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 cost 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 while 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 INTRODUCTON

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 al, 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 meets regulatory requirements and 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 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 for middle- and high-income earners who tend to be members of medical schemes (18% of the population), and for 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 realized 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 given rise 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 or her wishes. Security refers to 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):

- 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 message content, information derived from observing message flow, and information held in storage on an open system to an unauthorized user.
- Repudiation, in which a user or system denies having performed some action, such as modification of information.
- Denial of service – this prevents the system 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 physician's duty to respect the patient's 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 (National Research Council, 1997). 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 an 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 is 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 worth 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 the way in which the information would be secured and safeguarded (CMMS, 1996). The portion of the HIPAA law that has the most impact on 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 promulgated 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 (SANHA). In briefing media on the SANHA 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. 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.

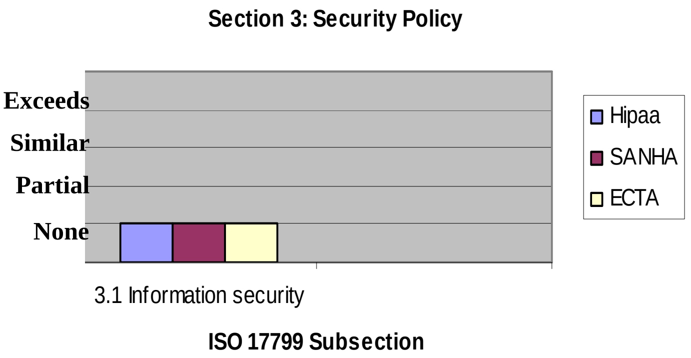
The Electronic Communication and Transaction Act (ECTA), or Act No.25 of 2002 was promulgated into Act by the South African president on 31 July 2002. Being the first South African law governing cyber activity, the Act facilitates the development and propagation of electronic communications and transactions 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.

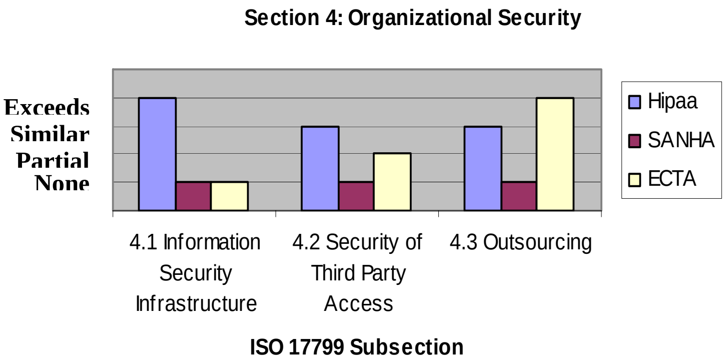
Currently there are a growing number of regulations that include requirements for healthcare organizations to provide security controls and demonstrate compliance assurance. The challenge encountered by most healthcare organizations is what compliance strategy should be followed to meet regulatory requirements while ensuring that the existing efforts already implemented are maintained. Therefore, a comparative analysis of compliance requirements is required, which in this paper is focused 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.

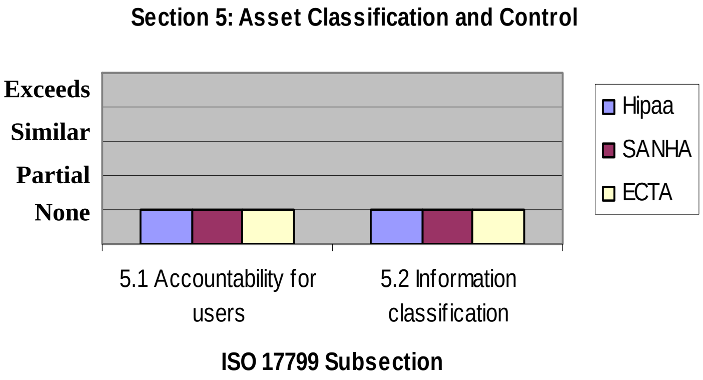
5 COMPARISON BETWEEN ISO 17799, HIPAA SECURITY STANDARDS, SANHA AND ECTA LAWS

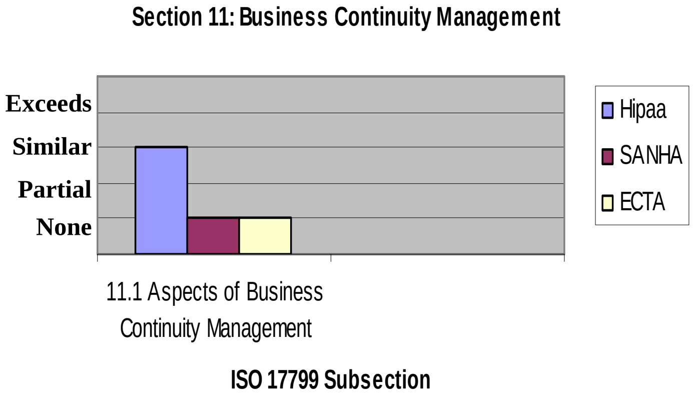
Following is a comparison of each of the ten ISO 17799 controls against SANHA, ECTA and HIPAA security standards. The ISO 17799 will be used as a basis for this comparison. For reasons of simplicity, the HIPAA security standard is often referred to as just "HIPAA" and the ISO/IEC 17799 International Standard is often referred to as just "ISO".

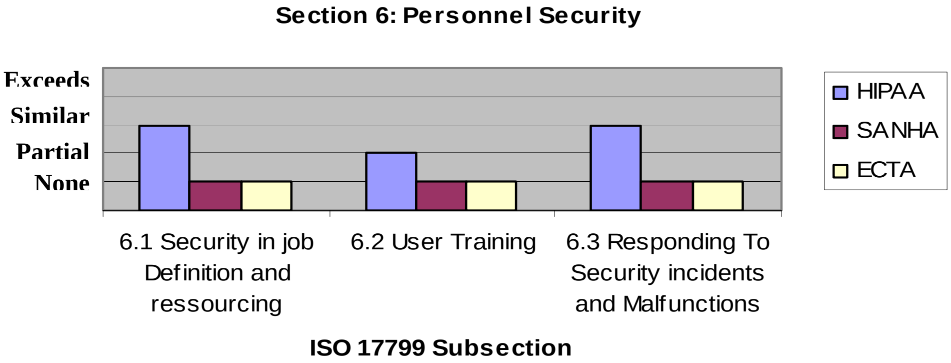
A graphic representation is used which depicts the particular ISO subsection as relating to its coverage in HIPAA, SANHA and the ECTA. Each graph will show to which extent the ISO subsection is covered by the regulation. This can either be not at all (none), partially, similar coverage (similar) or the 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 and goes beyond the scope of this paper.

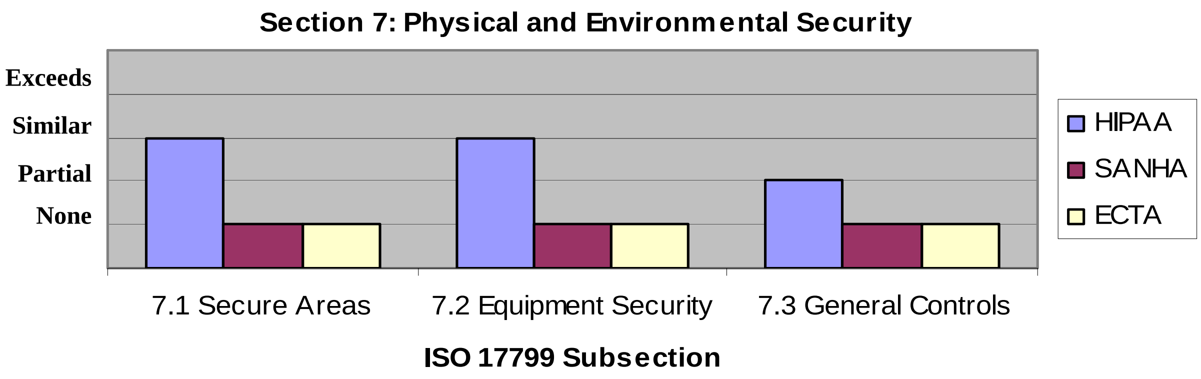


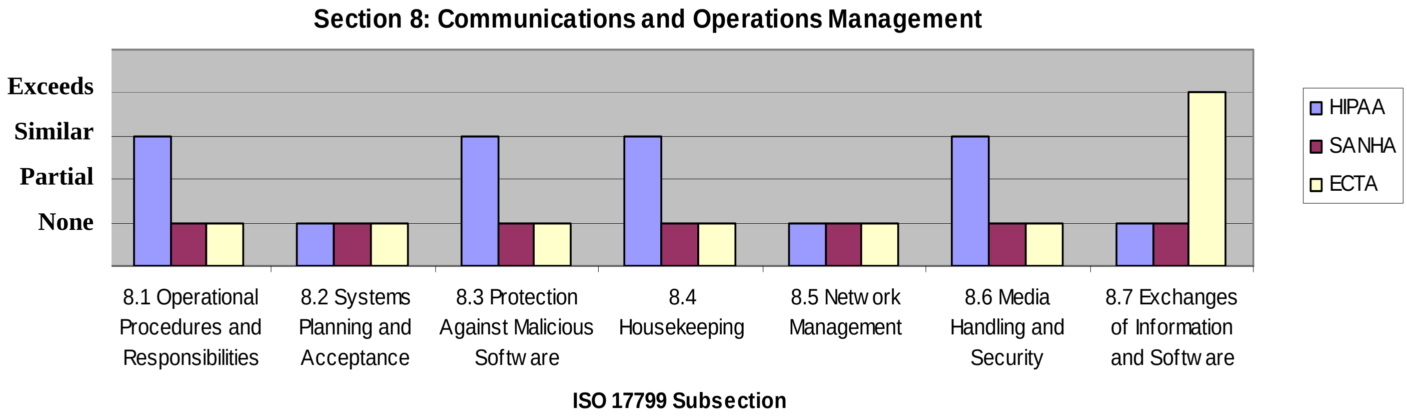


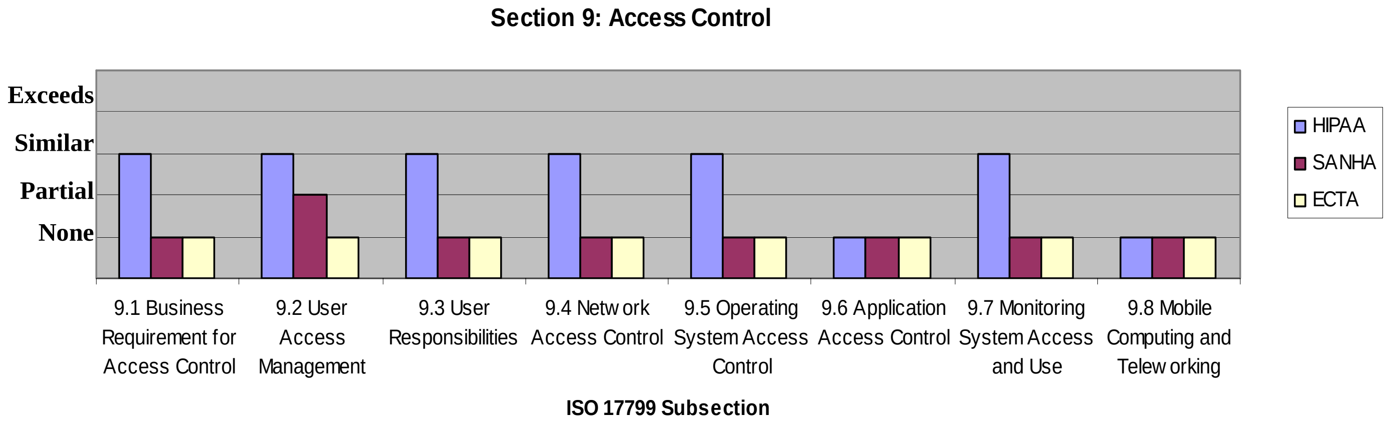


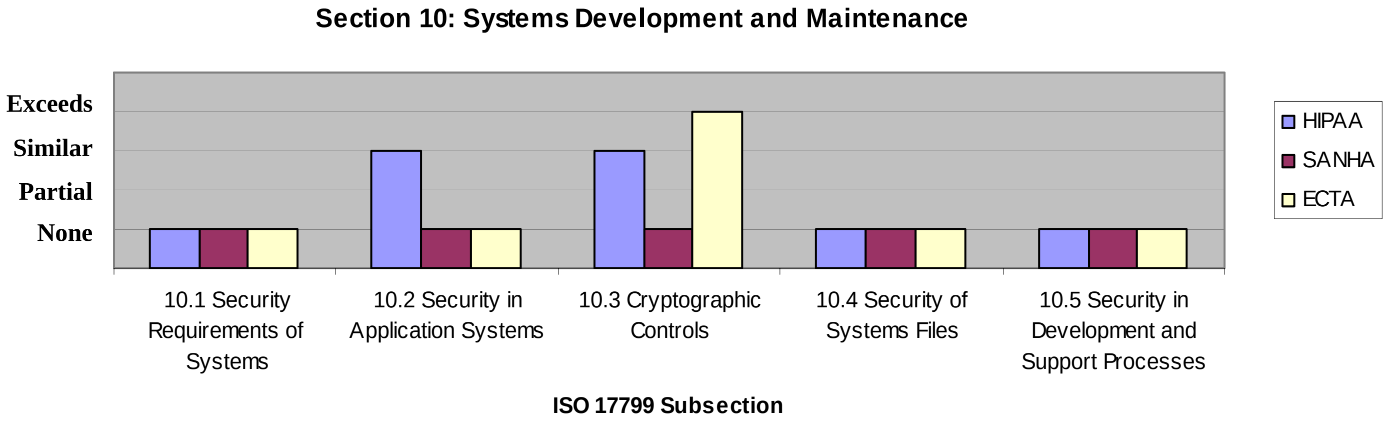


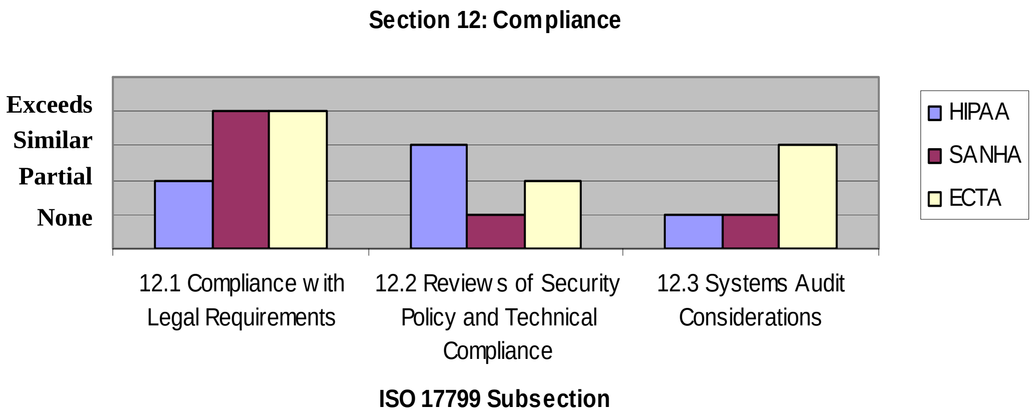



Section 7: Physical and Environmental Security
Exceeds
Similar
Partial
None
7.1 Secure Areas
7.2 Equipment Security
7.3 General Controls
ISO 17799 Subsection
HIPAA
SANHA
ECTA


Section 8: Communications and Operations Management
Exceeds
Similar
Partial
None
8.1 Operational Procedures and Responsibilities
8.2 Systems Planning and Acceptance
8.3 Protection Against Malicious Software
8.4 Housekeeping
8.5 Network Management
8.6 Media Handling and Security
8.7 Exchanges of Information and Software
ISO 17799 Subsection
HIPAA
SANHA
ECTA


Section 9: Access Control
Exceeds
Similar
Partial
None
9.1 Business Requirement for Access Control
9.2 User Access Management
9.3 User Responsibilities
9.4 Network 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 Teleworking
ISO 17799 Subsection
HIPAA
SANHA
ECTA


Section 10: Systems Development and Maintenance
Exceeds
Similar
Partial
None
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
HIPAA
SANHA
ECTA



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 databases	Not specifically covered by ISO
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 concerned with the protection of one kind of information namely “health information”, ISO 17799 is concerned with 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 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 (SANHA).

It emerges clearly from the comparison that healthcare 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 that ECTA puts more emphasis 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.

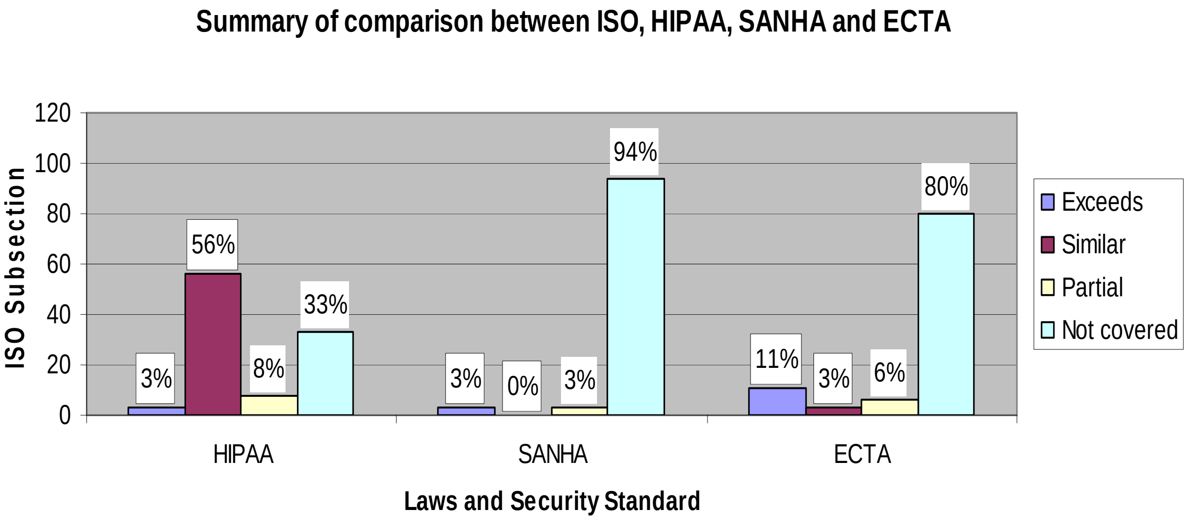


Figure1: Summary of the comparative analysis

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 of 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 organizations 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 for 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: *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.