security measure			164.528Accounting for Disclosures	>	CPT_4 Outpatient Procedures	>			45.Unsolicited goods, services or communications	>
New security measure			164.528 Accounting for Disclosures	>	HCPCS_Ancillary Services and Procedures	>			46.Performance	>
New security measure			164.5.4(a)-(c) Disclosures for Hybrid Entity	>	NDC_National Drug Codes	>			47.Applicability of foreign law	>
New security measure			160.306 & 160.312Complaints	>	Non Medical Code Sets	>			48. Non-excusion	>
New security measure			164.504(g) Disclosures for Multiple Covered Function Entity	>					49. Complaints to Consumer Affairs Committee	>
New security measure			164.504(f) Disclosures for Group Health Plan	>					52. Scope of critical database protection	>
New security measure			164.501 & 164.520 Disclosures for Organized Healthcare Arrangement	>					53. Identification of critical data and critical databases	>
New security measure			160.306 & 160.312 Complaints	>					54. Registration of critical databases	>
New security measure			160.308 & 160.310 & 160.132 Compliance Reviews	>					55. Management of critical databases	>
New security measure			164.512(i);164.514(e) Research.	>					56.Restrictions on disclosure of information	>
New security measure			164.510(b) & 164.522Disclosures to those Involved in Providing Care (Next of Kin)	>					57. Right of inspection	>

New security measure			164.504(a)-(c)Hybrid Entity. 164.504(d)Affiliated Covered Entity. 164.504(g)Multiple Covered Function Entity. 164.504(f) Group Health Plan (Restrictions on Disclosures to Employers). 164.501 & 164.520. Organized Healthcare Arrangement	>					58. Non Compliance with chapter	>
New security measure			160.201 & 160.202 & 160.203 & 160.204 & 160.205 Preemption	>					80.Appointment of cyber inspectors	>

Appendix B

ISO 17799 Main Sections

1.Security Policy	*Provides guidelines and management advice for improving Information Security through the issue of an Information Security policy through the organization.*
Information Security policy document	A set of implementation-independent, conceptual Information Security policy statements governing the security goals of the organization. This document, along with a hierarchy of standards, guidelines, and procedures, helps implement and enforce policy statements. Policies are organizations laws, in the sense that they dictate acceptable and unacceptable behaviour within the context of the organization's culture (Whitman & Mattford, 2003).
Review and evaluation	Ongoing management commitment to Information Security is established by assigning ownership and review schedules for the Information Security Policy document.
2.Organizational security	*Facilitate Information Security management within the organization. This addresses the need for a management framework that creates, sustains, and manages the Information Security infrastructure.*
Management Information Security forum	Provides a multi-disciplinary committee chartered to discuss and disseminate Information Security issues throughout the organization.
Information Security co-ordination	acts as a central point of contact for Information Security issues, direction, and decisions
Information Security responsibilities	individual Information Security responsibilities are unambiguously allocated and detailed within job descriptions
Authorization process for information processing facilities	ensures that security considerations are evaluated and approvals obtained for new and modified information processing systems
Specialist Information Security advice	Maintains relationships with independent specialists to allow access to expertise not available within the organization
Co-operation between organizations	Maintains relationships with both information sharing partners and local law enforcement authorities
Independent review	Mechanisms to allow independent review of security effectiveness.
Third-party access	Mechanisms to govern third-party interaction within the organization based on business requirements
Outsourcing	Organizational outsourcing arrangements should have clear contractual security requirements
3.Asset Classification and Control Section	*To carry out an inventory of assets and protect these assets effectively. This*

	section is more concerned with the effective administration, from a security viewpoint, of the organization hardware and software assets
Accountability and inventory	Mechanisms to maintain an accurate inventory of assets, and establish ownership and stewardship of all assets.
Classification	Mechanisms to classify assets based on business impact.
Labeling	Labeling standards unambiguously brand assets to their classification.
Handling	Handling standards; including introduction, transfer, removal, and disposal of all assets; are based on asset classification.
4.Personnel Security	*To minimize the risks of human error, theft, fraud or the abusive use of equipment". These risks increased dramatically as computing was first moved from the computer centre to the office worker's desk, and even more so when organizations linked their computers with networks*
Personnel screening	Policies within local legal and cultural frameworks ascertain the qualification and suitability of all personnel with access to organizational assets. This framework may be based on job descriptions and/or asset classification.
Security responsibilities	Personnel should be clearly informed of their Information Security responsibilities, including codes of conduct and non-disclosure agreements.
Terms and conditions of employment	Personnel should be clearly informed of their Information Security responsibilities as a condition of employment.
Security education and Training	A mandatory Information Security awareness training program is conducted for all employees, including new hires and established employees.
Reporting security incidents, weaknesses and software malfunction	Reporting security incidents, weaknesses and software malfunction
Learning from incidents	Mechanisms to quantify incidents for the future reference
Disciplinary process	A formal process to deal with violation of Information Security policies and procedures.
5.Physical and Environmental Security	*To prevent the violation, deterioration or disruption of industrial facilities and data.*
Physical security perimeter	The premises security perimeter should be clearly defined and physically sound.
Access control	Breaches in the physical security perimeter should have appropriate entry/exit controls commensurate with their classification level.
Location	Organizational premises should be analyzed for environmental hazards.
Equipment security	Equipment should be sited within the premises to ensure physical and environmental integrity and availability.
Isolating delivery and loading areas	Mechanisms to track entry and exit of assets through the security perimeter.
General controls	Policies and standards, such as utilization of shredding equipment, secure

	storage, and "clean desk" principles, should exist to govern operational security within the workplace.
6.Communications and Operations Management	*To ensure the adequate and reliable operation of information processing devices.*
Operational procedures	Comprehensive set of procedures, in support of organizational standards and policies.
Change control	Process to manage change and configuration control, including change management of the Information Security Management System.
Incident management	Mechanism to ensure timely and effective response to any security incidents.
Segregation of duties	Segregation and rotation of duties minimize the potential for collusion and uncontrolled exposure.
Capacity planning	Mechanism to monitor and project organizational capacity to ensure uninterrupted availability.
System acceptance	Methodology to evaluate system changes to ensure continued confidentiality, integrity, and availability.
Malicious code	Controls to mitigate risk from introduction of malicious code.
Housekeeping	Policies, standards, guidelines, and procedures to address routine housekeeping activities such as backup schedules and logging.
Network management	Controls to govern the secure operation of the networking infrastructure.
Media handling	Controls to govern secure handling and disposal of information storage media and documentation.
Information exchange	Controls to govern secure handling and disposal of information storage media and documentation.
7.Access Control	*To control access to information*
Business requirements	Policy controlling access to organizational assets based on business requirements and "need to know".
User access management	Includes mechanisms to register and deregister users; control and review of access and privileges.
User responsibilities	Informing users of their access control responsibilities, including password stewardship and unattended user equipment.
Network access control	Policy on usage of network services, including mechanisms to appropriate manage interfaces between organization's network and public networks; appropriate authentication and control of user access mechanisms for user access to information services.
Operating system access control	Ensuring that security facilities at the operating level should be used to restrict access to computer resources.
Application access control	Limits access to applications based on user or application authorization levels.

Access monitoring	Mechanisms to monitor system access and system use to detect unauthorized activities.
Mobile computing and teleworking	Policies and standards to address asset protection, secure access, and user responsibilities.
8.Systems Development and Maintenance	*To ensure that security is incorporated and maintained into information systems.*
System security requirements	Incorporates Information Security considerations in the specifications of any system development or procurement.
Application security	Incorporates Information Security considerations in the specification of any application development or procurement.
Cryptography	Policies, standards, and procedures governing the usage and maintenance of cryptographic controls.
Security of system files	Mechanisms to control access to, and verify integrity of, operational software and data, including a process to track, evaluate, and incorporate asset upgrades and patches.
Development security	Integrates change control and technical reviews into development process.
9.Business Continuity Management	*To minimize the impact of business interruptions and protect the company's essential processes from failure and major disasters.*
Business continuity planning	Business continuity strategy based on a business impact analysis.
Business continuity testing	Testing and documentation of business continuity strategy.
Business continuity maintenance	Identifies ownership of business continuity strategy as well as ongoing re-assessment and maintenance.
10.Compliance	*To avoid any breach of criminal or civil law, of statutory or contractual requirements, and of security requirements. Information Security is not a necessary an option that can be accepted or rejected by senior management of an organization. Increasingly, there are legislative and regulatory requirements that require an Information Security infrastructure for compliance.*
Legal requirements	Includes awareness of relevant legislation; intellectual property rights; Safeguarding of organizational records; Data protection and privacy of personal health information; Prevention of misuse; Regulation of cryptography and collection of evidence.
Technical requirements	Mechanisms to verify execution of security policies and implementations.
System audits	Auditing controls to maximize effectiveness, minimize disruption, and protect audit tools.

Appendix C

Paper published in the Proceedings of the 5th Annual Information Security South Africa Conference, 29-01 July 2005, Sandton, South Africa.

INFORMATION SECURITY MANAGEMENT AND REGULATORY COMPLIANCE IN THE SOUTH AFRICAN HEALTH SECTOR

T. Tuyikeze[a], D. Pottas[b]

[a] Faculty of Engineering: Computer Studies, Nelson Mandela Metropolitan University, tite@nmmu.ac.za
[b] Faculty of Engineering: Computer Studies, Nelson Mandela Metropolitan University,
dalenca@nmmu.ac.za

[a] tite@nmmu.ac.za, +27 41 504 3574, Private Bag X6011, Port Elizabeth, 6000
[b] dalenca@nmmu.ac.za, +27 41 504 9100, Private Bag X6011, Port Elizabeth, 6000

ABSTRACT

Information Security is becoming a part of core business processes in every organization. Companies are faced with contradictory requirements to ensure open systems and accessible information while maintaining high protection standards. In addition, contemporary management of organizations' Information Security requires various approaches in different areas, ranging from technology to organizational issues and legislation. These approaches are often isolated while security management requires an integrated approach.

Information Technology promises many benefits to healthcare organizations. By helping to make accurate information more readily available to health care providers and workers, researchers and patients, advanced computing and communication technology can improve the quality and lower the costs of health care. However, the prospect of storing health information in an electronic form raises concerns about patient privacy and security.

To ensure an appropriate and consistent level of Information Security for computer-based patient records, both within individual healthcare organizations and throughout the entire healthcare delivery system, healthcare organizations are required to establish formal Information Security programs, for example through the adoption of the ISO 17799 standard. However, proper Information Security management practices alone do not necessarily ensure regulatory compliance. South African health care organizations have to comply with the South African National Health Act (SANHA) and the Electronic Communication Transaction Act (ECTA). It is arguably necessary to consider compliance with the Health Insurance Portability and Accountability Act (HIPAA) in order to meet international industry standards.

The main purpose of this paper is to propose a compliance strategy, which ensures full compliance with regulatory requirements and at the same time guarantees customers that international industry standards are being used. This is preceded by a comparative analysis of the requirements posed by the ISO 17799 standard and the HIPAA, SANHA and ECTA regulations.

KEY WORDS

Information Security management, privacy, healthcare organizations, health information, legal compliance, international security standards, compliance strategy

INFORMATION SECURITY MANAGEMENT AND REGULATORY COMPLIANCE IN THE SOUTH AFRICAN HEALTH SECTOR

1. INTRODUCTION

The healthcare industry is as competitive and multifaceted as any industry in the world today. Healthcare information systems provide many advantages when used for improved access, collaboration and data sharing among healthcare providers, patients, and researchers (Zhang et all, 2002). However, the shift of medical records from paper to electronic formats has increased the potential for individuals to access, use, and disclose sensitive personal health data.

From a historical perspective, the concept of protecting information is a long established ethical code in the healthcare environment. Traditionally, physicians are bound by the Hippocratic Oath, which establishes that what is seen or heard during the course of treatment is to be kept to oneself (Smith, 2004). In today's electronic era, the Oath by itself is no longer sufficient and is extended by government laws and other standards.

Considering the importance of security and privacy, many countries have adopted different regulation frameworks and standards focusing on achieving data integrity, confidentiality and availability of health information.

To ensure an appropriate and consistent level of Information Security for computer-based patient records, both within individual healthcare organizations and throughout the entire healthcare delivery system, healthcare organizations are required to establish formal Information Security programs, for example through the adoption of the ISO 17799 standard. However, proper Information Security management practices alone do not necessarily ensure regulatory compliance and vice versa. South African health care organizations have to comply with the South African National Health Act (SANHA) and the Electronic Communication Transaction Act (ECTA). It is arguably necessary to consider compliance with the Health Insurance Portability and Accountability Act (HIPAA) in order to meet international industry standards.

The main objective of this paper is to propose a compliance strategy that will provide South African healthcare organizations with an approach towards Information Security management, which ensures full compliance with governing regulations and at the same time providing customers with the assurance of meeting an international industry standard for health Information Security and privacy. In order to achieve this objective, a comparative analysis of the ISO 17799 standard (as basis) and SANHA, ECTA, and HIPAA regulations will be done to determine areas of convergence. The outcome of this analysis will assist in formulating an Information Security compliance program, which does not only meet regulatory requirements but also ensures that best practices are being used.

2. AN OVERVIEW OF THE SOUTH AFRICAN HEALTH SYSTEM

According to Roemer (1991), "a health system is a combination of resources, organization, financing and administration that culminates in the health services offered to the population". South Africa's health system is composed of both public and private sectors with a grave difference between the two (Bassett, 2003).

Statistics obtained from safrica.info (2003) show that the public sector is under-resourced and over-used while the growing private sector, run largely along commercial lines, caters to middle- and high-income earners who tend to be members of medical schemes (18% of the population), and to foreigners looking for top-quality surgical procedures at relatively affordable prices. The private sector also attracts most of the country's health professionals. Although the state contributes about 40% of all expenditure on health, the public health sector is under pressure to deliver services to about 80% of the population. Despite this, most resources are concentrated in the private health sector, which sees to the health needs of the remaining 20% of the population.

Considering the increasing number of people in both sectors (35 million in the public sector and seven million in the private sector), the South Africa government has noticed that the use of Information Technology in handling medical records is a necessity not a choice.

The South African government depends on the State Information Technology Agency (SITA), which was established in 1999 with the objective of consolidating and coordinating the State's information technology. As stated in the SITA Act 38 of 2002 section 6, the objectives of the act are:

- To improve service delivery to the public through the provision of information technology, information systems and related services in a maintained information systems security environment to departments and public bodies.
- To promote the efficiency of departments and public bodies through the use of information technology.

Although South Africa's health system faces many challenges related to staff shortages, deteriorating infrastructure, increased centralization, equipment failures and shortages, and an increased influx of (especially HIV/AIDS) patients, the public and private healthcare sectors are showing confidence in information technology's ability to transform the industry and improve healthcare services (EthicSA, 2000). At a Health Informatics Association for Africa conference held in Johannesburg, delegates agreed that it was more prudent to increase investment in IT than in medical technology. IT in healthcare is growing in popularity because of its ability to provide the medical industry with the information it needs to make informed decisions (Powe, 2003). Nevertheless the application of IT to healthcare, especially the development of electronic medical records and linking of clinical databases, has increasingly generated growing concern regarding the privacy and security of health information (National Research Council, 1997).

3. PRIVACY AND SECURITY CONCERNS REGARDING HEALTH INFORMATION

Despite the widespread protection that it is offered in international instruments and constitutional provisions, 'privacy' is however a term that is inherently difficult to define and its definition varies widely (Electronic Privacy Information Center (EPIC) Report 2002). According to Meyer (2001), security and privacy are distinct but related. Privacy is the right of an individual to control the use of his or her personal information. It should not be divulged or used by others against his wishes. Security refers to all the ability to control access and protect information from accidental disclosure to unauthorized persons and from alteration, destruction or loss.

According to the National Research Council (1997), electronic medical records are potentially vulnerable to misuse from both authorized and unauthorized users who inappropriately access patient information for their personal or economic gain. Authorized users may take advantage of their legitimate authority to access information that they have no valid need to see (often regarding a friend, relative, or celebrity), or they may reveal patient information to others often without the patients' consent. Outside attackers may break into computerized information to steal, destroy, or to render the system dysfunctional, preventing legitimate users such as doctors and nurses from accessing information critical to care. Yet considering the highly personal and potentially destructive nature of the medical data, it comes with significant concerns to the privacy and security of such information. In order to gain an understanding of these concerns, it is important to look at major threats that could harm the privacy and security of health information.

The American Society for Testing and Materials (ASTM)'s Provisional Standard (PS 101) "Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information" identifies the following security threats relative to healthcare information (CPRI toolkit, 1995):

- Masquerading, in which one entity pretends to be another, facilitating any subsequent attacks.
- Modification of information, including message or data content, destruction of messages, data or management information.
- Message sequencing threats, including replay, and delay of messages.
- Unauthorized disclosure, which reveals to an unauthorized user message content, information derived from observing message flow, and information held in storage on an open system.
- Repudiation, in which a user or system denies having performed some action, such as modification of information.
- Denial of service – this prevents the systems from performing its functions.

In order to counteract the aforementioned threats, many countries have adopted various regulatory frameworks that focus on achieving data integrity, confidentiality and availability of health information.

4. PROTECTING THE PRIVACY AND SECURITY OF HEALTH INFORMATION

Medical data are considered to be amongst the most sensitive data for civil use as they contain very detailed, personal information about patients and their health information. For centuries, the Hippocratic Oath has expressed the physicians' duty to respect patients' privacy (Kohl, 95). Today, this is no longer sufficient and is extended by civil law and international security standards.

To ensure an appropriate level of Information Security management, South African healthcare organizations are required to establish a formal Information Security program, for example through the adoption of an internationally recognized standard such as the ISO17799 standard. However, it is indeed necessary to adopt the Healthcare Insurance Portability and Accountability Act (HIPAA) standards to overcome some of the criticisms of ISO17799, such as being too general and therefore not providing stringent solutions to specific organizations' requirements, such as in the case of healthcare organizations. In addition, South African healthcare organizations must ensure that they comply with the South African National Health Act (SANHA) and the Electronic Communication Transaction Act (ECTA) requirements in order to ensure due diligence practices.

4.1. Overview of SANHA, ECTA, HIPAA and ISO 17799

The increased use of IT in handling medical records has brought more concerns about privacy and security regarding health information. Such concerns are growing as more sensitive information, such as HIV status, psychiatric records and genetic information is stored in medical records. Addressing these concerns requires both understanding of regulatory requirements and various Information Security standards available for protecting such information.

The ISO/IEC 17799 International standard resulted from the British Standards Institution's (BSI) BS7799 code of practice, which was introduced in 1995 and revised in 1999. Part 1 of BS7799 became ISO standard 17799 in 2000 after being adopted by Joint Technical Committee ISO/IEC JTC1 – Information Technology. Part 2 of BS7799 "Information Security management systems – Specification with guidance for use" has not been yet adopted by ISO as such, but has been accepted by many national standards organisations, among which the South African National Standards (SANS). It is the Part 1 Code of practice for Information Security management that will be used in this paper.

Instead of mandating a specific implementation of Information Security practices, ISO17799 is intended to be used as a "best practice" framework in the development of organizational security policies and practices. The benefits of the framework are to provide a code of practice that induces organizations to consider all factors when developing their security program. However, ISO/IEC 17799 recommends that this code of practice be used as a starting point for developing organization-specific guidance, with particular emphasis on the fact that not all the guidance and controls in the code may be applicable to each organization. Conversely, additional controls not included in the code of practice document may be required (ISO17799). In this sense, healthcare organizations may decide to deal with a subset of controls instead of considering the full list. In addition, it is worthwhile to consider incorporating more controls from other security standards dealing with specific

organizational requirements, for example the use of HIPAA standards by healthcare organizations.

The Healthcare Information Portability and Accountability Act (HIPAA) became law on August 21, 1996. The primary focus of HIPAA is to mandate that healthcare information become "portable" and "available" by legislating the use of uniform electronic transactions and other administrative measures. In forcing the healthcare industry to adopt uniform electronic transaction standards for healthcare information, it is also necessary to protect that same information by including standards for how the information would be secured and safeguarded (CMMS, 1996). The portion of the HIPAA law that most impacts technology interests is the section on Administrative Simplification (Title II, Subtitle F). This section seeks to force uniform standards in the electronic interchange of health information (through the Transaction standard) and also mandates guidelines for the security (Security standard) and privacy (Privacy standard) of that information whether in transit or stored. This paper deals specifically with the security standards because it specifies a series of administrative, technical, and physical security procedures that healthcare organizations should follow to assure the security and privacy of electronic health information.

The South Africa National Health Act (SANHA) or Act 61 of 2003 was signed into act by the South African president on 18 July 2004. SANHA provides a framework for a structured, uniform health system in order to unite the various elements of the national health system in a common goal to improve universal access to quality health services (National Health Act). In briefing media on the National Health Act by the Minister of Health Dr Manto Tshabalala-Msimang, she highlights that this act rests heavily on the constitution with 50 sections of the Constitution relating directly to what is covered in this act. As noticed in section 27(2) of the constitution, the state must take reasonable legislative and other measures to progressively achieve the right of access to health care services and reproductive health care, within its available resources. This paper will only deal with chapter 2 section 17 ("Protection of health records") of this Act because it highlights security and privacy-related issues.

The Electronic Communication and Transaction Act (ECTA), or Act No.25 of 2002 was signed into act by the South African president on 31 July 2002. Being the first South African law governing cyber activity, the act facilitates the development and propagation of electronic communications and transactions within South Africa and aims to promote consumer confidence in electronic transacting and their online privacy (ECTA, 2003). With the increased use of electronic communication transactions in healthcare business transactions, this Act places a heavy burden on medical providers, insurers and claims clearinghouses and other healthcare services partners who need to communicate electronically on a day-to-day basis to accomplish their tasks. The ECTA is expected to facilitate electronic interchange relating to healthcare business transactions for example order placement and processing, shipping and receiving, invoicing, payment, cash application data, insurance transactions, and other data associated with the provision of products and health services.

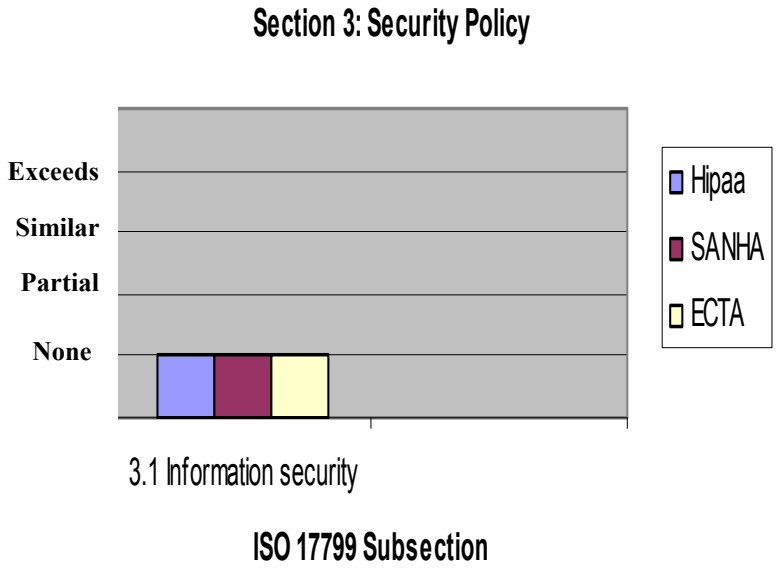
Currently there are a growing number of regulations that include requirements for healthcare organizations to provide security controls and demonstrate compliance

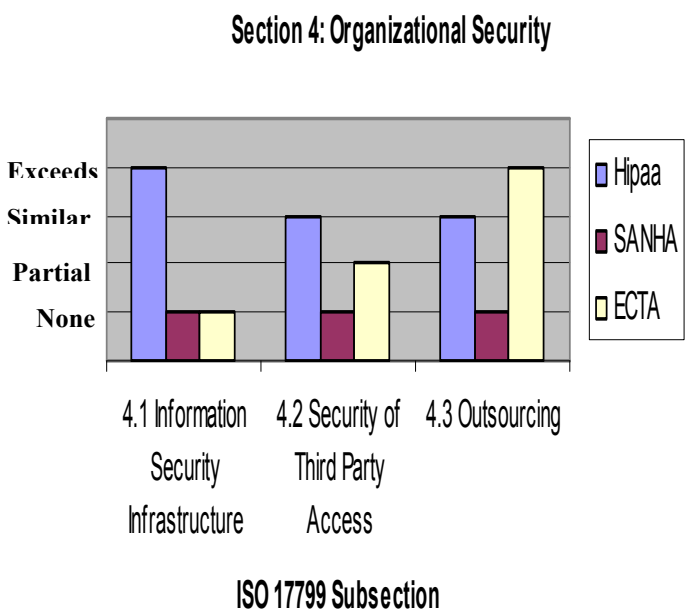
assurance. The challenge encountered by most healthcare organizations is what compliance strategy should be followed to meet regulatory requirements while ensuring that the existing efforts already implemented are maintained. Therefore, a comparative analysis of compliance requirements is required, which in this paper is focussed on the ISO 17799, HIPAA, SANHA and ECTA. The result of this comparison will help to ensure that no security controls are being duplicated in endeavours to satisfy requirements from the various standards and laws.

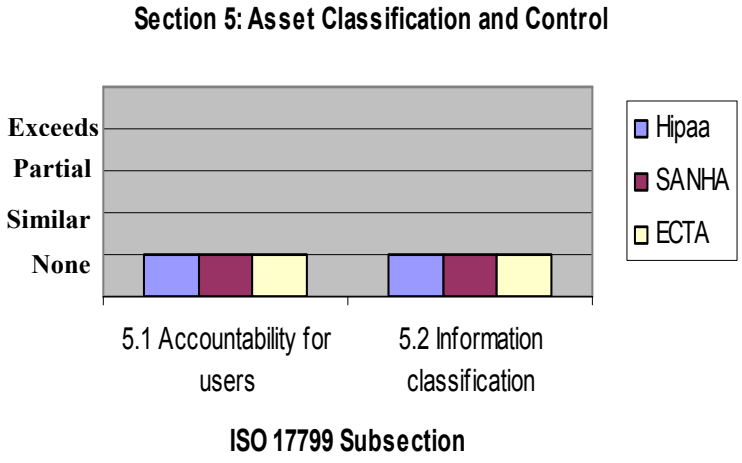
5. COMPARISON BETWEEN ISO 17799, HIPAA SECURITY STANDARDS SANHA AND ECTA LAWS

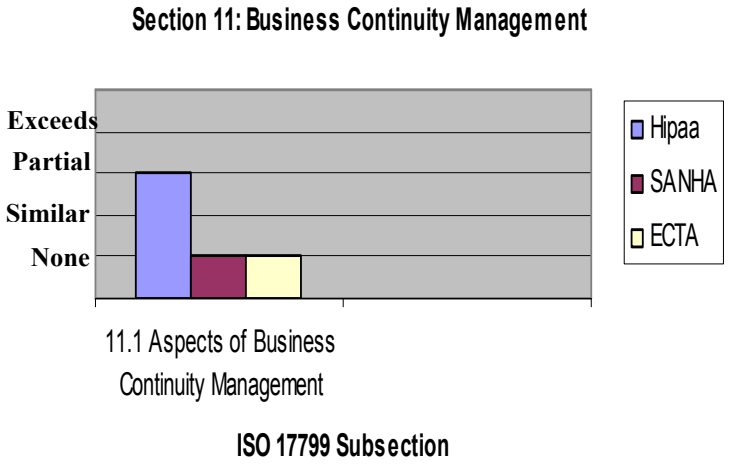
Following is a comparison of each of the ten ISO 17799 controls against SANHA, ECTA and HIPAA security standards. The ISO 17799 will be used as a basis for this comparison. For reasons of simplicity, the HIPAA security standard is often referred to as just "HIPAA" and the ISO/IEC 17799 International Standard is often referred to as just "ISO".

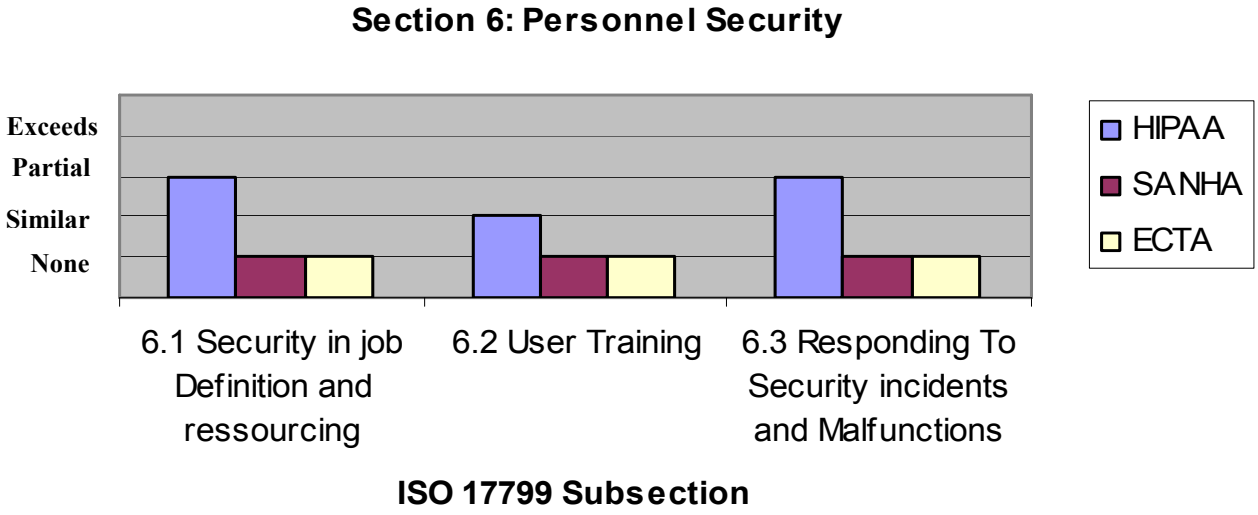
A graphical representation is used which depicts the particular ISO subsection as relating to its coverage in HIPAA, SANHA and the ECT act. Each graph will show to which extent the ISO subsection is covered by the regulation. This can either be not at all (none), partially, similar coverage (similar) or the regulation exceeds the requirements of ISO. It is also important to highlight that this comparison will only deal with the 36 subsections of ISO since dividing these subsections into more subsections will be too lengthy indeed and goes beyond the scope of this paper.

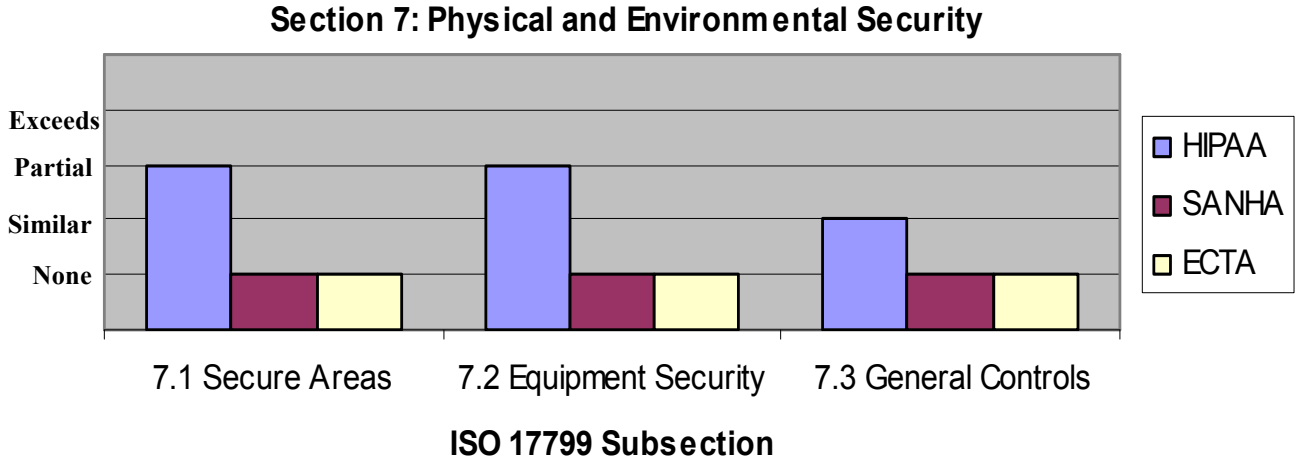


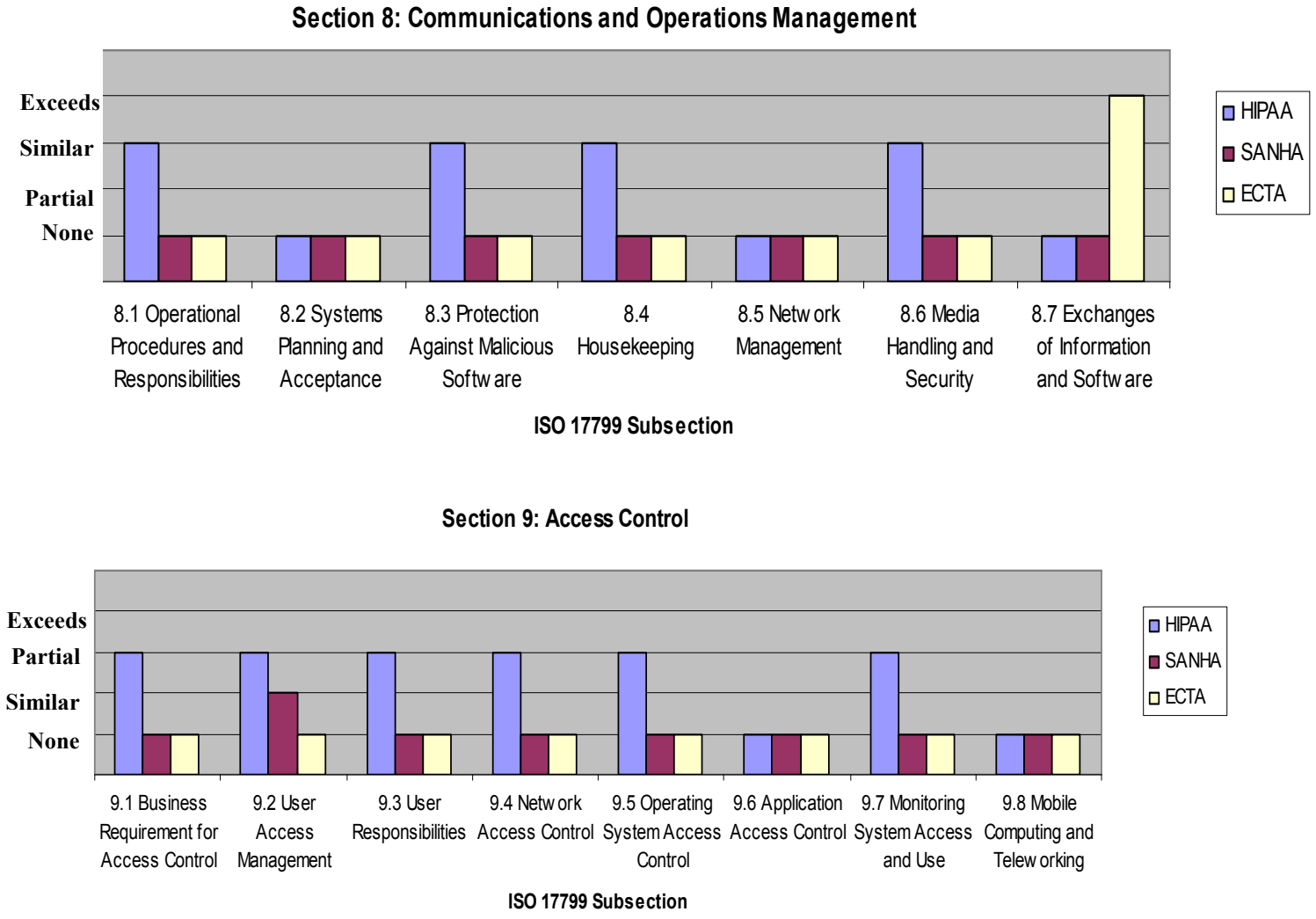



Section 5: Asset Classification and Control
Exceeds
Partial
Similar
None
Hipaa
SANHA
ECTA
5.1 Accountability for users
5.2 Information classification
ISO 17799 Subsection

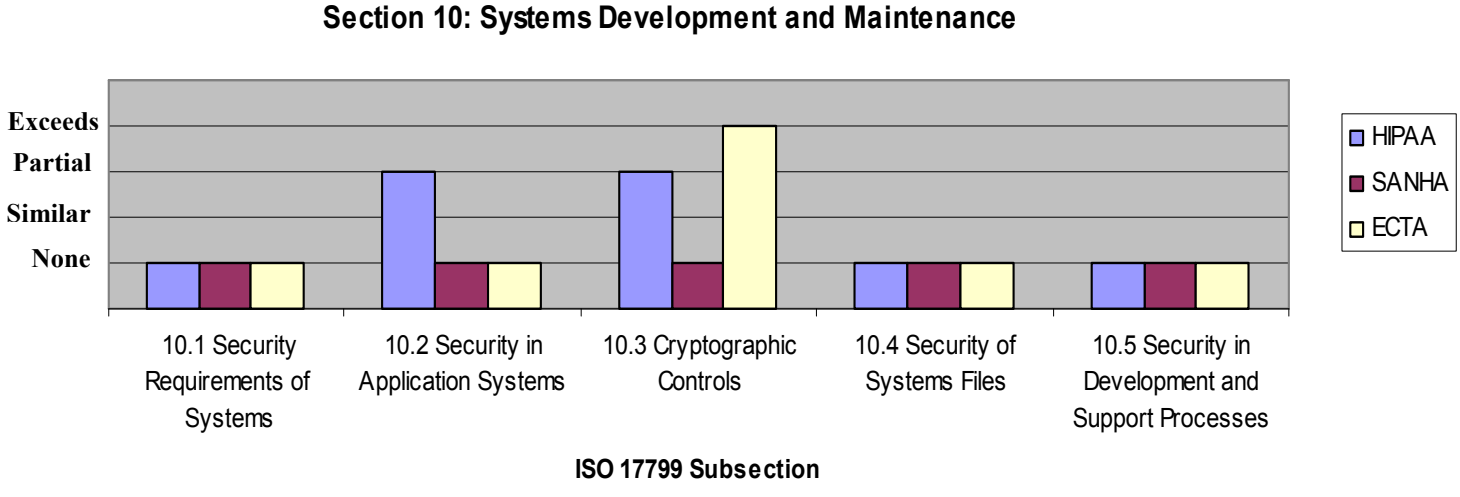

Section 11: Business Continuity Management
Exceeds
Partial
Similar
None
Hipaa
SANHA
ECTA
11.1 Aspects of Business Continuity Management
ISO 17799 Subsection

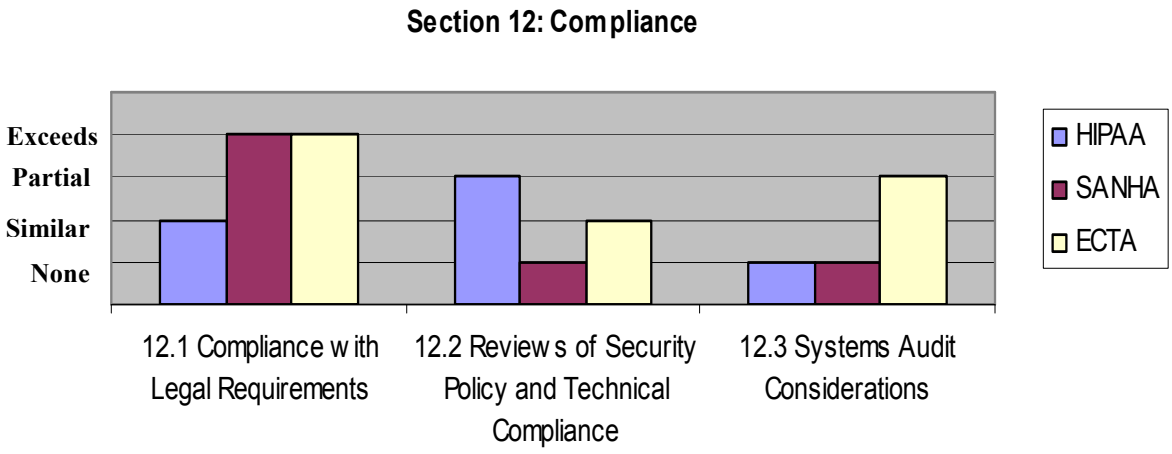

Section 6: Personnel Security
Exceeds
Partial
Similar
None
HIPAA
SANHA
ECTA
6.1 Security in job Definition and ressourcing
6.2 User Training
6.3 Responding To Security incidents and Malfunctions
ISO 17799 Subsection


Section 7: Physical and Environmental Security
Exceeds
Partial
Similar
None
HIPAA
SANHA
ECTA
7.1 Secure Areas
7.2 Equipment Security
7.3 General Controls
ISO 17799 Subsection


Section 8: Communications and Operations Management
Exceeds
Similar
Partial
None
HIPAA
SANHA
ECTA
8.1 Operational Procedures and Responsibilities
8.2 Systems Planning and Acceptance
8.3 Protection Against Malicious Softw are
8.4 Housekeeping
8.5 Netw ork Management
8.6 Media Handling and Security
8.7 Exchanges of Information and Softw are
ISO 17799 Subsection

Section 9: Access Control
Exceeds
Partial
Similar
None
HIPAA
SANHA
ECTA
9.1 Business Requirement for Access Control
9.2 User Access Management
9.3 User Responsibilities
9.4 Netw ork Access Control
9.5 Operating System Access Control
9.6 Application Access Control
9.7 Monitoring System Access and Use
9.8 Mobile Computing and Telew orking
ISO 17799 Subsection


Section 10: Systems Development and Maintenance
Exceeds
Partial
Similar
None
HIPAA
SANHA
ECTA
10.1 Security Requirements of Systems
10.2 Security in Application Systems
10.3 Cryptographic Controls
10.4 Security of Systems Files
10.5 Security in Development and Support Processes
ISO 17799 Subsection



6. ANALYSIS OF THE COMPARISON RESULTS

The main objective of this comparative analysis is to deduce how much effort is required for healthcare organizations to meet regulatory compliance requirements when there is already a well-established Information Security program, which in this case is assumed to be the ISO 17799 security standard.

As shown in the comparison results in section 5, there are some cases where HIPAA, SANHA and ECTA requirements exceed the ISO requirements. Conversely, those items that do not show up in ISO, but are covered in HIPAA, SANHA and ECTA, are shown respectively in Table 1, Table 2 and Table 3 with a brief explanation for each item.

Table 1: Requirements of HIPAA not fully present in ISO17799

	HIPAA requirement	Explanation
1	Administrative:(a)(2) Assigned Security Responsibility	HIPAA requires a single person responsible for both information and physical security
2	Administrative:(a)(3)ii(C) Termination Procedures	ISO has no mention of terminations anywhere in the document
3	Administrative:(a)(4)ii(A) Isolating Healthcare Clearinghouse Functions	Unique requirement of the HIPAA legislation
4	Administrative:(a)(5)ii(C) Log-in Monitoring	ISO does not have a specific training requirement with respect to log-in monitoring
5	Administrative:(a)(7)ii(C) Emergency Mode Operation Plan	ISO does not specifically address security for contingency operations
6	Physical:(a)(2)(i) Contingency Operations	ISO does not specifically address physical security for contingency operations

7	Physical:(a)(2)(ii) Facility Security Plan	Documentation not required by ISO
8	Physical:(a)(2)(iv) Maintenance Records	Documentation not required by ISO
9	Physical:(a)(2)(iv) Data Backup and storage	ISO does not specifically require data back-up before moving storage units
10	Technical:(a)(2)(i) Unique User Identification	ISO allows group user ids in some cases. Does not address entity authentication
11	Technical:(a)(2)(ii) Emergency Access Procedure	ISO does not specifically address access controls for contingency operations

Borkin, S. 2003. As part of Information Security reading room. SANS Institute 2003

Table 2: Requirements of SANHA not fully present in ISO17799

	SANHA requirement	Explanation
1	Access to health records by a health worker or healthcare provider, duty and procedures to disseminate information by National health department	Unique requirement of the SANHA legislation
2	Disclosure of health information only if the user provides consent in writing, a court order or any law requires that disclosure, non-disclosure of the information represents a serious threat to public health.	Unique requirement of the SANHA legislation

Table 3: Requirements of ECTA not fully present in ISO17799

	ECTA requirement	Explanation
1	Admissibility and evidential weight of data messages, Retention, Notarization, Acknowledgement and Certification of data messages	Not specifically covered by ISO
2	Registration of cryptography providers	ISO does not specifically require registering cryptography providers
3	Accreditation, criteria of accreditation of authentication products and services	Unique requirement of the ECTA legislation
4	Identification, Registration, and Inspection of critical	Not specifically covered by ISO

	databases	
5	Liability of Service Providers: Hosting, Caching, Mere conduit, Information Location tool	Unique requirement of the ECTA legislation
6	Appointment of Cyber Inspector and their power to inspect, search, seize, and obtaining warrant	Unique requirement of the ECTA legislation

The results of the comparison are now further analysed and summarised in Figure 1.

ISO and HIPAA: The HIPAA security standards meet the ISO 17799 controls for 20 (or 56 %) of the implementation requirements (quantified as ISO subsections). While HIPAA is only about the protection of one kind of information namely "health information", ISO 17799 is for the protection of all types of information. The HIPAA security standard includes 1 (or 3 %) control requirement for which it has a more stringent requirement than ISO. Table 1 details this requirement and provides more information about various other HIPAA control measures that are not included in the ISO.

SANHA and ISO: The ISO 17799 controls exceed the SANHA in 35 (or 97 %) of the implementation requirements. In fact, these controls are not covered in SANHA at all. SANHA contains 1 (or 3 %) control requirement that exceeds the corresponding requirement in the ISO. This is detailed in Table 2 together with a list of requirements included in SANHA that are not included in ISO at all These results come without any surprise as the two have different objectives and coverage scope. The scope of ISO 17799 states: "This standard gives recommendations for Information Security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings" (ISO 17799); whereas the main objective of SANHA is to provide a framework for a structured, uniform health systems in order to unite the various elements of the national health system in a common goal to improve universal access to quality health services (SANHA).

It emerges clearly from the comparison that health organizations that are ISO-compliant will exceed requirements pertaining to security and privacy as detailed in SANHA, by far. A small effort will be required to ensure compliance with the issues listed in Table 2.

ECTA and ISO: The ISO controls meet the ECTA for 1 (or 3 %) and exceed 31 (or 86 %) of the implementation requirements. While the ISO specifies controls that should be in place to ensure organization information assets' security, the main focus of ECTA is to provide a framework for the facilitation and regulation of electronic communications and transactions. This is an over-arching difference in focus between the two. ECTA contains 4 (or 11 %) control requirements that exceed the requirements of the particular ISO subsection. Further requirements of the ECTA that are not covered in the ISO are expanded on in Table 3. The reason for this is because the ECTA puts more focus specifically on E-commerce issues including the validity

of electronically concluded agreements, the legal validity of electronic data, the admissibility of electronic documents in courts of law and the legal status given to electronic signatures which are not specifically covered in detail in ISO 17799.

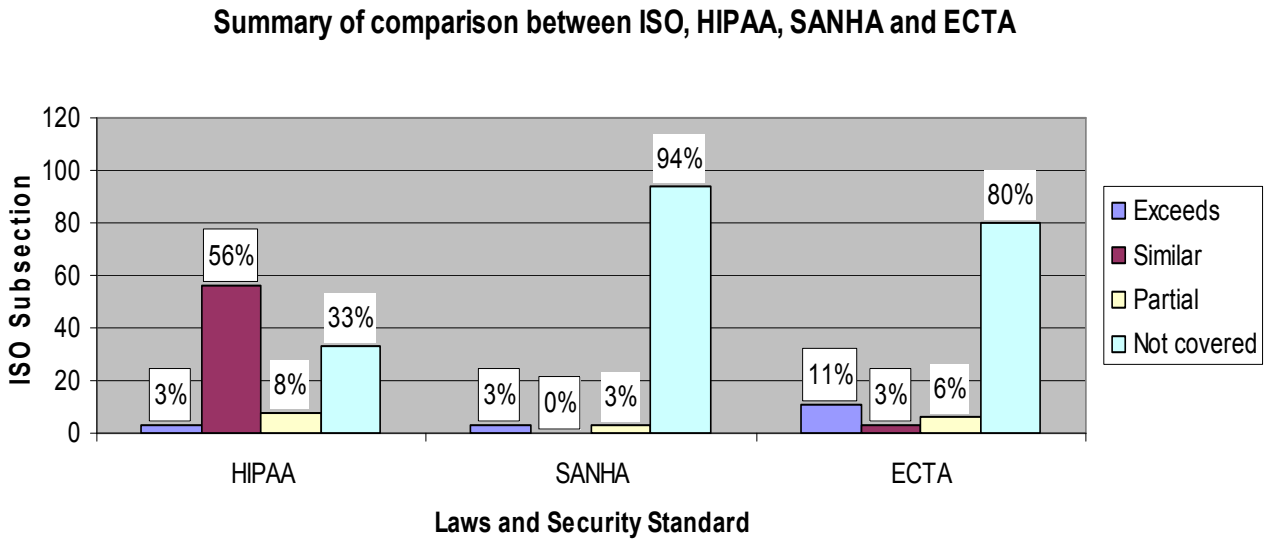


Figure1: Summary of the comparative analysis

From the comparison, it can be generalized that some legislation can certainly have quite an overlap with an Information Security management program, such as in this case the ISO and HIPAA. This confirms that a compliance strategy would serve well to eradicate redundancy in following an ad hoc approach to compliance with various standards and legislations.

7. PROPOSED COMPLIANCE STRATEGY

The challenge encountered by healthcare organizations is which compliance strategy to use to meet regulatory requirements while providing customers with the assurance of meeting international standards for information security?

In answering the above question, the strategy outlined in steps 1-5 is proposed:

1. Identify the scope of the compliance strategy. This must include the identification of an Information Security management framework (eg ISO 17799) as well as the regulations that should be complied with (eg HIPAA, SANHA, ECTA).
2. Determine the implementation requirements of the Information Security management (ISM) framework. For example, the ISO operates using security controls, which are extrapolated from organizational security requirements.
3. Identify a unit in each of the regulations, which could be used as a point of reference for comparison with the Information Security management framework. For example, the 42 HIPAA security standards implementation requirements would be on a level comparable to the ISO security controls. If such a unit, which facilitates a comparative analysis is not evident from the

particular regulation, it is envisaged that such a unit should be defined – it would require further research to substantiate this statement.

4. Use the implementation requirements of the ISM framework identified in step 2 as a basis to work from. This provides a single point of reference from which to collate all the relevant security controls (using the ISO terminology). For each legislation, add the necessary controls that are not covered in the ISM framework. This should be done sequentially (ie finish one legislation before starting with the next) to facilitate an incremental comparison. Comparing each legislation with the ISM framework could lead to redundancy in controls, which might be covered in more than one legislation.
5. Develop a compliance maintenance and review process that facilitates this collated approach. This would obviate redundancy in executing maintenance and review procedures designed to review the specific ISM framework and/or legislations in isolation.

This compliance strategy will ensure that common elements across regulations and those that are already covered in an Information Security management program, will not be repeated unnecessarily. In addition, it is proposed that a compliance approach should use a proper Information Security management framework as basis to work from. In the health sector this is particularly important in terms of the security and privacy of health information. The use of an internationally accepted standard such as the ISO will further enhance the desired level of security.

8. CONCLUSION

Managing Information Security in information systems has reached the point where sufficient, but dispersed knowledge exists in various domains (Denis, 2003). Some of the areas supporting the Information Security program may be required by law or regulations whereas others may be considered as best practices.

Compliance with SANHA and ECTA is a regulatory requirement for South African health care organization and ignorance of the law requirement is not an excuse. Ignorance of legal requirements can result in heavy punishment and loss of an organization's credibility. Also, South African Healthcare organizations' managers should keep in mind that being compliant with all legal requirements does not guarantee privacy and security protection of health information (and vice versa). In addition to meeting the regulatory requirements, they should also adopt international security standards as part of Information Security management in order to ensure that best practices are in use. Using this statement as a premise of this research, it is proposed that a compliance strategy should use an Information Security management framework as a point of reference to collate further requirements posed by regulations. This can help to reduce the security and privacy risks to a minimum level, while minimizing redundancy in the approach to complying with relevant legislations.

9. REFERENCES

Bassett, 2003. *Healthcare in South Africa* [online]. Available on the internet: http://www.medhunters.com/articles/healthcareInSouthAfrica.html (Sited 20 March 2005)

Borkin, S. 2003. *The HIPAA Final Security Standards and ISO/IEC 17799*. SANS Institute 2003 [online]. Available on the internet: http://www.sans.org/rr/whitepapers/standards/1193.php (Sited 10 March 2005).

Computer-based Patient Records Institute (CPRI) Toolkit, 1995. *Managing Information Security in Heath Care* [online]. Available on the internet: http://www.himss.org/CPRIToolkit/html/3.6.html (Sited 10 March 2005).

ISO17799 SOUTH AFRICAN STANDARD, 2000, *SABS ISO/IEC 17799, Information Technology - Code of practice for Information Security management.* SABS edition 1/ISO/IEC edition 2000. Pretoria: South African Bureau of Standards.

Centers for Medicare & Medicaid Services (CMMS), 1996. *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)* [online]. Available on the internet: http://www.cms.hhs.gov/hipaa (Sited 01 April 2005).

Denis, T. 2003. *An integral framework for information systems security management*. Computers & Security, Elsevier Science. Vol 22 (4), pp. 337-360.

Electronic Communication Transaction Act (ECTA) (25 0f 2002). Vol.446 Government Gazette, Cape Town 02 August 2002.

Electronic Privacy Information Center (EPIC) and Privacy International. Privacy and Human Rights Report (2002). '*An International Survey of Privacy Laws and Developments,' United States of America* [online]. Available on the internet: http://www.privacyinternational.org (Sited 20 February 2005).

EthicSA, 2000. *Chris Hani Baragwanath Hospital Ethics Audit* [online]. Available on the internet: http://www.ethicsa.org/article.php?story=20030919084251975 (Sited 14 February 2005).

Health Human Services, 2003. *Administrative Simplification in the Health Sector* [online]. Available on the internet: http://aspe.os.dhhs.gov/admnsimp/index.shtml (Sited 28 February 2005).

Meyer, S. 2001. *What is means for Privacy and Security* [online]. Available on the Internet: http://www.giac.org/certified_professionals/practicals/gsec/0609.php

South African National Health Act (SANHA) (61 of 2003). Vol.469. Government Gazette, Cape Town 23 Jully 2004.

National Research Council. *For The Record: Protecting Electronic Health Information*. Washington, D.C.: National Academy Press, 1997 [online]. Available on the Internet: http://books.nap.edu/catalog/5595.html

Powe, L. CSC Press Releases: *Technology could ease stress of nursing shortage* [online]. Available on the Internet: http://za.country.csc.com/en/ne/pr/680.shtml (Sited 20 February 2005).

Roemer, M. 1991. *Conceptual framework for the assessment of the performance of the Brazilian Health System*. [online]. Available on the Internet:

http://www.cahspr.ca/conference04/proceedings/Viacavareport.pdf (Sited 20 February 2005).

Safrica.info, 2003. *Healthcare in South Africa* [online]. Available on the internet at: http://www.southafrica.info/ess_info/sa_glance/health/health.htm (Sited 10 March 2005).

SITA Mandate. 1998 [online]. Available on the Internet: http://www.sita.co.za. Sited (2 March 2005).

Smith, C.2004. SANS Institute- GIAC Security Essentials Certification (GSEC) *Cross Walking Security requirements* [online]. Available on the internet:

http://www.sans.org/rr/whitepapers/country/1463.php (Sited 14 March 2005).

Zhang, L., Ahn, G, Chu.B (2002). *A Role-Based Delegation Framework for Healthcare Information Systems*. Proceedings of the seventh ACM symposium on Access control models and Technology (SACMAT), pages 153-162. Chantilly, VA, May 3-4, 2001.