A Framework for Secure Mobile Computing in Healthcare

Godwin D. A. Thomas

A Framework for Secure Mobile Computing in Healthcare

by

Godwin D. A. Thomas

Submitted in fulfilment
of the requirements
for the degree

Magister Technologiae

in

Information Technology

in the

School of Information and Communication Technology

in the

Faculty of Engineering, the Built Environment and Information Technology

of the

Nelson Mandela Metropolitan University

Supervisor: Prof. Reinhardt A. Botha

January 2007

DECLARATION

I, **Godwin D. A. Thomas** 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.

Godwin D.A. Thomas
12 January 2007

ABSTRACT

Mobile computing is rapidly becoming part of healthcare's electronic landscape, helping to provide better quality of care and reduced cost. While the technology provides numerous advantages to the healthcare industry, it is not without risk. The size and portable nature of mobile computing devices present a highly vulnerable environment, which threaten the privacy and security of health information. Since these devices continually access possibly sensitive healthcare information, it is imperative that these devices are considered for security in order to meet regulatory compliance.

In fact, the increase in government and industry regulation to ensure the privacy and security of health information, makes mobile security no longer just desirable, but mandatory. In addition, as healthcare becomes more aware of the need to reinforce patient confidence to gain competitive advantage, it makes mobile security desirable.

Several guidelines regarding security best practices exist. Healthcare institutions are thus faced with matching the guidelines offered by best practices, with the legal and regulatory requirements. While this is a valuable question in general, this research focuses on the aspect of considering this question when considering the introduction of mobile computing into the healthcare environment.

As a result, this research proposes a framework that will aid IT administrators in healthcare to ensure that privacy and security of health information is extended to mobile devices. The research uses a comparison between the best practices in ISO 17799:2005 and the regulatory requirements stipulated in HIPAA to provide a baseline for the mobile computing security model. The comparison ensures that the model meets healthcare specific industry requirement and international information security standard. In addition, the framework engages the Information Security Management System (ISMS) model based on the ISO 27000 standard. The framework, furthermore, points to existing technical security measurers associated with mobile computing.

It is believed that the framework can assist in achieving mobile computing security that is compliant with the requirements in the healthcare industry.

ACKNOWLEDGEMENT

My sincerest gratitude goes to

- Our Heavenly father who created me;
- My Promoter, Professor Reinhardt Botha, for his guidance, patience, support and supervision.
- Mrs Adele Botha and Bron Koplan for their proof reading effort, thank you.
- My Parents, for their love and motivation
- Nelson Mandela Metropolitan University, whose financial support made this research possible.
- My friends and colleagues, for their support and understanding. I thank you all.

CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AMPS	Advanced Mobile Phone System
CDMA	Code Division Multiple Access
CERT	Computer Emergency Response Team
CHAP	Challenge-Handshake Authentication Protocol
COBIT	Control Objectives for Information and Related Technology
CoE	Council for Europe
CPRI	Computer-based Patient Records Institute
DSS	Digital Signature Standard
DSA	Digital Signature Algorithm
DICOM	Digital Imaging and Communications in Medicine
ECTA	Electronic Communication and Transaction Act
EKG/ECG	Electrocardiogram
ESN	Electronic Serial Number
ECMA	European Computer Manufacturing Association
EAP	Extensible Authentication Protocol
GMITS	Guidelines for the Management of Information Technology Security
GPRS	General Packet Radio Service
GPS	Global positioning system
GSM	Global System for Mobile Communications
HIPAA	Health Insurance Portability and Accountability Act
HSCSD	High Speed Circuit Switched Data
HSN	Hardware Serial Number
HL7	Health Level 7
IEEE	Institute of Electrical and Electronic Engineers

IETF	Internet Engineering Task Force
IEC	International Electrotechnical Commission
IP	Internet Protocol
IPSec	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
L2TP	Layer 2 Tunneling Protocol
LEAP	Lightweight Extensible Authentication Protocol
MS-CHAP	Microsoft Challenge-Handshake Authentication Protocol
NIST	National Institute Standards and Technology
NRC	National Research Council
OECD	Organization for Economic Cooperation and Development
PAN	Personal Area Network
PAP	Password Authentication Protocol
PCDA	Plan, Check, Do, Act
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point to Point Tunneling Protocol
PSTN	Public Switched Telephone Network
RADIUS	Remote Authentication Dial-In User Server/Service
SANHA	South African National Health Act
SDR	Software Defined Radio
SIM	Subscriber Identity Module

SSID	Service Set Identifier
SSL	Secure Socket Layer
SSH	Secure Socket Shell
SoA	Statement of Applicability
TACS	Total Access Communication System
TACACS	Terminal Access Controller Access Control System
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UDDI	Universal Description, Discovery and Integration
UMTS	Universal Mobile Telecommunication System
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access
WCDMA	Wideband Code Division Multiple Access
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WWAN	Wireless Wide Area Network

Chapter 1.
Introduction

Mobile computing devices, such as notebooks, have become an indispensable part of modern business (Kakihara & Sørensen, 2006). With a simple connection to the network, employees stay in touch and are more productive outside the office. The introduction of smaller, wireless-ready handheld computers, PDAs and smart phones has further fuelled the interest in mobility (Fontelo & Chismas, 2005; GAO, 2005; Forman & Zarhojan, 1994). As this is true in many industries, it is also true in the healthcare industry. The drive comes from the desire to provide better healthcare service quality for patients; therefore, mobile computing has become a common place in healthcare (Finch, 1999; Wales, 2003).

The healthcare industry, initially considered lagging in Information Technology adoption, has witnessed a tremendous growth in the adoption of certain mobile computing devices (Havenstein, 2005). Mobile computing provides great benefits to the industry. These include improved data collection and timely access to the latest information to interested parties. Since this is now possible within and outside an institution, it could lead to productivity improvement and cost savings (Meridian, 2006). However, the portable nature of these mobile computing devices that make them so attractive is not without risk. As healthcare providers increasingly move toward mobile computing, demands for scalability, reliable access and security become prominent (Satyanarayanan, 1996; Herrera, 2006).

Today, mobile devices come with wireless-ready and built-in support for Wireless Local Area Networks (WLANs), Bluetooth and Wireless Wide Area Networks (WWAN) (Karygiannis & Owens, 2002). The capability of these access technologies provides easy access to medical information anywhere and anytime. However, with the ease of access comes great responsibility (Crounse, 2006). Crumbley (2003) stated that as valuable as mobile devices are to caregivers, they function in an extremely vulnerable environment, and pose new threats to the privacy and security of health information.

While protection is desirable (for economic reasons) to reinforce customer confidence and trust, regulatory implications makes it mandatory (Grove, 2003)

Prompted by these economic and regulatory pressures, hospitals and healthcare providers want new solutions that can address core business needs and manage the huge volumes of time and security-sensitive data that are involved (Portale, 2002).

This research proposes a framework model that will aid IT administrators in healthcare to guarantee the privacy and security of health information extended to mobile devices, while at the same time, taking full advantage of mobile computing benefits. The framework will encapsulate administrative, operational, technical and physical requisites aligned with health regulatory requirements. The framework will aim to take full cognisance of regulatory compliance, implement information security best practice, to build customer confidence and trust while meeting international standards.

1.1 Background

At a time when economic conditions are severe, identifying ways to increase productivity, decrease operational costs, improve revenue generating processes, and increase customer satisfaction provide a strong justification for technology investments (Dedo, 2004). Today, we are witnessing the dawn of the mobile and wireless technology era, influencing modern businesses and organizations. Although mobile devices, such as mobile phones and personal digital assistants (PDAs), were first developed as end-user products, a number of firms are adopting these technologies for innovative business applications (Kakihara & Sørensen, 2006).

The demand for mobility, illustrated by the fast adoption of devices by society, is a result of the features, abilities and convenience the devices possess. According to Dedo (2004), these features, along with business applications, are becoming available in converged devices. For instance, PDAs are coming with integrated cell phone features and cell phones (Lehrbaum, 2000; Linhoff, 2002; Wales, 2003).

Mobile computing provides great promise to organizations that adopt mobility to gain a competitive advantage, as well as users that demand anytime, anywhere computing capabilities (Gold, 2005). This is achieved by enhancing the utility of the portable computing device to improve customer service, speed up decision making and attract and maintain a high-quality workforce (Caldwell

& Koch, 1998; Nokia, 2005).

An IDC (International Data Corporation) projection in 2000 showed that mobile computing in the US will grow steadily at a compound annual rate of 9%, with remote access increasing from 39 million in 2000 to 55 million in 2004. Furthermore, in another IDC research report, Drake and Olofson (2005) projected that in the US alone, a number of mobile workers will reach 104.5 million in 2006. This will represent almost two thirds of the total workforce population. Likewise, the mobile-worker population in Western Europe is expected to reach 94.8 million in 2006, representing about 55% of the total workforce.

While there is a fast rate of adopting mobile computing in many industries, it is no different in the healthcare industry. Today, the healthcare industry is as competitive and complicated as any other industry and depends on the right technology to succeed (Newcombe, 2003). The desire to provide better healthcare service quality for patients, the shortage of caregivers throughout the world and tight margins have aided in giving thrust to the adoption of handheld and mobile technology in healthcare (Meridian, 2006; Sorensen, Naess, Strand, Wang, & Conradi, 2003).

Drake and Olofson (2005) show that one of the key applications driving the adoption of mobility is vertical-oriented application. The vertical application mentioned includes the health patient record and process manufacturing applications.

The healthcare industry, traditionally, has lagged considerably behind in the adoption of technology (Linhoff, 2002). However, it was only a matter of time before the leaders and decision makers in the industry began to realize the supporting role technology can play in their effort to maintain focus on quality care. Technology can aid in reducing costs through increased operational efficiencies, while meeting the pressures from regulatory bodies and a competitive environment (Finch, 1999; Keay, 2004).

According to Havenstein (2005), a 2004 study of wireless adoption in various vertical industries by the market research firm, IDC, found that more than 80% of 34 healthcare organizations polled said they have deployed wireless LANs or plan to deploy them in the next 12 months. A 2005 Healthcare Information and

Management Systems Society Leadership Survey (Havenstein, 2005), which was published in February, showed that 79% of 253 healthcare executives responding to an online questionnaire said they will use wireless information systems this year, while 54% said they will use handheld devices.

Although wireless networking greatly enhances the utility of mobile devices, it does not come without risks. In many ways the security concerns are similar to a wired infrastructure (Karygiannis & Owens, 2002; GAO, 2005). We are, for example, still concerned with protecting data, authenticating users and shielding against viruses. Unfortunately, mobile devices function in an extremely vulnerable environment. The portable nature of these devices presents additional security challenges.

According to Karygiannis & Owens (2002), Luo (2004), Light (2004), and Wang (2005), the following security challenges are associated with mobile devices:

- **Over the Air Attack**: The wireless capability of mobile devices is particularly susceptible to data interception or intrusion as transmission is done over the air.

- **Viruses and Malicious Code**: As mobile devices are directly under the control of the users, they are vulnerable to virus and malicious code attack. Mobile devices can create an easy route for virus and malicious code into a protected network.

- **Theft and Loss:** The small size and portability of mobile devices make them susceptible to loss and theft. In the absence of any security provision, any sensitive information on the device can be easily accessed or copied

- **Human Factor:** Users further compound the security challenges by not following safe computing procedures; hence, posing new threats to the privacy and security of confidential health information.

When an organization’s wireless and mobile network is compromised, financial losses and regulatory repercussion can be the result. It is imperative that the healthcare industry monitors all wireless activities and ensures that proper security measures are put in place and security policies strictly enforced (Cisco, 2006).

As healthcare providers and patients become increasingly aware of the need for data security to reinforce confidence and trust, the challenges associated with security are greater than ever (Crounse, 2006; Borzo, 2005). The development of electronic medical records and linking of clinical databases has increased concern about the privacy and security of health information (National Research Council, 1997). The increase in government regulations in different countries enforces protection of confidentiality, integrity and availability of patient information (Wales, 2003; Nealon & Moreno, 2002). Examples of government acts in different countries are: the Health Insurance Portability and Accountability ACT (HIPAA) of the United States and the South African National Health Act (SANHA) in South Africa.

To address these needs, it is imperative that healthcare organizations adopt sound security measures to ensure that healthcare information is adequately protected to meet information security standards, as well as to fully comply with regulatory compliance requirements while gaining a competitive advantage.

1.2 Key Concepts

This section describes the key concept that will feature in this research, for better understanding of the research. The following sub-section describes these important concepts.

1.2.1 Privacy

Privacy on its own is about protecting users' personal information (Nixon, Wagealla, English, & Terzis, 2005), it is the right to be left alone. This means that personal information should not be divulged or used by others against the user's wishes, thus unless authorized by the user (Uday & Pabrai, 2003; Tuykeze & Pottas, 2005). Privacy can be classified in terms of an individual or a group of individuals. Dobson et al. (1995), Allen (1995), and Moskop et al., (2005), distinguish three major usages of the term privacy: "**Physical privacy**", "**Decisional privacy**" and "**Information 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 healthcare. As patients grant their caregivers access to their bodies for medical examination and treatment, they expect caregivers to protect them from any unnecessary or embarrassing bodily contact or exposure.

- **Decisional privacy** refers to an ability to make and act on the personal choices of an individual without interference from others or the state. For instance, in the United States, the Supreme Court relies on a constitutional right to privacy to protect freedom of choice about contraception and abortion.

- **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 the information will be carefully restricted.

This project deals with Information privacy. The processing of an individual's information may occur without his/her knowledge and even without his/she being able to control what is stored, processed, sold or distributed. This act questions the right of the individual to protect his/her personal privacy. The right of a person to privacy entails that such person should have control over his/her personal information and should be able to conduct his/her personal information affairs relatively free from unwanted intrusions (Neethling & Potgieter, 1996). This is not easy with the expansion in the use of IT that enables such information to be available to various business partners anywhere and anytime.

According to Meyer (2001) and KPMG (2001) security and privacy are related but distinct. It is possible to secure health information without making it private; however, it is not possible to protect privacy without having security (KPMG, 2001). Privacy protection includes restrictions of a legal nature to the collection, handling, storage or transmission of personally identifiable or aggregate data collected from individual users. It means the ability to share an individual's personal and health information in confidence. Confidentiality is the controlled release of such information to a care provider under the agreement in which the information will be used or released further (Rindfleisch, 1997).

An organization employs security measures to protect the confidentiality of patient information. These measures control access and protect information from accidental disclosure to unauthorized persons and from alteration, destruction or loss (Ciampa 2004, p. 5).

In summary, the privacy of an individual's health information depends on the level of confidentiality maintained by organizations, which in turn depends on the security measures implemented by them. The next section elaborates more on the concept of security, with regard to healthcare.

1.2.2 Security

The security of medical information is a matter of great importance. As medical records contain sensitive information about users, access to the information must be controlled. In the event of unauthorized disclosure, it may cause a social embarrassment or prejudice, affect insurability as well as limit a user's ability to get a job (Rindfleisch, 1997). Without confidence in medical privacy, patients are likely to withhold important information that may be required for their care. Hence, it is imperative that medical information is protected.

According to Ciampa (2004, p. 5), as well as Whitman and Mattord (2003, pp. 9 – 10), in order to achieve security, healthcare organizations have to ensure that the three key characteristics of information, namely confidentiality, integrity and availability are preserved. In addition, authenticity and non-repudiation should also be preserved, as they are essential properties in the context of healthcare's transactional activities (HIPAA Consortium, n.d.). These characteristics are portrayed in a healthcare context as follows:

- **Confidentiality:** Information about a patient is given with the understanding that it will not be disclosed to others outside the patient's care, without the patient's consent (Stanberry, 2000). In healthcare interactions, patients communicate sensitive personal information to the caregivers ensuring that they understand the medical conditions in order to 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 unauthorized person or inadvertently by discussing patient information in a way that an unauthorized person can overhear it.

- **Integrity:** Information integrity plays an important role, particularly in a healthcare environment because having integrity guides medical staff members in the decision making process (Ritchie & Brindley, 2001). Information should not be accidentally or maliciously altered or destroyed. If 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.

- **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. Ensuring the availability of information is extremely important because without timely information a healthcare organization would be incapable of continuing normal operations (Gerber & von Solms, 2001).

- **Authenticity**: Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication (Whitman & Mattord, 2003, p. 11). Authentication validates the identity of caregivers partners and the origin of data or information. It is imperative that users and devices be properly authenticated before any medical transactions or processes are performed. When conducting electronic transactions, users need to know that electronic communications are from the source identified and that their contents have not been changed. The fabrication of data can lead to wrong patient medication or possible medical insurance claims.

- **Non-repudiation:** Non-repudiation provides proof of data transmission or receipt so that the occurrence of an operation cannot later be denied (Microsoft 2005; Elbaz, 2002). Non-repuditaion in healthcare will validate the origin and contents of notes, orders and other critical transactions. It establishes an irrefutable trail that transactions were performed (Ciampa, 2004, p. 274). A medication prescription can be sent by a doctor to a pharmacist, trusting him or her to provide medication as prescribed to a patient, or records can be sent to an insurer to justify payment for medical services rendered, this action should be irrefutable. For the development of health-information sources for consumers, validity and non-repudiation of health-related information should be ensured (Lampsas, Vidalis, Papanikolaou & Vagelatos, 2002). This typically means providing proof of the electronic equivalent of a signature.

The preservation of the confidentiality, integrity, availability, authenticity and non-repudiation 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. It is the violation of any of these components that quickly puts an organization at risks from a liability standpoint as well as their reputation.

1.3 Problem Statement

Using mobile and wireless devices in health care has advantages. It can give timely access to the latest information, improve data collection and speed up settlement, improve productivity and save cost. However, this does not come without risks.

On the one hand, the wireless and portable nature of these devices that make them so attractive, create an extremely vulnerable environment. This increases the risk of exposing confidential information, allowing network intrusion and importing infection inside the network. On the other hand, users compound the challenge by not following safe computing practices and misplacing devices, hence posing new threats to the privacy and security of health information.

While focusing on securing the wired network is a necessity for meeting regulatory compliance and gaining a competitive advantage, it is imperative to also take into account mobile devices that continually access and store sensitive information in order to fully meet compliance and information security best practices.

Therefore, this research deals with the question: “What should IT administrators in healthcare do to ensure the protection of sensitive information used on mobile devices?

The following objectives have to be achieved to answer the question.

1.4 Objectives

The primary objective of this research project is to develop a framework model that will address the security challenges mobile devices pose to healthcare organizations. This will be achieved by investigating existing health governing regulatory requirements and internationally acceptable information security management standards to serve as a base for the security compliance framework model. In this way, compliance with governing regulations can be ensured while providing 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:

- Analyze mobility, its influence on healthcare and how it affects the privacy and security of health information.
- Investigate the threats and vulnerabilities associated with mobile computing.
- Investigate existing security and management measures to ensure the privacy and security of health information.
- Investigate an information security management system, some existing health standard regulations and then identify a suitable standard to be used as a reference standard for a comparative analysis with a general information security management standard.
- Design a mobile security compliance framework based on the result of a comparative analysis, threats and vulnerabilities categories and existing security measures established on an existing Information security management system model.

1.5 Research Paradigm

According to Creswell (1994) and Groenewald (1999) a good research-undertaking starts with the selection of the topic, problem or area of interest, as well as the paradigm. A paradigm is a set of shared assumptions, concepts, practices or ways of thinking about some aspect of the world (Ash & Persall, 2002; Oates, 2006, p. 282). Oates (2006) stated that a wide variety of philosophical paradigms exist, arising from different ideas, views and perspectives of the world. This has brought about diverse ideas in the form of research questions and processes used to find solutions. The positivistic and the phenomenological paradigms, which focus on the natural and social worlds respectively, are discussed in this section.

The posivistic paradigm underlines what is called the "scientific method", i.e. the approach to research in natural science (Lee, 1999). Positivistic, or quantitative research, uses experimental methods and quantitative measures to test hypothetical generalizations (Hoepfl, 1997; Moody, 2002). The events are real, irrespective of an observer (researcher). In this case the researcher is neutral and objective; he/she is an impartial observer (Hoepfl, 1997; Orlikowski & Baroudi, 1991). While the posivistic research is well suited in studying aspects of natural sciences it is less suited for researching aspects of the social world (Oates, pp. 282 – 286, 2006). The phenomenological or qualitative research is well suited for this type of research (Oates, 2006, pp. 292 – 295; Orlikowski & Baroudi, 1991).

Phenomenological research is interpretative in nature. It does not try to prove or disprove a hypothesis as with posivistic research, but it tries to identify, explore and explain how all factors in a particular social setting are related and interdependent (Oates, 2006; Hoepfl, 1997; Thorne, 2000). The emphasis is more on the meaning of what is researched than on the measurement. It looks at how people perceive their world and try to understand phenomena through the meanings and values people assign to them.

According to Goede (2003), the development of an information system is viewed as a social activity combining social systems and technology to the benefit of the organization and society as a whole. The emphasis therefore is on social research. Although this study does not deal with the development of an information system per se, it deals with setting requirements for introducing a specific kind of information system, i.e. mobile application, into the healthcare domain. Therefore, it can be argued that the research conducted in this study is mainly phenomenological.

Phenomenological research is subjective. There is no observation that can be made independently of how the researcher chooses to conceptualize them on the basis of prior theory or previous experiences (Goede, 2003; Shaw, 2001). The researcher bears the burden of discovering and interpreting the importance of what is observed. In addition, using logical reasoning the researcher establishes a plausible connection between what is observed and the conclusions drawn in the research report (Hoepfl 1997).

Although phenomenological research does not engage in any statistical tests for significance, it does however, incorporate some posivistic methods such as surveys and some exploratory experiments to enrich the research. According to Shaw (2001) and Goede (2003), it is possible to use the two distinct research paradigms together. An interaction between the methodologies would enable more complete and therefore more effective research practice.

According to Shaw (2001) the invaluable knowledge provided by the positivistic paradigm has enhanced the level of sophistication of today's social research. Giddens (1978) provided an analogy to support this fact in his illustration of a physician using scientific knowledge to diagnose or determine the cause of social problems and to develop solutions. However, the choice of selecting research methods should depend upon the nature of research questions being posed (Oates, 2006, p. 304). It is therefore important for researchers to clarify what it is they want to discover about a particular phenomenon, i.e. the nature of the research questions, before making the decision about how it is to be revealed, i.e. what kind of data collection is required, and by what means of analysis the phenomenon is to be interpreted, i.e. what tools of analysis are to be adopted.

Since this research is predominantly phenomenological or interpretive oriented, the research methods chosen include literature studies, modeling and arguments. The use of these tools in this research is discussed in the next section.

1.6 Methodology

This section intends to answer the questions delineated in the section above, in an effort to meet the objectives stated in section 1.4. To begin with, the nature of the research question pertains to the healthcare industry in general. In order to help answer the question and meet the study objectives, an extensive

literature study was conducted. Since there was no particular physical access to any health provider or associate partner to use as a case study, the study was limited to only a literature study. Conscious and logical reasoning played an active role in this effort. The literature study analyzed mobility and established the current state of mobile computing and its influence in the healthcare environment.

Since the questions to be answered was general (at least in the sense of referring to a large business sector) the lack of case study work did not present problems for data collection. Journals, surveys, books and Internet sources were the predominant form of data collection used in this research. Such sources provided a broad base for understanding the domain of discourse. Logical reasoning played an important role in analyzing the validity of the data and interpreting and structuring the meanings that were derived from data to suit the research context. By finding patterns in the data sources and triangulating the different data sources, a quality point of convergence was ensured.

To ensure that both the general privacy and security requirements and the regulatory requirements of the healthcare environment were met, the analysis of the data used a comparison of controls identified by security best practices and requirements stipulated by healthcare regulations. This developed conceptualizations of the possible relations between the controls associated with the standard and regulation. Finally a well-known Information Security Management System was utilized to order and arrange the findings in a comprehendible and coherent whole.

1.7 Structure of the Dissertation

Chapter 1 serves as the introductory chapter which includes the background information, the problem statement, the objective of the dissertation and the research methodology. **Chapter 2** proceeds to look at the concept of mobility and how it relates to healthcare. The benefits of mobile computing in healthcare are discussed as well and the accompanying challenges with regards to the privacy and security of health information. **Chapter 3** moves on to identify the threats and vulnerabilities associated with mobile computing and how they impact on the privacy and security of health information. **Chapter 4** then investigates the technical countermeasures available to thwart the risks associated with the threats and vulnerabilities encountered in chapter 3 and the limitations associated with the measures.

Chapter 5 goes on to address the issue of how to manage and control the implementation of the mobile computing security countermeasures based on an Information Security Management System (ISMS) ISO/IEC 27001. The chapter moves on to provide an overview of the information security management framework and discusses some of the healthcare specific regulatory standards in some countries. Then finally, the chapter selects ISO 17799 and HIPAA as the comparison reference standards to be used as a baseline for mobile security in healthcare. **Chapter 6** is a comparative analysis of ISO/IEC 17799 and the Health Insurance Portability and Accountability Act (HIPAA) to find a baseline.

Chapter 7 puts together a compliance framework model for secure mobile computing in healthcare. The framework model is based on the ISO/IEC 27000 ISMS Plan Do and Act model, the result of the comparative analysis in chapter 6 along side the threat and vulnerabilities countermeasure discussed in chapter 4. Eventually, **Chapter 8** concludes the dissertation with a short summary of the work accomplished in the above-mentioned chapters. Issues, such as achievements and further research, are discussed briefly. Figure 1.1 graphically depicts the layout of the dissertation.

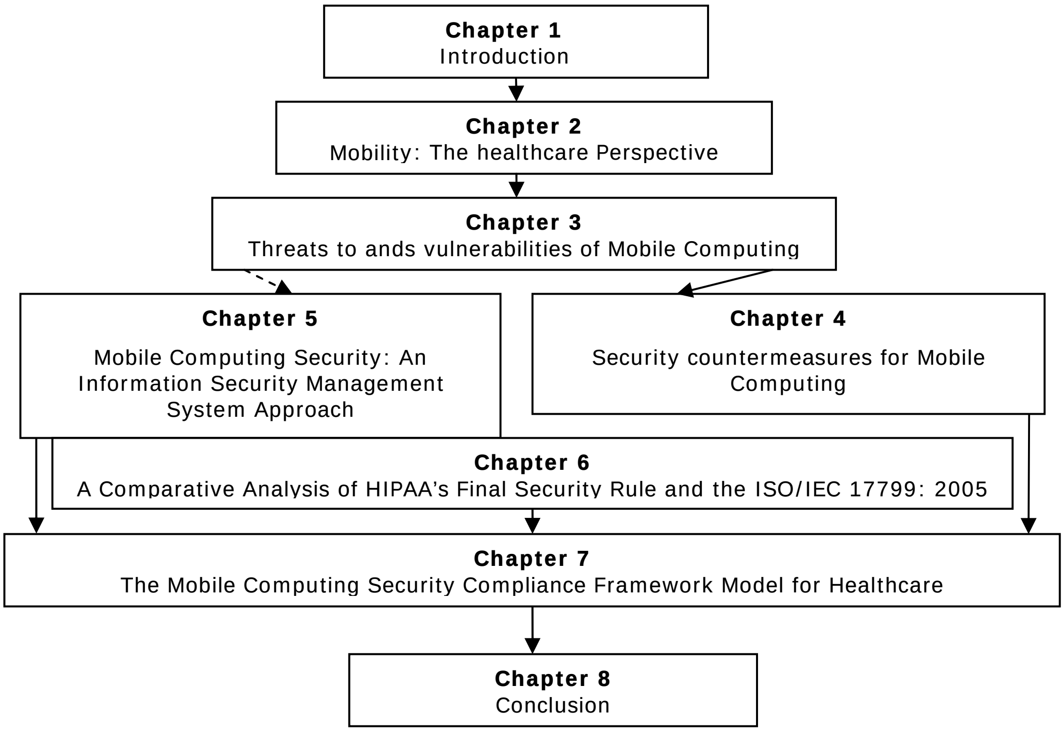
Chapter 1
Introduction
Chapter 2
Mobility: The healthcare Perspective
Chapter 3
Threats to ands vulnerabilities of Mobile Computing
Chapter 5
Mobile Computing Security: An Information Security Management System Approach
Chapter 4
Security countermeasures for Mobile Computing
Chapter 6
A Comparative Analysis of HIPAA's Final Security Rule and the ISO/IEC 17799: 2005
Chapter 7
The Mobile Computing Security Compliance Framework Model for Healthcare
Chapter 8
Conclusion

Figure 1.1 Layout of Dissertation

Chapter 2

Mobility: The Healthcare Perspective

This chapter introduces the concept of mobility in a computing environment. The technologies used in mobile computing and their relationships are introduced. The chapter further highlights, briefly, the basic types of mobility. The chapter proceeds to show how mobility influences a healthcare enterprise. It investigates the advantages the technology offers to healthcare, while highlighting the associated challenges to healthcare. Eventually, conclusions, based on the discussion, will be drawn. The chapter begins by providing an overview of the concept of mobility.

2.1 Mobility

What really is mobility? Generally, mobility can be defined as the ability to move, or be moved, from place to place. According to Kakihara & Sørensen (2006), the meaning of the concept of mobility spans a wide spectrum of human and non-human, as well as factual and theoretical spheres. Despite the broad extent of the general meaning, the concept of mobility has been habitually understood and quite narrowly used in modern industry and directorial contexts, for instance, “mobile technology”, “mobile office”, and “mobile work” (Kakihara & Sørensen, 2006; Wyatt, 2005).

Viewed from a technological standpoint, Gorlenko and Merrick (2003) consider mobility as an attribute of both a user and a device, defining mobility as the ability of a user and device to relocate while continuing to interact. Nikander et al. (2003) describe mobility as a phenomenon where an entity moves while keeping its interaction context active, and for this to happen, mobility requires a network to support seamless user roaming anywhere the user moves (Aruba, 2006). With these definitions in mind, it can be argued that mobility is defined in the context of its usage.

According to Cardelli (1999) and Ichiro and Niranjan (2002), there are two distinct areas of work in mobility. The first, “mobile computing or physical mobility”, is concerned with computation that is carried out in mobile devices such as laptops, personal digital assistants, etc. The second “mobile computation or virtual mobility" is concerned with mobile code that moves between devices such as applets, agents, etc. (Jansen et al., 1999; Zachariadis & Mascolo, 2003).

Mobile computing represents a different global computing paradigm which has evolved independently of the Web. Instead of connecting together all the LANs in the world, it extends the reach of a LAN by moving individual computers and other gadgets from one LAN to another, dynamically. In this case the very components of the network can move about as opposed to the notion "mobile computation" which is meant to be achieved over a fixed but possibly flaky network. Mobile computation provides the notion that running programs need not be perpetually tied to a single network node (Fuggetta, Picco & Vigna, 1998; Karnik & Tripathi, 1998; Cardelli 1999).

Although these areas are distinct, they are interrelated, (Ichiro & Niranjan, 2002; Cardelli, 1999). Together, the mobility areas work to provide fully distributed and ubiquitous mobile computing and communications, offering anywhere, anytime access. With the advancement in mobile wireless networks and the increase of powerful mobile computing environments that can roam across different types of networks, a variation and limitation of mobility types have emerged.

According to ECMA (2005) and Banerjee et al. (2003) the basic mobility types include terminal (device), user, service and session mobility. The classification is done on the functionalities the mobility management network provides "The management network represents a set of functions used in the core network to provide mobility within the home network and across visited networks" (ECMA, 2005). Furthermore, these basic mobility types can be further classifiedaccording to their ability to cope with crossing, diverse network infrastructure, such as different access technology or different network domains. However, for the purpose of understanding mobility in this study, only the basic mobility types will be discussed. The next section focuses its discussion on the basic mobility types.

2.2 Types of Mobility

Hasan et al. (2001), ECMA (2005), Banerjee et al. (2003), Dupré la Tour, Chouinard and Bochmann (2001) and Leggio et al. (2005) described the different basic types of mobility. These descriptions are based on the type of element that is considered to be moving and are described as follows:

2.2.1 Terminal (or device) mobility

Terminal (or device) mobility refers to the movement of a mobile device in a network environment, which enables it to receive continued access to services, independent of their location and while on the move (e.g., a cellular phone). Terminal mobility can be seen in Figure 2.1, where a user continues to access email on his PDA as he transits from domain A to B. Terminal mobility requires the capability of a network to identify and locate a given terminal.

Terminal mobility can be as simple as moving the terminal device (e.g., PDA) locally over a small area, for example, from one cell to another in the area of same base station (within a GSM or CDMA network), or as complex as a change in access technology, for instance, from GSM or GPRS to WLAN, usually referred to as network-level mobility, depicted in Figure 2.1.

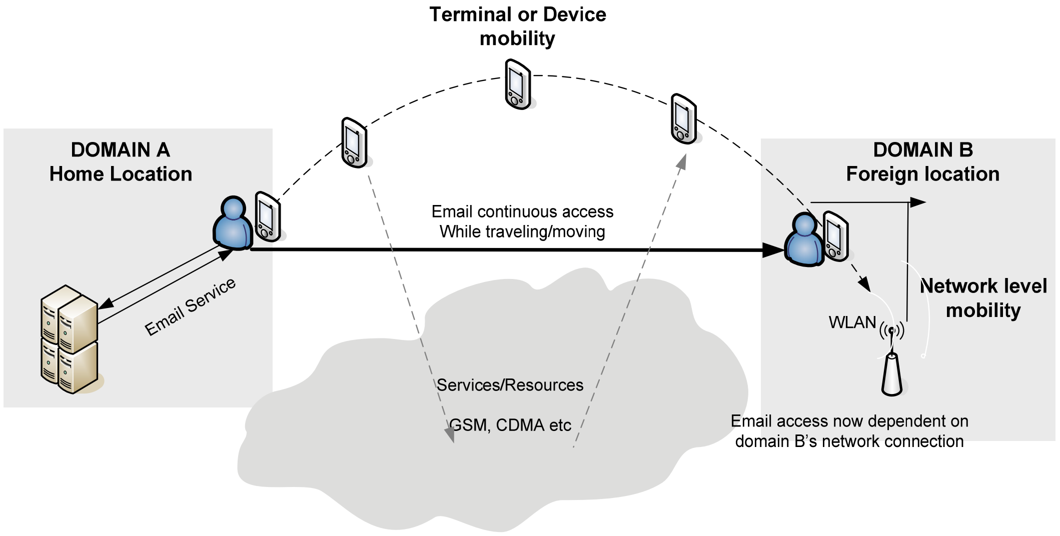

Figure 2.1 Terminal or Device Mobility

2.2.2 User mobility

User mobility is the ability of a network or networks to provide connectivity to a user even when his point of attachment changes regardless of whether or not this involves a change of terminal. As a user does not remain in the same place but moves around over time, this enables a user to access services irrespective of location.

User mobility allows a user to retain access to authorised services, for instance, in the case of persistent single sign-on capability. The concept used in mobile Internet Protocol (IP) networks can be attributed to this type of mobility. Mobile IP effectively hides IP address changes, allowing transport-level connections to survive a network handover. As depicted in figure 2.2, a user (A) migrates from domain A to B, but all requests to access Users A's mobile node X are sent to his home domain (A) then tunneled to network B. Network B, in turn, forwards the request to the visiting User A's mobile node X using its LAN. The approach enables a user to work as if he was directly in the home domain.

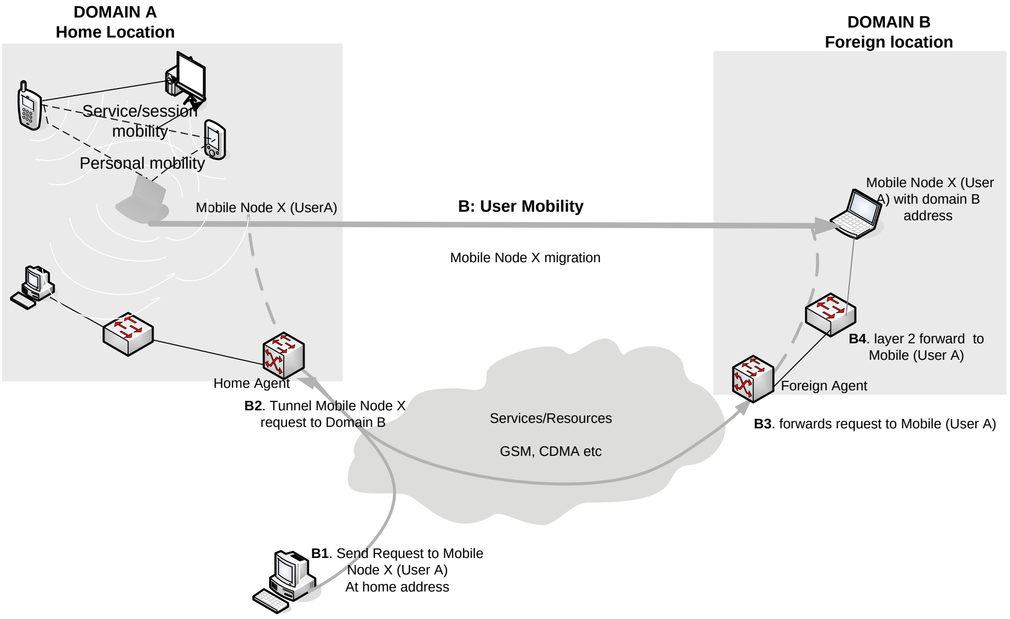
DOMAIN A
Home Location
Service/session mobility
Personal mobility
Mobile Node X (UserA)
B: User Mobility
Mobile Node X migration
DOMAIN B
Foreign location
Mobile Node X (User A) with domain B address
B4. layer 2 forward to Mobile (User A)
Foreign Agent
B3. forwards request to Mobile (User A)
Home Agent
B2. Tunnel Mobile Node X request to Domain B
Services/Resources
GSM, CDMA etc
B1. Send Request to Mobile Node X (User A) At home address

Figure 2.2 User Mobility

User mobility can also be referred to as personal mobility (El-Khatib, Hadibi & Bochman, 2003; Schulzrinne, 1996). Personal mobility is the ability of a user to get access to telecommunication services from any terminal (workstation) any time and from any place, based on a unique user identity, and the capability of the network itself to provide services in accordance with the user's service profile. This means the possibility of accessing services from several terminals simultaneously. For instance, a video conference session on a user's PDA can be handed off from a PDA to a wireless device screen and speakers in a conference room. The PDA, in this case, is using services provided by other devices. The analogy is depicted in Figure 2.3 with regard to a Wireless Personal Area Network (WPAN).

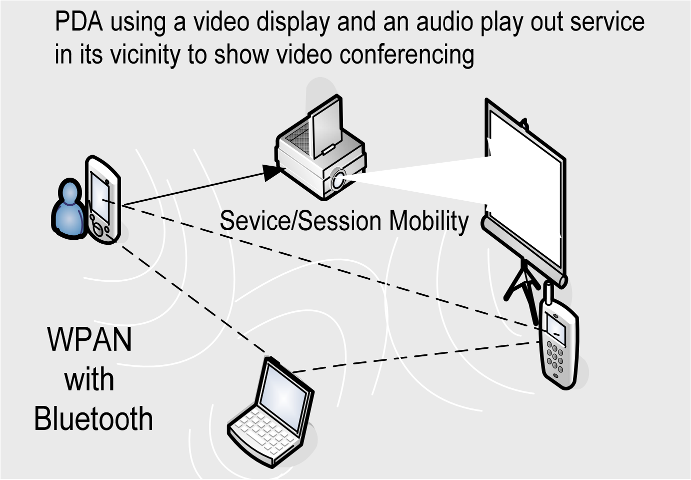
PDA using a video display and an audio play out service in its vicinity to show video conferencing
Sevice/Session Mobility
WPAN with Bluetooth

Figure 2.3 Personal Mobility

2.2.3 Session mobility

Very much related to the subject of personal mobility is session mobility. This provides the possibility of suspending a service on a device and picking it up on another device at the same point where it was pending (Kahane et al., 1997). It enables the user to maintain an active session while switching between terminals or changing to another subnet or access network. Furthermore, it can be seen as the ability of a user to transfer an ongoing communication session from one device to another device (Mingqiang et al., 2005).

Thus, it is possible to use different devices, with diverse characteristics, while maintaining an active session or state. For example, a user can read electronic mail on a mobile phone while traveling to work, and once arriving at the office, can change to a desktop computer, and continue email reading or writing from exactly the point at which he left off on his mobile phone. Figure 2.4 shows this mobility.

2.2.4 Service mobility

While device and user mobility define the mobility of service users, service mobility defines the capability of the network to provide a set of users the subscribed services, irrespective of their current locations or device types.

Service mobility can be achieved if a user can obtain subscribed and personalized services consistently, even if connected to a foreign network service provider; this requires access to a service to be guaranteed, anywhere, anytime. El-Khatib et al. (2003) state that service mobility is a service handoff process.

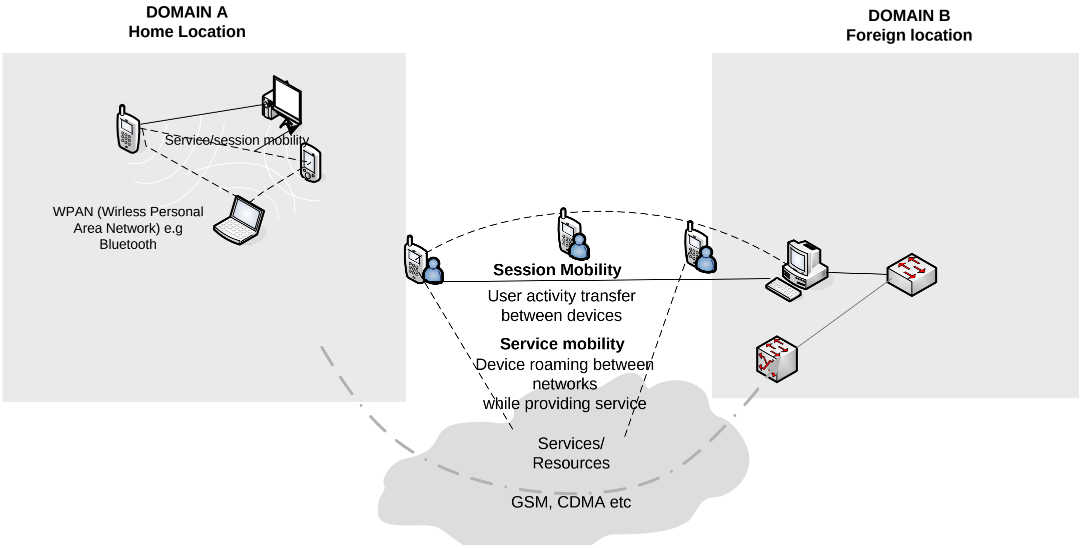
DOMAIN A
Home Location
DOMAIN B
Foreign location
Service/session mobility
WPAN (Wirless Personal Area Network) e.g Bluetooth
Session Mobility
User activity transfer between devices
Service mobility
Device roaming between networks while providing service
Services/ Resources
GSM, CDMA etc

Figure 2.4 Session and Service Mobility

As a user moves from one device or network service to another, a similar service on another device or network can carry on the active communication session. An example of service mobility is the ability of a call session to transfer from one cell tower to another as a cell phone user moves from one location to another. This mobility is shown in figure 2.4. In another example, El-Khatib et al. (2003) illustrated that it is possible for a user to receive a call on his PDA for a multimedia conversation with a partner. The user's PDA tries to find a microphone, a speaker, a video display service and a camera to make for a full multimedia session. Assuming the user moves with his PDA into a conference room where other team members are waiting, the PDA tries to discover similar services to continue the session in the conference room.

The difference between terminal, user, session and service mobility is that in terminal mobility, devices move; in user mobility, one person uses different devices and moves from one location to another while having access to services; session mobility describes actively moving from one device to another while remaining in communication; and service mobility means having access to a required service, regardless of location or device type, to either continue a session or perform some other task.

Although these mobility types differ, they work together to provide a seamless user experience (Cardelli, 1999; Dupre la Tour et al., 2001; El-Khatib et al., 2003). For instance, session and service mobility can not be used without terminal or user mobility (ECMA, 2005). In order to achieve the best possible user experience, mobility must be seamless. The next section shows how the various types of mobility work together to provide a seamless mobility experience.

2.3 Seamless Mobility

In order to make mobile computing so embedded, so fitting, and so natural that it is used without even thinking about it, the transition between networks must be seamless. Seamless mobility means a smooth connection of users across multiple geographical spaces (e.g., offices, hotspots and homes), and the provision of network, application, content and service interoperability across a wide variety of devices.

Section 2.3.2 provided an analogy that showed devices collaboratively providing an *ad hoc*-distributed computing environment to deliver services that could not be delivered by a single device in a Bluetooth network. The same analogy can be attributed to a GSM roaming service.

A GSM roaming service provides the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services when travelling outside the geographical coverage area of the home network, by means of using a visited network (Molloy, 2003). Another example is the Web services' Universal Description, Discovery and Integration (UDDI) protocol, which discovers services for users to enable them to perform their tasks over the Internet (Oasis, 2005).

Seamless mobility provides access to application and service contents by automatically switching between technologies and physical environments (Kapil, Emily & Gupta, 2006; Bogdon & Ferguson, 2004). The ubiquitous computing applications frequently exploit physical location and other background information about users and resources to enhance the user experience (Campbell, Al-Muhtadi, Naldurg, Sampemane & Mickunas, 2002). The hand-offs between protocols, networks, and services are transparent to the user, providing the best possible user experience (Bogdon & Ferguson, 2004; Ross, 2006).

In an effort to achieve seamless mobility, mobile devices now come with a number of enabling technologies that allow them to connect to both cellular and non-cellular networks (Wiehler, 2004, p. 27). New models of devices are capable of communicating via Bluetooth, WLAN and GPRS. The devices, therefore, can provide seamless access and connectivity across personal, local and wide area locations.

Facilitating seamless mobility is the introduction of the Software Defined Radio (SDR) (Wipro, 2002; Cotton, 2005). SDR technology can implement a wide range of radio applications like Bluetooth, WLAN, GPS, Radar, WCDMA and GPRS. The technology enables the implementation of radio functions or air-interface standards in networking infrastructure equipment and subscriber mobile devices as software modules running on a generic hardware platform. This helps in building multi-mode mobile devices and equipment, resulting in ubiquitous connectivity irrespective of underlying network technology used.

For instance, if a mobile device is incompatible with a network technology in a particular region, an appropriate software module needs to be installed onto the device. This is possible over-the-air, resulting in seamless network access across various geographies.

Furthermore, SDR technology helps both network operators and mobile devices manufacturers (Youngblood, 2002; Wipro, 2002). Network operators can perform migration of networks from one generation to another using SDR. Furthermore, it enables faster deployment of new services on a subscriber’s device since it would only involve a software upgrade. With SDR, manufacturers can perform remote diagnostics and provide fault fixes by merely uploading a newer version of the software module to a consumer’s device, as well as network infrastructure equipment.

Besides that, mobile devices have the power to support enterprise applications and are increasingly connected to an enterprise network, via high-speed wireless networks (Funk, 2004, pp. 1 – 8; Dedo, 2004). A user therefore can connect to relevant content, which will continuously synchronize automatically as he or she transmits. The next section provides more information on mobile device types, and their proliferation and role in the mobile environment.

2.4 Mobile Devices’ Evolution

Mobile devices started as single-function devices, such as cellular phone handsets, text pagers, bar-code readers, walkie-talkies, and Personal Digital Assistant organizers, offering minimal functionalities (Dedo 2004; Wiehler, 2004, p. 25). Advancements in the technology have made it possible to incorporate these functionalities with additional capabilities in the newer devices (Slawsby, 2004). The functionalities and the additional capability, along with business applications, are becoming available in converged PDAs and cell phones.

Today’s PDAs come with integrated phone features or as cell phones with integrated PDA software functions, providing both voice and data capability (Lehrbaum, 2000; Linhoff, 2002; Wales, 2003). The new breeds of devices with integrated features are referred to as smart phones. In fact, new mobile devices now enjoy megabyte access to the Internet, can store gigabytes of information on memory cards or embedded memory and have much stronger processing capabilities (Dedo, 2004; Lehrbaum, 2000) .

According to Slawsby, in an IDC Report (2003), more than 19 million mobile devices were shipped worldwide, with operating systems designed to offer highly capable personal computer synchronization, software application execution, and user data storage functionality. These capabilities make these devices ideal for a greater computing infrastructure (Forman & Zahorjan, 1994).

PDA-sized devices, most often referred to as handhelds, provide support for a calendar, contacts, e-mail, multimedia, and business data along with a built-in phone and full wireless capability. The converged functionalities of these devices help to reduce the costs and decrease the complexity associated with equipping a mobile workforce (Dedo, 2004).

Mobile devices, whether personally owned by employees or part of an organization deployment, are already helping to streamline business process efficiency, customer service responsiveness, and corporate competitive differentiation (Slawsby, 2004; Dedo, 2004).

Other examples of mobile devices include laptop computers or even the modest floppy disk that is capable of storing corporate information. Computer hard disks, PDAs, compact flashes, digital media memory cards or devices, removable media, such as CDs, DVDs, and tapes and cellular phone add-on memories are all mobile devices (Sadlier, 2003). As devices used in business may need to store large amounts of data, smaller add-on cards with increasing storage volume are available for devices, such as pocket PCs and smart phones (Dedo, 2004).

Although laptops are no longer a new technology, they have evolved over a number of years and have consequently become as powerful as typical desktop computers, with fully built-in wireless capability.

Organizations are taking advantage of these mobile technologies in order to gain competitive advantage as well as increase productivity (Kalakota, 2004). Although mobile devices were first developed as an end-user product rather than a business solution, a number of innovative firms are adopting these technologies to reform their business (Kakihara & Sørensen, 2006).

Today, handheld devices, such as PDAs and smart phones, are used in nearly every business. These handhelds now have the power to support an organization vertical application and are increasingly connected to the organization via high-speed wireless networks (Wiehler, 2004, p. 27). The next section looks at the wireless technologies accessible by mobile wireless-capable devices.

2.5 Difference between Mobility and Wireless

Most often people tend to use the terms “wireless” and “mobility” interchangeably, but that, however, is not entirely accurate. From the discussions in Sections 2.2 and 2.3, it can be argued that mobility can be achieved devoid of any underlying access technology, and it can be either wired or wireless, providing access from anywhere. According to RIM (2005), mobility is a strategic approach that highlights how business problems should be solved. Mobile workers, devices, and applications do not necessarily use wireless capabilities. Many mobile laptop users rely solely on dial-up connections to access and transfer corporate information (Hayes, 2001).

RIM (2005) states that wireless is a technology that is capable of solving these problems. Wireless is simply a technology that helps achieve a wider mobility spread by using radio waves. With a wireless network in place, users can access shared information without looking for a place to plug in, to gain access to back-office systems whilst on the move (Fontelo & Chismas, 2005). Being mobile is not a requirement for using wireless technologies (Hayes, 2001). It is possible for a fixed, stationary machine to access a wireless network as well as access resources in a foreign network. This process is referred by Gorlenko and Merrick (2003) as partial mobility.

The explosive growth of Wireless Local Area and the Wide-Area Cellular systems networks, along with the fast and growing adoption of mobile devices, has brought about the mobile computing evolution. The advancement in these technologies has changed the way we compute, communicate, interact and do business. The main categories of wireless networks that have enhanced the mobile computing evolution are discussed in the subsequent section.

2.6 Types of Wireless Networks

There are basically three main categories of wireless networks: the Wireless Personal Area Networks (WPANs), the Wireless Local Area Networks (WLANs) and the Wireless Wide Area Networks (WWANs). These were designed with mobility in mind (Hayes, 2001) to cover the full spectrum from short-range technologies (Bluetooth, WLAN) through to globally deployed technologies (GSM, GPRS), as depicted in Figure 2.5.

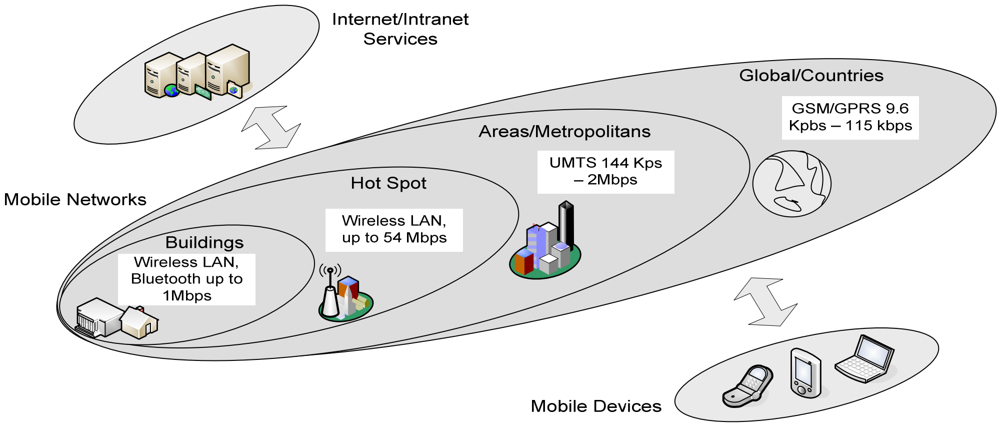
Internet/Intranet Services
Global/Countries
GSM/GPRS 9.6 Kpbs – 115 kbps
Areas/Metropolitans
UMTS 144 Kps – 2Mbps
Hot Spot
Mobile Networks
Wireless LAN, up to 54 Mbps
Buildings
Wireless LAN, Bluetooth up to 1Mbps
Mobile Devices

Figure 2.5 Scope of Mobile Network Technologies (Wiehler, 2004)

These networks are categorized by different focuses and parameters in terms of bandwidth, quality of service, standards, range, costs and services.

Priscetello (2004), Karygiannis and Owens (2003), Blount (2004, p.6), Wiehler (2004, pp. 21 – 24), Luukkainen (2003), and Nelson (2002), described these networks as Wireless Personal Area Networks, Wireless Local Area Networks and Wireless Wide Area Networks as discussed in the subsequent sections.

2.6.1 Wireless Personal Area Networks (WPANs)

WPANS are composed of *ad hoc* networks, most often created by Bluetooth and infrared signals. WPANs are usually designed to dynamically connect remote devices, such as cell phones, laptops, and PDAs, printers, digital cameras, scanners, keyboards and mice. The network is usually small and uses connecting mobile devices in a room, instead of the wiring that would normally connect one piece of equipment to another. These networks are termed "*ad hoc*" because of their shifting network topologies.

An *ad hoc* network is usually formed on the fly, and it is temporary, with shifting network topologies maintaining random network configurations (Juha, 2000; Kumar, 2006, p. 5). Mobile devices in a PAN communicate directly with other devices, which are relatively close together: typically devices are within 10 meters of each other, which is a small area in comparison with the WLANs.

2.6.2 Wireless Local Area Networks (WLANs)

WLANs provide all the functionality of a wired LAN, without the limitation of the physical link. WLANs allow greater plasticity and portability than the traditional wired LANs. A WLAN connects computers and devices equipped with wireless network adaptors to a network, using a wireless access point device connected to the wired network.

An access point connects to a wired Ethernet LAN, via an RJ-45 port. Access-point devices typically have coverage of areas of 100 meters in range, and are capable of covering greater distances when used as repeaters. Wireless users move freely within the range or between access points with their laptop or other network device, without losing the connection.

2.6.3 Wireless Wide Area Networks (WWANs)

WWANs are the most common networks and mostly referred to as cellular networks. These networks provide phone-call services as well as services like Short Message Service (SMS) and data on a national or global scale (RIM, 2005; Luukkainen, 2003, p. 7).

The technologies have evolved over the last few years. The traditional analogue network has since then evolved into the digital wireless network with data transmission capabilities and is now in its 3rd generation (Kagranen, 2005, pp. 15 – 24).

The first-generation networks, the Advanced Mobile Phone System (AMPS) and the Total Access Communication System (TACS) have evolved giving way to the Global System for Mobile Communications (GSM), Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA), also referred to as second-generation networks.

The data side extensions of these networks are GSM/HSCD, GPRS, EDGE, CDMA2000, and UMTS, a third-generation network (3G). The differences lie in the speed and mode of transmission. For instance, the HSCSD (High Speed Circuit Switched Data) and GPRS (General Packet Radio Service) are advanced wireless data networks, based on the GSM network. Unlike HSCSD, which uses circuit switching and achieves high data rate of up to 57kps, GPRS is based on the relaying of individual data packets transmission rates of up to 171kps. A GPRS network, usually referred to as the 2.5G, is faster than a 2G data network (CDMA 1x One) but slower than EDGE, classified as a 2.75G network technology (HP, 2006). The 3G networks are expected to complete the globalization process of all mobile communications (Ahtianen, Kaaranen and Naghian, 2005, p. 5).

In a WWAN, you can use wireless to reach a carrier's voice or data network instead of plugging a notebook into a phone jack and dialing into the Internet. For example, field personnel can check prices or inventory while visiting a customer site by using a WWAN to query a database back at the office.

In a WWAN, each mobile device communicates to a public carrier's base station. The amount of data that can be transferred over these networks is increasing and allows for more robust applications. This network provides a wider coverage. According to RIM (2005), if users require access everywhere, then carrier-based technology is best, as access is provided within and between countries. There is no coverage that can surpass that provided by a standard carrier, hence, enhancing greater mobile computing capability.

As mentioned in previous sections, the vast extent and capability of these networks have greatly impacted on mobile evolution, providing the business industry with numerous advantages. The next section looks at mobility from a healthcare perspective.

2.7 The Mobility Evolution in Healthcare

From an enterprise perspective, mobility is the means of providing universal access to the communication tools or devices, information, and applications employees rely on to be productive (Wyatt, 2005). This access is regardless of where they are or what device they have access to at any time. This means making office desktop communication and information resources available at different locations while on the move for mobile workers (ECMA, 2005).

Traditionally, mobility in health care was commonly referred to as telemedicine. Telemedicine is defined as the “delivery of health care and sharing of medical knowledge over a distance using telecommunication means” (Strode, Gustke & Allen, 1999). This process was mostly carried out over the traditional desktop infrastructure.

According to Coiera (1997), the essence of telemedicine is to exchange information, whether it is voice, image, and elements of medical records or commands to a surgical robot, at a distance. It can be argued that the aim of telemedicine is to provide expert-based healthcare to understaffed remote sites and offer advanced emergency care through modern telecommunication and information technologies (Kyriacou et al., 2003).

Traditional telemedicine relied on technologies like the Public Switched Telephone Network (PSTN) to deliver medical diagnoses and remote education and stationary patient monitoring (Zhao, Yagi, Juzoji & Nakajima, 2002; Varshney & Vetter, 2000). The traditional wireless concept in healthcare was more associated with bio-monitoring. This wireless concept is in the form of physiological monitoring and physical activity monitoring (Kyriacou et al., 2003; Budinger, 2003). Physiological monitoring includes monitoring of parameters, such as heart rate, blood pressure, and other physiological signals. Physical activity monitoring involves monitoring parameters, such as monitoring of movement, fall detection, location tracking, gastrointestinal telemetry, and other physical activities.

The concept of bio-monitoring has been used widely in the last two decades to perform data acquisition tasks. However, there was no timely integration of data into medical records; hence, no immediate action occurred if abnormalities are detected. A typical example is the Electrocardiogram (EKG/ECG) monitoring with a Holter monitor during an initial evaluation of a patient who is suspected to have a heart-related problem (ASM, 2006).

Today, telemedicine systems are supported by state-of-the-art technologies like interactive video, high-resolution monitors, high-speed computer networks and switching systems, as well as telecommunications' superhighways (Kyriacou et al. 2003). Developments in these areas were mainly driven by the sprouting mass markets for cell phones and portable computing devices, which represent an evolution of the previous generation of telemedical systems (Laxminaryan & Istepanian, 2000).

According to Budde (2002), the technologies for high-speed data transmission in mobile networks, such as HSCSD and GPRS, can be used to assist emergency services. For instance, ambulances at the scene of a major accident could send real-time video, pictures and medical data to a specialist centre. A current application can be seen the UK, where the Fife Fire Service use photo messaging to save lives by sending real-time pictures of casualties from accident scenes, enabling consultants to assess the extent of injuries (Bitcon, 2003). In addition, clinics also send scans and X-rays to medical experts in another region or country for emergency examination (Budde, 2002).

The advancement in enabling Internet and telecommunications' technologies has propelled the recent advancement in telemedicine applications (Zhao et al., 2002). In addition, the increasing demand for access to high-quality medical care, irrespective of location or geographical mobility, further incited the development.

The new 3G cellular networks (UMTS) and the new generation of WLAN and *ad hoc* networks have extended the medical information coverage, further flexibility and new applications for telemedicine (Ganz, Istepanian & Tonguz, 2006). Today's mobile broadband applications, such as wireless-streaming video and real-time collaborative videoconferencing are increasing productivity and bringing a world of information whenever and wherever it is needed.

It can, therefore, be argued that the emerging wireless concept represents the evolution of e-health systems from the traditional desktop "telemedicine" platforms to wireless and mobile configurations (Istepanian & Lacal, 2003). The advantages in wireless and mobile telecommunications technologies will enable swift and better healthcare delivery, regardless of any geographical barriers and time and mobility constraints (Zhao et al., 2002).

The perceived advantages associated with the advancement in technologies, has redefined mobile healthcare as mobile computing, medical sensor, and communications technologies for healthcare (Istepanian et al., 2004). The following section looks at the possible role of mobile computing in healthcare.

2.8 Mobile Computing in Healthcare

Mobile computing can be seen as both an emerging and enabling technology. In the sense that continuous evolution of wireless technology and the seemingly endless introduction of newer portable user devices provide direct value to clinicians and across the health organization (Finch, 1999). Rapid advances in mobile and wireless network technologies in recent years have opened new opportunities for new and innovative means of healthcare delivery (Ganz et al., 2006). Mobile computing is the next technological cutting edge for healthcare providers (Siwicki, 2003).

Spurred by the desire to provide better quality healthcare service to patients, the shortage of caregivers throughout the world, financial pressures, availability of mobile devices, wireless connectivity and tight margins have propelled the adoption of mobile computing in healthcare (Meridian, 2006; Sorensen, Naess, Strand, Stanford, 2002; Conradi, 2003). The key challenge is to provide better healthcare services to an ever-increasing number of population using limited financial and human resources. The increasing cost of healthcare services has created numerous challenges for policy makers, healthcare providers, hospitals, insurance companies and patients (Varshney, 2004; Stanford, 2002).

The healthcare industry, initially, was considered a lagged industry in the adoption of technology (Linhoff, 2002), and it was a matter of time before healthcare industry leaders and decision-makers began to realize the supporting role of technology in their effort to maintain a focus on quality care, while meeting the pressures from regulatory bodies, competition, and achieving business and performance goals (Finch, 1999; Portale, 2002; Sawyer, 2003).

A Forester report by Brown, Holmes and McEnroe (2006) titled "Hospital I.T. Spending Trends for 2006", showed that hospitals are more likely than entities in other industries to make new investments in information technology, rather than focus on maintenance and operations of existing information systems. The push for electronic medical records, picture archiving and communication systems, wireless and mobile infrastructure has driven investments in new products for healthcare providers.

Healthcare information technology or information systems provide many advantages when used for improved access support, collaboration and information sharing among healthcare providers, patients, and researchers (Zhang et all, 2002; EthicSA, 2000). By helping to make accurate information more readily available to healthcare providers, workers, researchers and patients, advanced computing and communication technology can improve the quality and lower the cost of healthcare (Chao, et al., 2005; Lampsas, Vidalis, Papanikolaou & Vagelatos, 2002). This is better achieved with improved level of automation, integration and reduced reliance on paper-based forms (Dedo, 2004; Keay, 2004).

Due to the mobile nature of caregivers, the traditional networked desktop system is not the most suitable solution, as caregivers make decisions at the point of care. According to Portale (2002), the networked desktop systems introduced several key drawbacks. The drawbacks include a high cost of ownership, as a result making room for only a few. The traditional networked desktop systems simply served as administration systems with caregivers queuing to use a desktop application. More importantly to healthcare providers, the traditional system impeded the ability of healthcare practitioners to efficiently document care as they moved from patient to patient.

However, mobile devices provide the solution to data access needs and help support a nurse's clinical practice at the point-of-care (Darwin, 2000; Dedo, 2004). The ability to access medical calculators and reference information, such as drug databases, clinical guidelines, formularies and electronic textbooks at the point of care, has guaranteed the future of mobile devices in healthcare (Meridian, 2006).

According to Newcombe (2003), a National Governors Association report in the US showed that the States is facing a massive budget shortfall as a result of the growth in Medicaid in the national health-care system for the poor and disabled. While holding down Medicaid and other public healthcare costs was not an option, the one way they could improve the situation was by ensuring that the programs and the professionals in charge get the most from their resources. By embracing mobile technology, a new chapter in the public sector's efforts to improve the services and programs, while keeping costs to a minimum, was opened (Newcombe, 2003).

It can be argued that caregivers are fueling the growth of mobile technology in healthcare, requiring that their institutions keep pace and support the process (Darwin 2000; Scheepers, 2003). While most establishments are just beginning to evaluate how to best utilize mobile devices, many physicians have sprinted ahead (Hau, 2001). Physicians are purchasing devices, such as PDAs, on their own to help manage administrative and clinical tasks. Thanks to the Internet, many doctors and nurses have already grown familiar with information technology, and are attracted by the promise of anytime, anywhere access (Portale, 2002).

A 2004 Forrester research study showed that 57% of all physicians and 73% of residents regularly use mobile devices during the work day (Bishop, 2005). Clearly, mobile computing is becoming increasingly popular in the practice of medicine (Hau, 2001). The explosive increase of pervasive computing in healthcare has begun to generate many useful applications, systems, and tools (Stanford, 2002). The data capture and retrieval capability of new mobile devices, such as new Personal Digital Assistants (PDAs) and smart phones provide enhancement for mobile healthcare applications with improved convenience and versatility to health providers and patients.

Although caregivers are interested in increased efficiency and improved workflow, they are even more interested in how wireless applications can reduce medical errors. Many medical errors are caused by the time-consuming, paper-based processes used throughout the industry (Wales, 2003; Portale, 2002). Pairing mobile devices with doctors and nurses who are always on the move could reduce errors by allowing data to be accessed and entered into systems at the point of care (Havenstein, 2005).

Besides that, good nursing practice requires tools to extend the human mind's limited capacity to recall and process large numbers of relevant variables. Huge amounts of data and information are collected during healthcare processes. The data and information, together with tools such as medical references and calculators, are of little use unless they can be made available where they are needed at the point of care (Darwin, 2000; Dedo, 2004).

Furthermore, mobile computing provides numerous advantages to patients. Patients can use their cell phones to send physicians their medical and insurance information under new initiatives (Broder, 2006). Patients are using the wireless-capable technology to track their own progress and relay the results to doctors miles away (Trom, 2002).

Mobile computing provides prospects for organizations to increase the amount of time available for patient care, make more informed decisions at the point-of-care, and create "virtual teams" for collaborative patient care.

2.9 Benefits of Mobile Computing in Healthcare

Mobile devices and mostly wireless networks transform the methods physicians and caregivers use to provide services. By using PDAs, caregivers are able to spend more time interacting with patients, make fewer errors which have an influence on cost, achieve enhanced personal productivity and improve care. The benefits associated with the marriage between the mobile and the wireless network, according to Portale, (2002), AireSpace, (2004), MacDonald, (2003), Dedo, (2004), Wales, (2003), Crumbley, (2003), and Luo, (2004) include:

- **Increased Time with Patients**: Wireless connectivity enables healthcare professionals to spend less time on administrative tasks, such as retrieving records, and more time with patients. Mobile computing presents opportunities for organizations to increase the amount of time available for patient care, make more informed decisions at the point of care, and create "virtual teams" for collaborative patient care through computing.

- **Improved Decision-Making**: Real-time access to patient records, drug information and medical reports can help to ensure that appropriate diagnoses are made in a timely fashion. Handheld, wireless applications can enable doctors and nurses to gain ready access to complete patient treatment histories, and gain access to the right information, at the right time, to prescribe the right course of treatment.

- **Reduced Errors:** In most healthcare settings, there is a significant number of manual steps and procedures involved when dealing with a patient. The manual steps and procedures are slow and prone to errors. Research has shown that lack of access to information during decision-making, and ineffective communication among patient-care team members, are proximal causes of medical errors and other adverse events in patient care (Eneida et al., 2004). Research by the Institute of Medicine in the United States calculated that medically preventable errors are responsible for 1.3 million injuries in the US every year, resulting in 98,000 deaths and costs of US$ 77 billion (Meridian Healthcare, 2006).

  The automation of manual steps and processes, combined with the “error checking” and “reminder” capabilities of an automated system, has proven to significantly reduce errors. Wireless technology and mobile PDAs bring this capability to a much broader range of healthcare settings.

- **Response to Patient Needs**: With a wireless network, physicians can pro-actively monitor a patient’s vital statistics from almost anywhere and rapidly respond to the slightest of changes. In addition, they can respond with minimal delay, ensuring that care is provided as expeditiously as possible.

- **Patient Privacy**: Using a mobile device to directly save patient’s sensitive information to a database can enhance privacy. Paper forms potentially put patients’ information at risk since it is often easily accessible by inapt third parties. Using a mobile computing process offers more privacy since information is immediately protected by access control mechanisms.

- **Outpatient Monitoring**: Outpatient patient monitoring reduces the number of unnecessary hospitalizations, while offering healthcare services to those in critical state who really need it. Patient monitoring using mobile and wireless technologies can reduce the stress and strain on healthcare providers, while enhancing their productivity and reducing work-related stress. In the long-term, affordability, portability, and re-usability of wireless technologies for patient monitoring and preventive care will also reduce the overall cost of healthcare services.

- **Point of Care Data Access**: Handheld and other wireless devices give healthcare providers point-of-care data access and data capture throughout the hospital facility. Handhelds, like PDA or tablet computers, are a technology enabler for ubiquitous data access (Andreas et al., 2004), delivering benefits, such as providing quick answers to questions or queries by accessing medical information; processing efficiencies and consistent reporting; increasing revenue as well as improved data accuracy and reducing errors. Using handheld devices, caregivers can capture charges for services rendered at the point of care.

- **Alerts and Emergency Responses:** In a hospital environment, the alerts and emergencies could be a patient emergency, a lab test result that becomes available (especially if it is out of the normal bounds for the test), a new alert for an outbreak in some part of the world issued by the Center for Disease Control, or a prescription which requires a refill when it has expired. Providing emergency response service using WLAN technology, allows hospitals to admit patients and take histories in the waiting room or at a bedside.

  Utilizing wireless cellular networks and a range of client devices, EMTs can transmit patient data to hospitals while en route in ambulances. Emergency-room doctors can view patient information on an electronic white board delivered straight from back-end systems to their PDAs over wireless networks. Physicians can quickly retrieve and review laboratory, radiology and other test results sent to their PDAs. The subsequent section looks at some real-life applications of mobile computing in healthcare.

2.10 Real-Life Applications of Mobile Computing in Healthcare

Wireless applications meets healthcare needs by taking advantage of devices that healthcare professionals are already using: mobile phones, pagers, and personal digital assistants (PDAs). The benefits of wireless technology are illustrated in a number of different examples and applications, which have been applied in several countries for either emergency or general healthcare.

The variety of wireless technologies, such as mobile computing and global positioning systems (GPS), has been applied to ambulance care in Sweden and the Netherlands. In an emergency situation, vital information about the patient and ambulance's exact time and location can be transmitted to the hospital in real-time (Wu, Wang & Lin, 2005). Hence, the hospital can be well prepared for the arriving of the ambulance at any time. The objective is to provide the best possible treatment and appropriate hospital to the patient at the right time (Geier, 2005).

Furthermore, a Vodafone policy paper series in (2006) by Gough & McCulloch shows a number of studies revealing the wide use of SMS-based applications in health services. Many report efficiency gains and benefits to patients and public health depending on the context they are used. For example, in England, France and Thailand, SMS messaging has enabled improved self-monitoring by diabetic patients and more regular reporting to clinicians (Sittampalam & Atun, 2006). This is also true of diabetes treatment initiated in Arizona, US; however, they were using a more advanced mobile device and reporting strategy (Becker, Sugumaran & Pannu, 2004).

In New York, a city battling an epidemic of asthma among poor children, care givers are using mobile application. They study the effects of preventative treatments in the field, tabulate the results on mobile devices and transmit back to headquarters for quick analysis. This has reduced the cost for asthma treatment (Newcombe, 2003).

At the Technische Universität München in Germany, a task-flow analysis within the transplantation unit revealed that valuable time could be saved in pre-transplantation management being able to retrieve data of organ receivers universally. Inspired by this clinical scenario, a mobile application was designed and implemented, providing surgeons with decision-relevant information on potential organ receivers (Andreas et al., 2004).

What is more, doctors in Africa, who until now have been battling epidemics like AIDS with limited resources, are turning to new technology to give them the information they need to help save lives. They are trying to overcome the difficulties of getting up-to-date medical information into the hands of medical professionals in underdeveloped countries. In 2002 Skyscape announced that its medical reference software is being used by African doctors to treat patients as part of the Satellite PDA Project (Wales, 2003).

In South Africa, SMS reminders are being used to enhance adherence to treatment in patients with tuberculosis in the indigent Transkei region of the eastern side of South Africa (Wright, 2001). In addition, SMS is also used to monitor treatment adherence levels of patients with AIDS in a township near Cape Town (Lindow, 2004). For instance, information on the dangerous side effects of the anti-retroviral, or ARV, drug is sent to patients.

Although mobile computing provides great benefits to healthcare, it is not without risks (Crounse, 2006; Borzo, 2005; Beard, 2006; Nokia, 2005). The size, portability, increased storage and processing capability of mobile devices put them at risks to all kinds of attacks. When caregivers access sensitive health information from their devices, ensuring that information is stored and transmitted securely becomes a primary concern.

2.11 Mobile Computing Security Challenges in Healthcare

Apart from the challenges associated with defining the mobile workforce and its responsibilities, the integration and management of technology and devices, security remains a major concern in mobile computing (Beard, 2006; Sun & Sauvola , 2002a; HP, 2005; Hau, 2001 & Shaw, 2003).

The phenomenal growth of mobile computing has brought about greater security challenges (Peterman, 2003, pp.1 – 9; Pullela, 2002). A 2006 Symantec global survey showed that one of the biggest obstacles in the widespread adoption of wireless and remote computing in business is security.

According to the survey, more than 60 % of companies are holding back on deploying mobile solutions, citing security reasons. The survey showed that almost one in five businesses have already experienced financial loss due to attacks, via mobile data platforms.

As ubiquitous computing involves location and other context information about users and resources to enhance the user experience, privacy and security become issues (Campbell et al., 2002; Langheinrich, 2001). Tackara et al. (1996) found that patients are concerned about the use of telemedicine in their treatment. Their concern is centered on the fear regarding the privacy of their transmitted medical records and personal information from which they can be identified.

As healthcare providers and patients become increasingly aware of the need for data security to reinforce confidence and trust, the challenges associated with security are greater than ever (Crounse, 2006; Borzo, 2005). According to the National Research Council (1997) it is the development of electronic medical records and linking of clinical databases that has increased concern for the privacy and security of health information.

In an effort to ensure the protection of privacy and security of patients health or personal information, many countries have enforced the protection of an individual’s medical data (Nealon, Moreno 2002; Wales, 2003). Nowadays, it is no longer a practice; it is required by law that healthcare providers in possession of patients’ private information employ security measures to protect it (Beard, 2006). According to the General Medical Council (GMC, 2002), when caregivers are responsible for confidential electronic information, they must make sure it is efficiently protected, whether it is stored, in transit or received.

Unfortunately, the size and portable nature of mobile devices that make them so attractive, increasingly place sensitive data accessed or stored by these devices at serious risks of theft, sabotage, exploitation and manipulation (Ottaway, 2002). As mobile and remote systems become prevalent, data is being carried to locations never reached before. It can be argued that mobile computing introduces a wide range of threats and vulnerabilities that threaten the privacy, confidentiality, integrity, availability, authenticity and non-repudiation of health information (Campbell et al., 2002; Langheinrich, 2001). These threats and vulnerabilities are investigated in Chapter three.

2.12 Conclusion

This chapter illustrated that although there are different notions of mobility, they are interrelated. In order to achieve a ubiquitous mobile computing environment, the types of mobility must work together in a seamless fashion to enhance a user's experience.

Mobile and wireless technology has greatly enhanced mobility in computing. The healthcare industry, like many business industries, has taken advantage of the new features of mobile devices and the affordability of wireless technology to improve the quality of care. Mobile computing has clearly become part of healthcare's electronic landscape and is becoming commonplace in the healthcare environment.

Although the mobile computing provides great advantages to healthcare, it is not without risks. The risks associated with mobile computing threaten the privacy and security of health information. Faced with a highly competitive business environment and regulatory pressures, mobile computing must be considered for compliance, as the flaws associated with it very much affect the privacy and security of health Information.

In order to have a successful mobile deployment in healthcare, it is imperative that the risks associated with mobile computing are carefully evaluated when employing a mobile solution in healthcare. The next chapter investigates the threats and vulnerabilities associated with mobile computing, which may pose threats to the privacy and security of health information.

Chapter 3
Threats to and Vulnerabilities of Mobile Computing

In the previous chapter, general mobility and computing concepts were discussed. It was discovered that the two great enablers for mobility are mobile devices and wireless technology. Mobile and wireless technology has greatly enhanced mobility in computing. The healthcare industry, like many businesses and industries, can take advantage of the new features of mobile devices and the affordability of wireless technology to improve the quality of care.

While mobile computing provides a lot of benefits to healthcare, it is not without risk. The characteristics of the wireless environment, and the size and portable nature of the mobile devices make them vulnerable. Faced with a highly competitive business environment and regulatory pressures, healthcare is under great pressure to ensure the privacy and security of sensitive health information.

This chapter investigates the threats and vulnerabilities and the types of attacks that are associated with a mobile computing environment. The chapter breaks the investigation into three broad categories: those associated with the wireless nature, those associated with the devices and those associated with the human factor. The chapter begins by introducing the mobile computing security risks' profile.

3.1 Mobile Computing Security Risks' Profile

The growing number 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).

A Provisional Standard (PS 101), titled "Guidelines for a Technical Security Framework for Transmission and Storage of Healthcare Information", by the

American Society for Testing and Materials (ASTM) identifies masquerading, modification of information, unauthorized disclosure of information, denial of service and repudiation as security threats relative to healthcare information (CPRI toolkit). For instance, the British Journal of Healthcare Computing (1994), reported that a nurse was jailed under the Computer Misuse Act of 1990 (CMA) for altering prescription information on a computer. Another report in “The Times” in 1993 stated that a teenager hacked into a cancer patient’s file.

While these threats and attacks were based on a wired environment, they are also practical in a wireless environment. Appendix B shows some of these threats and their impact. According to Microsoft (2004), Humphreys (2000) and Rindfleisch (1997), threats will continue to evolve with overall technological development in computing and networking. Radack (2003), Wiehler (2004 pp.139 – 140), GAO, (2005), Karygiannis and Owens (2003), all state that wireless networks and most mobile devices are vulnerable to many of the same threats as the conventional wired network and they provide greater challenges. Since a wireless network perimeter is not as well defined as it is in the case with a wired network, having a network perimeter firewall is not enough to secure against wireless attacks, nor is it enough in the wired network.

A wired network normally has a fair degree of physical control in the form of guarded buildings and locked offices, and the logical access control imposed by firewalls on the perimeter of the network, and a well structured Demilitarized Zone (DMZ) (Ciampa, 2004, pp. 165 – 166). Although far from perfect, physical access control and network intrusion protection are generally considered acceptable in a wired environment, while attention shifts to protecting data in transit of connected computers (Lee, 2003).

In contrast, mobile computing devices must be assumed to be residing outside of physical access controls and without the presence of electronic access control. Intruders who gain access to information systems, via wireless communications, can bypass firewall protection. Once they have accessed systems, intruders can launch denial of service attacks, steal identities, violate the privacy of legitimate users and track their movement, insert viruses or malicious code, and disable operations (Radack, 2003). The absence of credible physical and electronic access controls makes the risks’ profiles different from desktops.

Although a wired network is regarded as relatively secure, it is important to keep in mind that the network should be reviewed to ensure that there is no exploitable vulnerability that can be used as a medium to attack a wireless LAN (Lee, 2003). The review should include the wire line synchronization and the connection of an imposter or rogue access point to a LAN socket. For example, it would be easy for a visitor or staff to plug a wireless access point into a spare LAN socket, which will provide access to an unauthorized user from a parking lot.

Nevertheless, as mentioned, mobile computing provides unique security challenges over their wired counterparts (Karygiannis & Owens, 2003; Gayer, 2002). Sensitive information that is transmitted between two wireless devices can be easily intercepted and disclosed, if not protected by strong encryption. In addition, there is possible unauthorized physical access to the data and credentials stored in the device memory. Mobile devices, because of their size, can be easily stolen or lost, which eventually, can reveal sensitive information to unauthorized users. Furthermore, users compound issues, by not following safe computing procedures.

Therefore, threats and vulnerabilities can be classified into two categories relating to technical and human factors. The technical factors will further be divided into two sub-categories: one dealing with "Over-the-air access technology" aspects and one dealing with the actual devices. These will be discussed in turn in sections 3.2 – 3.4. The following section begins by discussing the threats and vulnerabilities associated with over-the-air access technologies.

3.2 Over-the-Air Access Technologies

One of the obvious sources of risk in wireless networks is the underlying communication access medium; airwaves can easily be monitored by outsiders and intruders (Results, 2005; RIM, 2005; Gayer, 2002; Radack, 2003; Hayes, 2001).

Section 2.8 identified three varieties of wireless networks: Personal Area Networks (PANs), Wireless Local Area Networks (WLANs) and Wireless Wide Area Networks (WWANs). Each variety uses different access technologies, each with its own peculiarities. The threats, vulnerabilities and attacks associated with each option are discussed accordingly in the subsequent section.

3.2.1 Personal Area Networks (PANs)

Section 2.6.1 defined PANs as networks that enable users to connect everyday devices wirelessly. Examples are connecting digital cameras to printers, and handheld devices to earpieces, resulting in small *ad hoc* networks. There are three different types of PANs, namely: Infrared, Bluetooth and the UltraWideband (UWB) networks.

3.2.1.1 Infrared (IR)

Infrared data allows for point-to-point communication. The technology requires that devices are in a line-of-sight to communicate, allowing the device to directly interface with another device to exchange data (Mitchell, 2005; RIM, 2005). IR is usually referred to as the Bluetooth alternative (HP, 2006).

According to Henzel & Watson (2004), the IR port is a relatively secure means of communication, considering the close physical proximity of the beaming devices, and most devices allow users to control what he or she receives. Some devices have the functionality to disable or deactivate the beaming feature. However, there are numerous accounts of inexperienced users beaming other users far more information than intended, including passwords and other sensitive data (Ottaway, 2002).

While the IrDA Data standard specifies that the communication is in a range of 1 meter, the possible operating range is between 0.2 to 2 meters, depending on the power available (Karty, 2000). It is also possible that whilst a document is being ‘beamed’ to a legitimate receiver, a third party, who happens to be in range and in sight of the infrared emitter, also receives it (Ottaway, 2002). In addition, the IrDA standards do not specify any security measures for data transfer. It can be argued that handheld devices can transmit applications and potentially malicious code through these connections, which likely may affect the integrity or availability of health information (Burrell, 2002).

Furthermore, the transmitted data may be unencrypted, allowing users in close proximity to the device the opportunity to intercept and read the data traversing the connection (DOD, 2005; Burrell, 2002). When data is intercepted and read, privacy and confidentiality of sensitive health information may be violated. IR depends on application-level security to be used to provide encryption and authentication (Ottaway, 2002).

3.2.1.2 Bluetooth

Bluetooth does not have to be in the line of sight of another device (point-to-point) to communicate; in fact, it supports point-to-multipoint communication. Communication in a Bluetooth network can be held between two to eight devices with a transmission capability of one megabyte per second (Henzill & Watson 2004). Devices can be effectively linked in a range of 10 meters (Niem, 2002) but can carry on transmission to a maximum range of 100 meters, depending on the class of devices used (Walsh, Wan & Sadlier, 2005) .

Bluetooth can be used to set-up a peer-to-peer wireless network where there is no centralized database and infrastructure (Karygiannis & Owens, 2003; Blount, 2004, p.6). Devices communicate directly with each other. This means there is no centralized point of security control. An *ad hoc* network is usually formed on the fly, and it is temporary, with shifting network topologies maintaining random network configurations (Juha, 2000; Kumar, 2006, p.5).

In a Bluetooth network, individual devices can act as routers to relay messages to other devices, which are too far apart from the sending device (Bialoglowy, 2005). Furthermore, new devices can discover what services other hosts provide and start using them (Blount, 2004, p. 6). It can be argued that the possible wide range, relay capability and non-centralized security control of a Bluetooth network make it vulnerable to attacks (Edlund, 2005; Ottaway, 2002).

If uncrypted data is sent on a wireless network such as Bluetooth , the data is susceptible to man-in-the-middle attacks (Karygiannis & Owens, 2003; Whitman & Mattord, 2003 p. 68). A man-in-the middle attack involves eavesdropping on the communcation parties to steal identity. Once an identiy is obtained, a perpetrator can masquerade as a legitmate user, send false or altered messages or access system resources. Such an action will violate the privacy, confidentiality, integrity, availability, authenticity and non-repudiation of health information. The violation of privacy and confidentiality is as a result of eavesdropping; integrity, by sending false or altered messages; availability, as a message is modified and not received in the required format; authenticity, by stealing identity; and masquerading and non-repudiation, when information is sent without the knowlegde of a legitimate user.

Furthermore, devices in a Bluetooth network may have no pre-configuration of security mechanisms (Blount, 2004 p.6). Improperly configured Bluetooth devices can provide unauthorized accesses to sensitive information on the device. In addition, unauthorized access into a core network through an *ad hoc* device that is authorized to access the core network is very possible (Karygiannis & Owens, 2003).

According to Wiehler (2004) and Edlund (2005), although Bluetooth provide some level of security support for device level authentication and encryption on transit attacks, it has a level of weakness and does not provide end-to-end security. Edlund (2005) continued that attacks witnessed on a bluetooth network are as a result of implementation issues on a mobile phone platform by manufacturers.

Nevertheless, Shinder (2005) stated that, by listening (eavesdropping) to the initial one-time pairing process an attacker can guess the security settings on a pair of Bluetooth devices. After listening, an attacker can use an algorithm to brute force or guess the security key and masquerade as the other Bluetooth device to access sensitive information. Wiehler (2004, p.143) supported that challenge laid in the initial authentication of the device, where there is a possibility of insecure exchange of secret keys.

Karygiannis and Owens (2003) added that the PIN code required during an initial pairing process, used by internal algorithms to generate a secure key, are very short, making them easy to guess. Bluetooth devices, according to Edlund (2005), Henzill & Watson (2004), Laurie and Laurie, (2003), Layton and Franklin (2006), Walsh, Wan and Sadlier (2005), are vulnerable to attacks such as bluejacking, bluebugging, bluesnarfing, the Backdoor and Warnibbling attack described below.

- **Bluejacking:** A process where an anonymous message is sent to a user, via Bluetooth, requiring the user to react. This, however, does not involve the removal or alteration of any data from the device. A malicious user can issue a deceptive message, like “Click here to win”, to can gain access to someone's Bluetooth device. Devices that are set in non-discoverable mode are not susceptible to bluejacking. This type of attack questions the authenticity of a message.

- **Bluesnarfing**: This process does not alert a device user of the connection made. The connection is not a clear violation of the user's security expectations. It silently allows hackers to gain access to data stored on the device. The information that can be accessed in this manner includes the phonebook and associated images, calendar, and IMEI (International Mobile Equipment Identity) which identifies a phone. This type of attack may violate the privacy of a patient's information, confidentiality, authenticity, integrity and non-repudiation of health information.

- **Bluebugging:** This is a process that allows hackers to access the mobile phone commands via Bluetooth. Like bluesnarfing, it does not notify or alert the phone user silently, giving way to identity theft or impersonation. The vulnerability also allows hackers to initiate and divert phone calls, send and receive text messages, manage phonebook contacts, eavesdrop on phone conversations, and connect to the Internet, via off-the-shelf tools like gnokii. This attack clearly violates user authenticity, message integrity, and non-repudiation.

- **Backdoor hacking:** This process establishes a trust relationship through the "pairing" mechanism, but ensures that the user cannot see the register of paired devices. In the event where a device is no longer trusted, it can still gain access to a mobile phone and its data, as with bluesnarfing, while also using other services as well. The authenticity of a user or device has been violated in this case.

- **Warnibbling:** This is a hacking technique using software, like Redfang or similar, that allows hackers to reveal corporate or personal sensitive information. Redfang allows hackers to find Bluetooth devices in the area. Once found, the software goes through the process of accessing any data that is stored on that device. Clearly, the privacy and confidentiality of information is at risk with this attack.

What is more, Bluetooth devices can also be targets of Denial of Service (DoS) attacks, by bombarding the device with requests to the point that it causes the battery degradation (Shinder, 2005). This attack impedes the availability of information. Finally, there are worms such as Cabir that can use the Bluetooth technology to propagate to other Bluetooth devices.

3.2.1.3 UltraWideBand (UWB)

This technology is currently a standard effort and also referred to as 802.15.3a. Though similar to the current capabilities of Bluetooth, it uses a very different technology (Kay, 2006). It helps deliver television programmes, movies, games and multimegabyte data files throughout our wireless homes and offices (Fleishman, 2003). UWB technology delivers a high data rate, availability of low-cost transceivers, low transmit power, low interference and high security capability (Kay, 2006; Fleishman, 2003).

UWB was designed on the security model used with the current cabled USB. The security model connects the nodes the user specifically wants connected. All data in transit is protected from casual observation or malicious modification. This provides the user the same level of user-confidence for UWB as for wired (Beaver, 2003; Tegar & Waks, 2006).

According to the report by Teger and Waks (2006), the technology has not undergone field testing to discover weaknesses, as was the case with Ethernet, the earlier versions of 802.11 and USB technologies. This has raised security concerns speculating that the single radio approach may turn out to have security gaps similar to those already encountered with 802.11 and Bluetooth.

Furthermore, due to the short-range characteristic, there appears to be no need for periodic rekeying, meaning same keys will be used for a long time. Therefore, in an event where the keys are compromised, there is no limit to the damage a malicious user can perform. So far, there is yet to be a confirmation of a vulnerability in the technology; however, it is important to bear in mind that the security is only limited to data in transit.

3.2.2 Wireless Local Area Network (WLAN)

WLANs act as cable replacements for local area networks, referred to as the 802.11 family. WLANs are very popular and widely deployed by different organizations or industries. The technology is cheap and easy to deploy and these characteristics have influenced its adoption (Ottaway, 2002). However, risks are inherent in this technology.

The built-in security has witnessed negative publicity due to its encryption vulnerabilities and poor authentication associated with Wired Equivalent Privacy (WEP), exposing organizations to security risks (Wiehler, 2004, p.142). In addition, security provided by manufactures is not enabled by default and the interoperability between manufacturers is not very good, consequently introducing security holes (Ciampa, 2004, pp.252 – 253; Ottaway, 2002, SonicWALL, Inc, 2003).

In an effort to reduce the insecurities of WLANs, interoperable standards, called "Wireless Fidelity" (Wi-Fi), have been created to take care of the disparity among manufacturers (Ottaway, 2002). The IETF, IEEE and the 802.11 Task Group (TGi) provided initiatives to improve the authentication and encryption vulnerabilities of WEP.

In order to improve authentication in WLANs, IEEE designed the 802.1x standards, currently adopted by different manufacturers (Karygiannis & Owens, 2003; Ciampa, 2004). For example, the implementation of the 802.1x can be seen in Cisco's LEAP (Lightweight Extensible Authentication Protocol). The protocol provides mutual authentication, based on password challenge response.

However, some of the 802.1x authentication upgrades to control LAN access have also proven vulnerable. For instance, the Cisco LEAP protocol is vulnerable to dictionary attacks, which can be exploited by a tool called "asleap". The tool is capable of capturing authentication information as it travels the network as well as de-authenticate a user. Once the authentication information is captured, the tool can be used to crack the passwords (Cisco, 2004). The fact remains, although 802.1x is a secure standard, the implementation can sometimes be a problem.

More so, in order to address the problem with WEP encryption, the immediate initiative was the introduction of Wifi Protected Access (WPA) using Temporary Key Integrity Protocol (TKIP). This solution implementation is achieved through software drivers and firmware upgrades of existing systems (Karygiannis & Owens, 2003; Ciampa, 2004). However, there are vendor issues, like not releasing the firm or software upgrade in time, lack of proper compatibility or simply requiring to obtain an entirely new device (SonicWALL , 2003).

The second initiative proposed is based on the Advanced Encryption Standard (AES) algorithm to provide a long-term robust solution for the future, also known as WPA2 or 802.11i. Although, the solution requires new hardware and protocol, WPA2 is finely compatible with WPA (Karygiannis & Owens, 2003; Ottaway, 2002; Schroder, 2006). However, it does not provide end-to-end or application-level encryption. The WPA2 only encrypts the traffic between a wireless NIC and whatever wireless access point is being connected to; anything upstream of that is not protected (Herman, 2005; Result, 2005).

Furthermore, most often the limited security measures available on wireless devices are not enabled by default and, in addition, administrators may not properly configure the devices. The Computer Emergency Response (CERT) emphasizes that many ongoing network failures come from failures to configure systems properly and maintain them.

According to Schroder (2006) and Wang (2005), although 802.11 is quickly achieving parity with its wired counterparts, it is susceptible to transmission attacks, such as bandwidth theft, message insertion, forgery, and denial of service attacks. In addition, malicious receivers in range can discover network identifiers, eavesdrop and intercept confidential data, addresses, or logins (Wang, 2005). For example, when the compromised device attempts to connect to the network, the attacker can steal the re-association requests, which contain each client’s Media Access Control (MAC) address and Service Set Identifier (SSID).

With a MAC and SSID, an attacker can impersonate a legitimate device on that wireless network. Such an attack can enable other attacks when a user’s authentication credentials are captured (Slawsby, 2004). The wide proximity enhances such attacks, as it may not be possible to control the distance over which the transmission occurs. Adversaries can, thus, potentially detect transmission from a parking lot or nearby roads (Kumar, 2006; Karygiannis & Owens, 2003). When transmission is detected, attackers can apply cracking tools to gain further access, decrypt message packets, and possibly gain access to the wired infrastructure through the wireless gateway. The next section looks at some possible attacks on WLANs.

3.2.2.1 WLAN Attacks

According to Blount, (2004, p. 61), Kumar, (2006, pp. 11 – 13), Karygiannis &

Owens, (2003) and Result (2005), there are basically two types of attacks: passive and active. A **passive attack** is a type of attack where unauthorized parties gain access to information but do not modify its content. Examples are eavesdropping, traffic flow analysis or surveillance. Conversely, an **active attack** is a situation where an unauthorized party makes modifications to a message, data stream, or file. These attacks include:

- **Eavesdropping/Sniffing:** This is a process that monitors transmissions of message content. For instance, someone listens into the transmissions on a LAN between two workstations, or on a WWAN by tuning into transmissions between a wireless handset and a base station. This, as shown in section 3.2.1.2, can compromise the privacy and confidentiality of health information. In addition, privacy may be compromised if the broadcast address of a wireless device is captured and is associated with a particular user. Once the address is associated with a particular user, that user's activities could be logged, resulting in a loss of privacy. The success of such an attack paves the way for subsequent attacks, which can be detrimental to an organization.

- **Surveillance and Traffic Analysis**: These two go hand-in-hand. The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. An attacker can gain information about users and the network including user ids, passwords, and other sensitive information. These attacks, as well as eavesdropping, provides the possibility of replay attacks where the attacker monitors transmissions and retransmits messages as the legitimate user. This attack clearly compromises the authenticity, privacy and confidentiality of the user's personal or heath information. This attack can also lead to non-repudiation.

- **Masquerading/Impersonation/Spoofing:** The attacker pretends to be an authorized user and thereby gains certain unauthorized privileges. Much as discussed in section 3.2.1.2, intruders can setup imposter wireless clients or unauthorized access points, usually known as rogue access points using the information gathered by probing and surveillance tools. With the identity of valid users and an access point, the intruder can gain access to the network, or gather additional information about authorized wireless users.

Rogue Access Points (AP) can be installed by employees or visitors to ports in the wired networks, allowing unauthorized connections into the networks. If a rogue (imposter) device is in close proximity to the users of a WLAN or *ad hoc* network, and it is configured to appear as a legitimate AP or mobile device to wireless clients, then the rogue AP or handheld can successfully convince wireless clients of its legitimacy. The rogue AP or device can now intercept the wireless traffic between an authorized AP and wireless clients, as such violating the privacy of users and confidentiality of information.

- **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it. Usually an attacker hijacks a user session, and then takes over the existing connection and effects changes to information in transit. Here, integrity of sensitive health information is violated.

- **Denial-of-service:** Ensuring the availability of information is crucial, because without timely information an organization would be incapable of continuing normal operations. In wireless networking, denial of service is more likely to occur than in the wired environment. The attacker prevents or prohibits the normal use or management of communications facilities. DoS attacks can block (jam) network access completely or severely degrade network performance and client system performance making it unavailable to legitimate users. This attack clearly affects the availability of health information.

- ***Ad Hoc* Networks:** Bluetooth or infrared networks may have connections, via devices, to 802.11 networks and also to Wide Area Networks. In that case, 802.11 will be subject to the vulnerabilities associated with *ad hoc* networks.

Although the attacks discussed above are common in WLANs, they are not confined to WLANs alone. These attacks can also be carried out on WWANs, as will be highlighted in the next section. The next section discusses some security threats and vulnerabilities associated with WWANs.

3.2.3 Wireless Wide Area Network (WWAN)

As mentioned in section 2.6.3, WWANs provides a great platform for business; however, they possess a growing number of security concerns (Ottaway, 2002;

Niemi & Kagranen, 2005). For instance, the built-in security system of GSM focuses on the radio path only. The security architecture uses a weak 64- bit algorithm to encrypt voice over-the-air and provides no encryption support for SMS messages (Wiehler, 2004, pp. 140 – 146; Ottaway, 2002). Furthermore there are no integrity checks and user authentication does not prevent man-in-the-middle attacks (Wiehler, 2004).

According to Niemi & Kagranen (2005), as GSM and other 2G networks become increasingly successful, the necessity of the basic security needs becomes more evident. This has been a leading principle in the specification work of the UMTS security to carry the GSM features over to the new system. In UMTS, counter measures have been developed for the vulnerabilities associated with the GSM network.

Although the CDMA 2000, another aspect of the 3G cellular systems used in the US, is inherently secure (Herman, 2005), the improved GSM and the CDMA networks' security are only focused on the radio path (Niemi & Kagranen, 2005; Herman, 2005). The "radio path" or "air interface" is the open-air transmission of information between a wireless device and the service provider's network. The high level of security (encryption and authentication) built into the transmitting technology does not provide end-to-end security. Network elements, such as the cell phones PDAs and devices within the service provider network, are left vulnerable to threats (Herman, 2005). Therefore, it can be argued the 3G networks are not entirely secured.

Furthermore, the network is susceptible to attacks, such as social-engineering, eavesdropping, spoofing, session hijacking, and denial of service (Wiehler, 2004, pp. 122 – 123; Niemi & Kagranen, 2005). Social-engineering on its own is not an attack, but a process that aids an attack. It is a process that requires practically no technical ability but is highly effective. It relies on tricking or deceiving someone to access a system (Ciampa, 2004, pp. 35 – 36).

According to Niemi & Kagranen (2005), social engineering for subscribers means ways of gaining access to their terminals. It is not infrequent for people working with network elements in an operator's premises to receive calls requesting a user ID or password of some equipment in the pretence of the legitimate user being unreachable. This clearly compromises the authenticity of a user.

As mentioned earlier, mobile devices on their own are at risks of attacks. The next section discusses some of the threats and vulnerabilities associated with these devices.

3.3 Mobile Devices

Mobile devices today are much closer in features and functionality to personal computers than their single-function cellular phone and PDA ancestors (Slawsby, 2004). These devices share several common vulnerabilities, regardless of their model or platform. According to Wiehler (2004, p. 144), Karygiannis and Owens (2003), Ottaway (2002) and Symantec (2006), mobile devices provide additional security concerns in a ubiquitous computing environment such as the following:

- The small size and portable nature make them more likely to be stolen or lost.
- Employees often purchase and use mobile devices without notifying the organization.
- Wireless handheld devices are often used for both personal and business data. Users that purchase these devices on their own often do not consider security implications of their use in the work environment.
- Many users have limited security awareness or training with the use of handheld devices and are not familiar with the potential risks introduced by these devices.
- Mobile capability to download a number of programs, such as games and utilities, including freeware and shareware programs from untrusted sources. These downloads may contain Trojan horses or other malicious code that can affect the user's mobile device, the user's PC through synchronization, or the organization's network resources.

As discussed in Chapter 2 section 2.4, nowadays, mobile devices are shipped from the factory with multiple communication ports such as infrared, Bluetooth, 802.11 and GPRS providing the possibility of transmitting sensitive data over a variety of wireless networks. However, the transmission capability is achieved with little or no security, which can provide an opening for unauthorized users to exploit. For example, a mobile device that connects over WiFi, Bluetooth, or other non-secured means can become infected with a virus or worm, and that infection may try to propagate when the mobile device reconnects to the wireless service provider's network.

Mobile devices' vulnerabilities can be divided into two categories namely, mobile hardware and mobile software. The mobile hardware is composed of the mobile device itself, its accompanying underlying access or communication technology. The latter encompasses the vulnerabilities associated with the software and application that run on these devices.

3.3.1 Mobile Hardware

As caregivers increasingly become mobile, clearly, the potential for the storage of sensitive health data on mobile devices is high and growing (Eastwood, 2006; Symantec, 2005). Fresh and critical data may reside on an employee workstation (laptops, PDAs, Smartphones, memory sticks), not servers.

A worldwide survey conducted by Pointsec among 73 IT managers, with 34% coming from companies with over 1,000 employees, shows that workers store huge amounts of sensitive data on their mobile devices. The sensitive data includes customer contacts, e-mails, passwords and bank account details, as well as personal and private information such as friend's details, personal images and even PIN numbers, without giving much consideration to security (Ravindran, 2005; Symantec, 2005).

According to Slawsby (2004), the improved functionalities and features of the new mobile devices influence such behaviour. Apart from the database of business contacts and appointments, a wide range of new functionality, such as email attachment viewing, office document editing and file storage, makes it rather possible that these devices may hold even more sensitive data within their memory. Although improving the features of mobile devices is a good thing, these devices are frequently used in public places, providing opportunities for unauthorized access, as well as theft or loss.

3.3.1.1 Theft and loss

When a device is lost or stolen, an organization is most likely to suffer the exposure of confidential or private data than monitoring transmission to and from the device. When a device falls into the hands of an unauthorized person, he or she will have enough time to get to the data on the device. In addition, the organization is at risk from the loss or misuse of information stored on the device or its removable storage card (Ravindran, 2005; Good, 2005). This action may affect the availability and integrity of information.

Unless a means is developed to avoid loss and theft, the threat is not likely to go away any time soon (Hickey, 2005). According to Symantec (2005), careless employees pose a bigger threat than criminals operating online, as they also frequently lose their devices, which, at the very least, hold e-mails carrying business data.

A survey by mobile security specialist Pointsec revealed that 63,135 mobile phones, 5,838 PDAs and 4,973 laptops were left in the back of London taxis in the last six months of 2004 (Eastwood, 2006). Furthermore, a report by O'Brien and McKinnon (2006) from the Australian IT news stated that a memory stick containing classified information was misplaced by the Australian High Tech Crime Centre between Sydney and London in the middle of an investigation.

The memory stick contained records on "phishing" scams by Russian mafia, as well as banking details of 3,500 customers from 18 Australian banks, including names and account numbers. The data on the memory stick, however, threatened to reveal details of police inquiries into the organized crime networks. The memory stick was not protected in any way; as such, the information stored could be accessed by merely plugging it into a computer.

According to Slawsby (2004) and Good (2005), if users do not protect their mobile devices with basic security mechanisms as passwords, then data stored on these devices becomes susceptible to unauthorized users. Ravindran (2005), states that this can have a huge impact on customer confidence and cause an organization to breach data protection legislation or ruin the organization's reputation. Lost or stolen mobile devices can cause more financial loss than malicious attacks from outside an organization (Symantec, 2005). As loss and theft requires only physical access without any special skill, an organization is more likely to suffer the exposure of sensitive data through loss and theft than from someone monitoring transmissions to and from a device.

3.3.1.2 Interception and Intrusion

As mentioned in the previous sections, mobile devices entail the use of wireless networks with varied channels of data transmission. An organization's sensitive data flows to and from a mobile device, via these channels. Although solutions exist to ensure the security of these channels, they are either not enabled or are inadequate. Therefore, insecure transmission of information is typical, paving the way for man-in-the-middle attacks.

In a successful man-in-the-middle attack, an attacker is able to read, insert and modify messages between two parties, without either party knowing that the link between them has been compromised. Such an attack can enable other attacks when a user's authentication credentials are captured. Furthermore, ubiquitous wireless connectivity provides fertile ground for remote intrusion into devices themselves. Mobile device hackers can target devices in order to launch larger attacks on organizations' networks (Ciampa, 2004, pp. 47 – 48), with the intent of accessing critical health information or hampering healthcare activities.

In addition to malicious attacks, integrity may be compromised because of radio interference or other natural disturbances (Juha, 2000), so some kind of integrity protection is definitely needed in the mobile environment.

3.3.1.3 Location Aware Devices

According to Jason (2003) and Ottaway (2002), location aware technology, such as Global Positioning Systems (GPS), is available on mobile phones. The technology allows mobile phone companies, network providers and possibly others to determine exactly where the phone, and probably the user, is anywhere in the world. GPS-enabled phones can identify the phone's location to within a few meters and also relay the user's position information. In the case of an emergency, e.g. injury or assault, a user can relay his location to the proper authorities for help.

Other cell phone companies use a technology, called triangulation, to find a missing person or a criminal (News8austin, 2005; Hyrkas & Paunonen, 2005). Their equipment can triangulate or map out when a cell phone is on, and where an individual can be located. This location is based on the signal strength between the phone and a cell tower. Although the location capability is a good thing, it is sometimes considered illegal or unethical, as it may give away the position of an individual who wants his or her privacy.

While there are certain security issues associated with mobile device hardware itself, the software that runs on the devices is not secured, and is also susceptible to attacks. The next section discusses some of the threats and vulnerabilities associated with device software.

3.3.2 Malicious Mobile software (Malware)

In the past, there existed malicious codes that sent files to random addresses, and other codes that captured passwords and sent them to the creator of the program. It was only a matter of time before the use of malicious codes became a serious problem, and attackers began to target mobile devices (Ottaway, 2002). According to Brookson (2005), now mobile devices are faced with the same threats as PCs. The robust and deep application capability of today's mobile device platforms make them easy targets for malicious codes to enter an organization's internal network and computer systems (Ranger, 2005).

The Symantec Internet Security Threat Report Volume IX (2006a) showed that the threat landscape is increasing, dominated by attacks and malicious code that are used to commit cyber crime. The report highlighted that malicious code that targets mobile devices, particularly smart phones, has continued to grow through the second half of 2005. The report also highlighted several new examples of malicious code for smart phones, including Cardtrp, the first cross-platform threat with the ability to affect both Symbian and Windows-operating systems.

A virus report by Shevchenko (2005) stated that in June 2004, a proof-of-concept worm, called Cabir, was discovered for the Symbian 60 operating system. The Cabir worm sends itself, via Bluetooth, from an infected Symbian Series 60 smart phone to other devices, including printers and any Bluetooth-enabled device. This was merely to demonstrate possibilities of attacks. However, in August 2005, Commwarrior.B became the first virus to infect all of the smart phones belonging to a company (Virusoffice, 2005).

The common vulnerabilities with these devices could be missing critical operating system patches, application patches or antivirus software (Karygiannis & Owens, 2003; LANDesk, 2005). Usually a problem arises as a result of out-of-date signature files or simply missing or misconfigured personal firewalls. Malicious codes, in this case, are like those found on desktop computers, because mobile devices can be used for email and file sharing in a similar way. A malicious code can be in the form of a virus, worm or Trojan-Horse as described below (Ciampa, 2004 pp. 48–52; Slawsby, 2004; Wang, 2005):

- **Viruses**: This is a type of software program which secretly attaches itself to a document or script, depending on an action initiated by a user on the document to execute or propagate. Actions, such as opening the document or running a script, can cause the virus to execute and propagate. A virus can contain instructions, such as displaying annoying messages, erasing files from a device or causing a device to crash, hence, compromising availability. A virus can replicate itself and spread by inserting copies of itself into executable codes or documents, which violates the integrity of the content.

- **Worms**: A worm is similar in nature to a virus, but does not attach itself to a document and does not necessarily depend on a user-initiated action to be executed. A worm can travel by itself, but is frequently distributed via email. It is a self-replicating computer program that can clog available resources, such as device memory or bandwidth connection. A worm can be designed to delete files or send documents at will.

- **Trojan Horses**: These are malicious programs that disguise themselves as legitimate ones. This program reveals itself when activated. Once installed on a device, it can open up a backdoor for an unauthorized user to perform harmful activities.

Mobile devices can influence the dissemination of malicious codes in two ways. Firstly, the malicious code may execute on the device itself, so that it becomes unusable or causes service disruption (availability). Secondly, it can become another avenue for malicious codes to be executed on another computer, when an infected file is transferred into the network.

These infections are usually downloaded or distributed via an email attachment or file transfers through the infrared port (“beaming”) or over a Wi-Fi connection in a hotspot (Good, 2005). Mobile devices can connect via a range of networks, including GSM, GPRS, UMTS, Wi-Fi or Bluetooth; a virus can enter the device or network using one of these communications paths. Figure 3.1 shows some of the malicious code delivery vectors for mobile devices.

A 2005 survey, derived from nearly 600 US-based IT professionals by Good

Technology, showed that e-mail is the greatest source of risk, followed by organizations' intranet applications. 79% of respondents consider e-mail to be the greatest source of security risk among the applications deployed on mobile devices. Following, 26% regarded an organization's intranet applications as having the greatest vulnerabilities (Thayer, 2005).

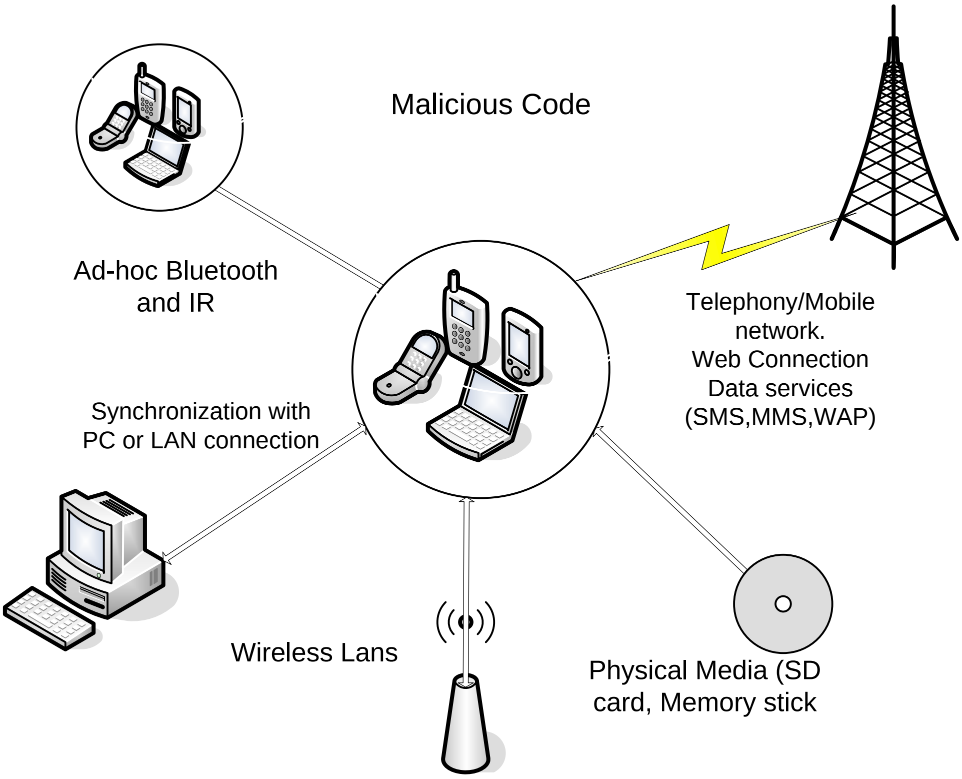
Malicious Code
Ad-hoc Bluetooth and IR
Telephony/Mobile network.
Web Connection
Data services (SMS,MMS,WAP)
Synchronization with PC or LAN connection
Wireless Lans
Physical Media (SD card, Memory stick

Figure 3.1 Malicious Code Vectors for Mobile Devices

According to Ranger (2005), hackers have discovered ways to embed malicious codes in pictures in order to attack a number of different applications used to render images. Clicking on an infected image could set off a virus or worm without the user's knowledge. Appendix B summarizes some of the threats, vulnerabilites and attacks associated with mobile devices and shows their impact on privacy, confidentiality, intergrity, availability, authenticity and non-repudiation.

However, risks associated with mobile computing are not subject to technology alone; users can also pose a threat. When people use information systems, mistakes sometimes happen (Whitman & Mattord 2003, p. 44). Inexperience, improper training and making incorrect assumptions can cause mishaps resulting in catastrophic consequences. Furethermore, some users may have malicious intents. The next section looks at how the human factor affects mobile computing.

3.4 Human Factors

Any network is only as secure as it weakest point (Wang, 2005, Whitman & Mattord, 2003). According to Hickey (2005), human error is still the biggest threat to valuable information stored on mobile devices. Factors like how well the users secure their own devices become critical (Wang, 2005). Employees and partners, such as insurers and pharmaceutical payers, accessing or receiving they may not handle it according to specified security standards (Rindfleisch, 1997). This may lead to the violation of patients privacy and confidentiality of their information.

Internal users with authorized access to computing resources can pose more danger than external users, who must breach a perimeter firewall to get inside the network (Kurtz, 2004; LANDesk, 2005; Symantec, 2005). Sometimes out of curiosity, medical personnel may abuse their privileges, perhaps out of concern for a family member or employee or loved one to find out their medical status.

Furthermore, users may frequently make errors that will contribute directly or indirectly to security problems. In some cases, an error can be a threat, such as a data entry error or a programming error that crashes a system (NIST, 1996). In an event where things go wrong, it icannot be blamed on the carelessness of an employee alone, but also on the organization not putting the right policies in place and enforcing them (Eastwood, 2006).

In many organizations, the greatest security threat comes from the mobile phones and handheld devices owned by employees (Friedlander, 2004; Karygiannis & Owens, 2003). Users often bring in their own devices without following proper procedures to validate the devices. These devices, originally purchased for personal use, slowly infiltrate into the organization's infrastructure. Employees can connect mobile devices to their machines, using desktop synchronization tools, and extend management of an organization's resources to the devices (Slawsby, 2004). In addition, the devices can be difficult or impossible to upgrade or have relatively few or no security patches released for mobile device platforms, making them vulnerable to malicious code (Friedlander, 2004).

What is more, a user with malicious intent can take advantage of the trusted user, saving him the trouble of penetrating an organization's perimeter firewall or application gateway (LANDesk, 2005). Moreover, it can be an easy target for a hacker, as authorized users potentially load sensitive information onto personal devices. According to Friedlander (2004), even if an organization has policies regarding mobile device usage, users often have a significant degree of control over what data and files are carried on mobile devices**.**

3.4.1 Employee sabotage or espionage

Other than hackers or crackers carrying out fraud or theft, authorized users are most likely to carry out such acts (Coleman, 2005; NIST, 1997; Symantec, 2005). Sometimes some users try to get around a system to engage in fraudulent activities or simply to avoid inconvenience (Kurtz, 2004; IDC, 2004). According to the National Research Council (1997), electronic health records are possibly liable to exploitation from both authorized and unauthorized users, who inappropriately access patient information for their private or monetary gain.

On the one hand, according to Kurtz (2004), while the majority of fraudulent activities are attributed to external exploits of mobile devices, part of these activities could be from internal employees or partners manipulating their mobile network weaknesses. Partners who have access rights to patients information for the purpose of primary care may exploit that access for other unauthorized purposes (Rindfleisch, 1997). Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud or theft. In addition, user activity logging in an organization can be exploited by both intruders and employees with malicious intent.

On the other hand, according to Friedlander (2004), executives and knowledge workers can circumvent policies or even technology, especially if it inconveniences them. Circumvention of security controls is usually caused by lack of education and training of users. These users are the most likely to bring their own devices into the organization, and they also frequently handle sensitive information. Therefore, an effective supervisory and legal structure that will sanction against detected misuse is required.

3.5 Conclusion

In this chapter, the threats and vulnerabilities associated with mobile computing were identified. The risk areas were broken down into three categories covering wireless or over-the-air technologies, the mobile devices themselves and their software and human factors.

It can be concluded that mobile computing threats range from technical and human operational perspectives and will continue to evolve. Attacks in a mobile computing environment can be performed using the same general techniques that are used to compromise the wired environment. Attackers may break into the network to steal, destroy information, or to render the system dysfunctional, preventing legitimate users such as doctors and nurses from accessing information critical to care.

In addition, authorized users or partners may take advantage of their legal authority to access information that they have no legitimate need to see, or reveal patient information to others often without the patients' agreement. Sometimes, security negligence on the part of a legitimate user can cause detrimental problems to an organization.

The attacks associated with the threats and vulnerabilities of mobile computing provide greater security challenges and negatively impact on the confidentiality, integrity, availability, authenticity, non-repudiation and privacy of sensitive health information. Fortunately, there exist measures that can help protect these components of information security from accidental or malicious attacks. The next chapter focuses its discussion on the technical security measures that aim to protect the privacy, confidentiality, integrity, availability, authenticity and non-repudiation of information.

Chapter 4
Security Countermeasures for Mobile Computing

When extending healthcare applications and sensitive information to mobile devices, it is important to maintain the same level of performance, privacy and security that users have become accustomed to within their organization's walls.

In the previous chapters it was discussed that wireless channels, ranging from infrared, Bluetooth, WLAN and WWAN, represent the conduits through which sensitive health information may flow to and from a mobile device. Although these channels have security measures in place to ensure security, these measures are limited. Furthermore, the ubiquitous nature of mobile computing provides opportunities for remote intrusion into mobile devices themselves, providing high risks to healthcare organizations.

Fortunately, technologically-based mechanisms and services necessary to secure mobile devices' access to the organization network and their resident data exist. Among these mechanisms are authentication protocols, antivirus protection, intrusion prevention, message integrity checking, firewall capabilities and data encryption. These technical countermeasures involve the use of hardware and software solutions to help secure wireless networks and mobile devices.

By implementing these mechanisms, organizations can protect their data and communications. The key objectives of the countermeasures are securing sensitive data stored on the remote devices, ensuring that the devices attempting to access the organization's network are legitimately authorized to connect, protecting devices from exploits of malicious code and protecting data in transit against eavesdropping or data theft. The subsequent sections will discuss in more detail these technical countermeasures.

4.1 Protecting Authenticity

Authentication provides a means of confirming the identity of a user, a system or an application. It provides proof that a party is who he or she claims to be (Weiler, p. 128, Ciampa, 2004, pp. 78–88). User authentication is a common first line of defence, ensuring that only authorized users can gain access to system resources (Karygiannis & Owens, 2003; Whittaker, 2003; Lindstrom, 2001). Before a user can access a system, the user must present credentials to prove he or she is indeed who they say they are. After a user is authenticated, access to services he or she requires is granted (authorization) and a user's activities can be monitored (accounting).

According to Kay (2005) and Ciampa (2004, p. 78), authentication can be done in three ways. Firstly, "something the user knows", which is based on knowledge committed to an approved user's memory, e.g., a password or personal identification number (PIN). Secondly, "something the user has", which is similar to the first, but only this time the authentication details are placed on a device a user possesses, such as a security token, smart card or a certificate. Thirdly, "something that a user is or part of a user", which is achieved based on the unique characteristic of the user to authenticate the individual, e.g., fingerprints or voice samples, referred to as biometrics.

However, it is possible for a system to use a combination of these methods to verify identity, referred to as multifactor authentication. To protect valuable assets, like sensitive health information, a multifactor authentication is usually advisable (Ciampa, 2004; Dedo, 2004b).

In mobile computing, authentication can be considered at three levels: the device, the network and the remote authentication. The following section further discusses these levels of authentication in detail, beginning with device authentication.

4.1.1 Mobile Device Authentication

Usually, the first level of authentication involves accessing the device itself. Caregivers, at the point of care or remotely, will access and write directly to mobile devices at that point. The devices need to be able to verify that the person attempting to access them is a legitimate user (Dedo, 2004b). The three subsections below illustrate how mobile device authentication can be achieved, beginning with "what a user knows" in section 4.1.1.1, "what a user possesses" in section 4.1.1.2 and "what the user is" in section 4.1.1.3.

4.1.1.1 Something the user knows

As mentioned in section 4.1, one form of authentication is the use of **passwords** or **pins.** This is a popular approach of authentication employed in many Information systems adopted on mobile devices (Zeisz, Keil, & Lee, 2005). Today's mobile devices come with power-on password authentication to prevent unauthorized users from gaining access to the devices and any networks accessible by these devices (Karygiannis & Owens, 2003; Dedo, 2004b). Users set a password that must be entered before the device can be accessed. When relying on usernames and passwords for authentication, it is important to have policies specifying minimum password length, required password characters, and password expiration.

There are installable, managed security solutions available that allow administrators to enforce authentication protection and policies (Dedo, 2004b). These mandate requirements, such as length and type of password, frequency of password change and timeouts, as well as control encryption and application access.

Managed security solutions protect against brute-force password attacks and usually come with data-wipe functionality. For instance, a third party solution, PointSec, intervenes at a mobile device boot start-up process to prevent any access to the operating system prior to user authentication. The solution allows an administrator to offer a choice of passwords, numeric pins, picture pins, smart cards and biometrics for authentication.

4.1.1.2 Something the user possesses

This section looks at the use of **smartcards** as a form of authentication. In general, smart cards are tokens that can be used in a whole range of organization security applications (Wiehler, 2004 p. 129). These application scenarios include admission control for buildings and rooms, cashless staff restaurant payment and user authentication for applications.

These media are portable, standardized and exchangeable among different devices, which means that users carry their private keys with them like a credit card and can use them with various devices. User certificate and additional information are stored on the cards and generally require the user only to remember a PIN number (Karygiannis & Owens, 2003).

In wireless networks, smart cards provide an added component of authentication. Like authentication software, these tamper-resistant devices can be integrated into a WLAN solution to enhance the security of a system. Smart cards are advantageous in environments requiring authentication beyond a simple username and password combination (Karygiannis & Owens, 2003; Sadlier, 2003).

Smart cards tamper-resistant chip technology implies hardware and software protection measures, which represent a very high security level (Wiehler p.129). According to Sadlier (2003), when smart cards are kept separately from the mobile device, the risk of losing both at the same time is low. This ensures that anybody who comes into possession of the mobile device, that requires a smart card, will be unable to use it.

4.1.1.3 Something the user is or part of the user

This aspect of authentication method, as described in section 4.1, is referred to as **biometrics**. Biometric authentication combines convenience with strength. A variety of biometric authentication methods, such as voice recognition and fingerprints are available for mobile devices (Boertien & Middelkoop, 2002; Maltoni & Jain, 2004). Some of these devices have the capability to set authentication limits to optimize data security. The optimization feature is meant to lower the number of false positives or to minimize a user's legitimate chances of being falsely rejected (Ciampa, 2004, p. 348).

Device authentication protects an organization's data and network access in the event of theft. For example, a fingerprint reader can be attached to a handheld device through a serial or USB port and can be set to lock the whole device or lock an individual application. As mobile devices are more difficult to secure physically, it is important to ensure that if an unauthorized person gains possession of the device, they will not be able to activate it. Biometric authentication can be used in combination with the other authentication methods to provide an added layer of protection to devices (Karygiannis & Owens, 2003). For example, fingerprint and voice recognitions can be combined with a public key cryptography system on a smart card.

However, authentication at device level alone is not enough to secure health information that traverses the wireless network; therefore, it is imperative that authentication is considered at the network level. The next section discusses wireless network authentication.

4.1.2 WLANs' Network Authentication

This section focuses on the devices to WLANs access. WLANs' security can be categorized in three areas namely: "what the device is", such as a device-unique identifier, MAC or Hardware Serial Number (HSN), "what the device possesses", such as SIM cards and digital certificates and "what the device knows", such as SSID, WEP keys. Each of these is discussed in the following section.

4.1.2.1 Something the device is

This section discuses the use of **device-Unique Identifiers** as a form of authenticating a device**.** A unique-device identifier, like a Media Access Control (MAC) address of an approved wireless device, can be entered on an access point. Only those devices with approved addresses are allowed to connect to the wireless network. This process is referred to as MAC filtering (Ciampa, 2004, p. 251). According to Karygiannis and Owens (2003), unique-device identifiers can be used as part of an authorization mechanism to authenticate and provide network access to a handheld device. In addition, they state that mobile devices can take advantage of several methods to identify a unique device, including flash ID, device ID, and Electronic Serial Number (ESN), as will be shown in subsequent sections.

However, using this factor of authentication alone is not enough, as these unique identifiers can be spoofed (Ciampa, 2004; Edlund, 2005); hence, a multifactor authentication is required.

4.1.2.2 Something the device possesses

In this section the **Subscriber Identity Module (SIM)** and **Digital Certificates** respectively are described as something the device possesses.

Subscriber Identity Module (SIM)

Currently, GSM (Global System for Mobile Communications) operators provide a Subscriber Identity Module (SIM) for each subscriber on their network. The role of the SIM is to authenticate the user on the GSM network and to facilitate effective billing (Ahmad, Chandler, Dharmadhikari, & Sengupta, 2003). This form of authentication has been extended to WLANs. Wireless LAN access can be authenticated and charged with the GSM SIM (Ala-Laurila, Haverinen, Mikkonen, & Rinnemaa, 2002; Tsai & Chang, 2003). With a Bluetooth network or a SIM reader attached to the computing device, an authentication server, via an EAP-SIM protocol resident on a device, can use the SIM credentials for authentication. The EAP/SIM also enhances the basic GSM authentication mechanism by providing mutual authentication, not only one way. Like the smart card, the SIM is a tamper-resistant device in which the access credentials of a mobile network subscriber can be securely stored.

However, using cryptanalysis, hackers can find a way to calculate the value of the secret data by analyzing a huge number of command-response pairs. According to Ahmad et al. (2003), the risks of such attacks are relatively low since the cell phone is "closed" to the outside world and also depends on the weakness of the cryptographic algorithm used. The next section discusses how authentication is achieved on a device using digital certificates.

Digital Certificates

Digital certificates play an important role in securing wireless local area networks (WLANs) (Phifer, 2006). Protocols to secure WLANs using digital certificates include the most popular EAP types which are EAP-TLS, EAP-TTLS and PEAP (Ou, 2005; Phifer, 2006). Mutual certificate authentication can be achieved using EAP-TLS, which requires clients and servers to provide certificates for validation by each other after a TLS session is established. The EAP-TTLS and PEAP provide one-way authentication where the certificate is provided by the server only. Using a client certificate is possible with EAP-TTLS and PEAP to provide mutual authentication, but it is optional. Appendix C section C.3 provides more information about the use of digital certificates. The next section looks at WLANs' security, based on what a device knows.

4.1.2.3 Something the device knows

In this section the **Service Set Identifier (SSID)** and **Wired Equivalent Privacy (WEP)/ Wi-Fi Protected Access (WPA)** respectively are described as something the device knows

Service Set Identifier (SSID)

One of the basic WLAN securities is based on the Service Set Identifier (SSID), also referred to as the network password (Ciampa, 2004 p. 250). Each WLAN is given a unique SSID, which is required for any device that wants to connect to the WLAN. However, because of the vulnerability associated with access points as they broadcast, the SSID, which can be picked up by an unauthorized user, should be entered manually on each device. This configuration avoids broadcasting SSIDs to clients. However, gaining access into the network by just knowing an SSID depends on how network administrators have configured their WLAN, particularly WEP, security (Mitchell, 2006).

Wired Equivalent Privacy (WEP) / Wi-Fi Protected Access (WPA)

WEP can be used for authentication. When a wireless device attempts to connect to a WLAN, an AP sends the device a challenge text. The device encrypts the challenge text with its WEP key to return it to the AP. The AP compares the encrypted text to its own encrypted version of the challenge text using its WEP key. If there is a match, then the device is authenticated.

However, as discussed in section 3.3.2, WEP has some vulnerabilities. In order to correct WEP vulnerabilities, IEEE ratified the WPA, the interim standard that strengthened WEP authentication, and Wi-Fi Protected access (WPA) improved WEP security by using the 802.1x authentication and the temporary Key integrity Protocol (TKIP) encryption and message integrity checks (Ciampa, 2004, pp. 254 – 255). The next section discusses the 802.1x technology in detail.

4.1.2.4 802.1x

802.1x is an IEEE standard that defines how to identify a user and grant a user access to a network. 802.1x is a Layer 2, authorization protocol that defines how a user is granted port-based access to a network (Cisco, 2006a; Ciampa, 2004; Simpson, pp. 280 – 283). To support 802.11 LANs, a security solution, based on the IEEE 802.1x standard, is a good start (Karanam, 2006; Blount, 2004, p.64). 802.1x uses EAP (Extensible Authentication Protocol) to authenticate between a wireless device and an access point before a device can access the WLAN. In addition, 802.1x uses automatic key rotation to solve WEP's key reuse issue (Karygiannis & Owens, 2003).

As mentioned before, some the most popular EAP types are PEAP, TLS, TTLS and, notwithstanding, LEAP. Cisco's LEAP (Lightweight EAP), based on the 802.1x standard, enforces mutual authentication between a client and an access point, based on password challenge-response. LEAP addresses the WEP key reuse weakness by exchanging dynamic WEP keys.

Since LEAP was specifically designed to be “lightweight” in processing usage, it is particularly well suited to mobile devices. LEAP addresses the security vulnerabilities of WEP (Pereira, 2001). However, because of LEAP’s reliance on password authentication, it is susceptible to dictionary attacks (Cisco, 2005, p. 74), fortunately, the vulnerability can be countered by limiting failed password attempts at the server. For devices which do not support LEAP, TLS/SSL+ encryption over an 802.11 wireless link, combined with a login to the backend clinical data, can be used (Sutherland & Madrid, 2003). Better still, they use EAP PEAP, TLS, and TTLS that allow the use of digital certificates.

802.1x blocks traffic on a port-by-port basis until the client is authenticated, based on information contained in authentication servers, such as RADIUS, TACACS or similar type servers (Karygiannis & Owens, 2003; Sutherland & Madrid, 2003). The RADIUS server can be used in conjunction with Windows Active Directory and other major network operating systems to provide authentication. In a situation where a user needs to transmit information over multiple networks, VPNs may be used to provide another layer of security over 802.1x-based solutions. 802.1x authentications can be used then to allow only authorized users to establish a VPN connection to an organization’s network. As caregivers come with the need to remotely access their organization’s network, it is imperative that this is done securely. The next section discusses remote authentication.

4.1.3 Remote Network Authentication

In addition to being authenticated on mobile devices, many healthcare applications may require the user to authenticate to remote systems. Authenticating a transmission to ensure that it comes from an approved sender provides an increased level of security for remote access users (Ashley, 2006; Blount, 2004).

An organization’s networks and servers will require users to authenticate with a username and a secret and/or unique identifier before access is granted to resources. Server authentication allows users to confirm they are indeed talking to a legitimate server and not a rogue one masquerading as a legitimate server. As patients pay for services rendered, server authentication should be used in transactions where the user is providing sensitive information, such as a credit-card number.

According to Ciampa (2004, p. 235), RADIUS and other similar servers are also designed to support different types of remote connections. The RADIUS protocol manages remote authentication and authorization. It supports authentication protocols, such as PPP PAP, CHAP, MS-CHAP, MS-CHAP v2, and EAP (Parker, 2005; Ciampa, 2004, p. 233). Mobile devices come with support for the use of these protocols (Dedo, 2004b).

As witnessed in the previous sections, EAP is a flexible authentication ‘framework’ allowing for different authentication protocols and methods, such as smartcards and certificates, in addition to username and password credentials. This capability makes it possible for users to connect to remote databases or applications over a wireless network when authentication is done via these means (Karygiannis & Owens, 2003). Also, these methods can be used together to provide strong authentication to the network (Wiehler, 2004 p. 148).

Furthermore, for a server to prove its identity, the server can use Secure Socket Layer/Transport Layer Security (SSL/TLS) to send a digital certificate, signed by a certificate authority, to a user or device (Robinson, 2001). The TLS provides server authentication, confidentiality, and integrity (Wiehler, 2004 p. 158). A user authentication protocol authenticates the device to the server. Unique-device identifiers can be used to authenticate a mobile device for access. Appendix C discusses more on digital certificates and certificate authorities.

According to Elbaz (2002), WAP version 2.0 adopted the TLS protocol within its WAP Transport Layer Security specification. The TLS protocol allows for true end-to-end security while browsing the Internet by allowing a Web server and a mobile phone to authenticate each other and establish an encrypted connection. The authentication is part of the handshake process, where public key cryptography is utilized to provide mutual authentication and negotiate a shared key (Dierks & Allen, 1999). Once the handshake is successfully completed, application data is securely exchanged by means of symmetric key encryption using the shared-key.

However, depending on the sensitivity of an application, authentication to the network alone may not be considered sufficient. Therefore, there may be a need to authenticate various applications. The next section discusses some of the possible authentication methods at the application level.

4.1.4 Application-level authentication

Like network- and device-level authentication, only authorized users should be able to access a sensitive application (Dedo, 2004b; Ashley, 2006). This approach includes requiring users to enter their password in order to gain access to a device or remote application or a smart card application. Application-level authentication can be derived from a session or be specific to a transaction. It is usually common to authenticate for a session that may contain multiple transactions (Lindstrom, 2001). The requirement could be set up to apply to each access attempt, to apply only when the application has not been used within a certain time period, or to require reauthorization every certain amount of minutes.

Furthermore, the use of a digital certificate based on the Public key Ifrasructure (PKI) PKI can authenticate a user to an application. The certificate verifies that the user is who he claims to be (Ciampa, 2004, pp. 315–331; Simpson, 2005, pp. 305–306). Digital certificates and private keys can be stored on a smart card and presented from it when required.

In addition, on the message level, by using the public key cryptography, a message can be encrypted with a sender's private key, and the receiver decrypt it with the sender's public key as a form of authentication (Simpson, 2005, p. 299). However, digital certificates are used to further verify the claim. Appendix C provides details of how cryptography and the Public Key Infrastructure (PKI) work.

4.2 Protecting Confidentiality and Privacy

Protecting the confidentiality and privacy of health information associated with mobile computing can be approached from two perspectives: firstly, the data stored on the device perspective and secondly, the communication or transmission perspective. The subsequent sections will discuss the security countermeasures from these perspectives.

4.2.1 The Device Perspective

This section discusses the various mechanisms required to ensure that privacy and confidentiality of information is protected on a device. The following sub-sections describe the mechanisms.

4.2.1.1 Device Data Encryption

Encryption is one of the strong mechanisms of data security (Simpson, 2005, pp. 297 – 305; Schneier, 2006). It can protect sensitive health information during storage and transmission. As discussed in chapter 3, any data that is stored on non-secured media or device or transported across a network can be susceptible to attack. This makes encryption necessary to make information stored or in transit meaningless to an eavesdropper or attacker.

Data encryption can be applied to protect text, data graphics, voiced and video stored on mobile devices (Wiehler, 2004, p. 128). Among other devices are servers or other storage mediums capable of storing sensitive data, such as an expansion card or add on memory modules, which should also be encrypted (Dedo, 2004b, Sadlier, 2003). Sensitive health information should be encrypted when not in use and should be encrypted before it is transmitted. The encryption mechanism should be strong so that the encryption cannot be easily bypassed.

However, encryption algorithms usually require different amounts of processing overhead (Long, 2005; Dedo 2004b); hence, it is important to employ an efficient encryption algorithm that protects data without degrading mobile device performance or battery life.

Symmetric key cryptography requires less computational overhead, so data can be encrypted and decrypted more quickly as opposed to asymmetric keys (Ciampa, 2004, pp. 279 – 291). This type of encryption works well for applications, such as encrypting data on the mobile devices where the encryption key never leaves the device. A variety of symmetric encryption algorithms exists. In the cases where a removable media must be carried, encryption is an obvious solution. Solutions, such PGP3, offer the ability to encrypt removable media (Sadlier, 2003). Appendix C further discusses encryption, how it works, types and its suitability for mobile devices.

4.2.1.2 Compression

Data compression strengthens cryptographic security. Most cryptanalysis techniques exploit patterns found in the plaintext to crack a cipher (Schneier, 2003; Ciampa, 2004, p. 199). Data compression reduces this redundancy in the plaintext, thereby greatly enhancing resistance to cryptanalysis (Harding, 2003). In addition, data compression saves transmission time and disk space. It may take longer to compress plaintext than to encrypt it, but from a security standpoint, it may be worth the extra time, in the case of loss or theft of a device. Nonetheless, with the continuous increase in computational resources on mobile devices, compression should be advantageous. Data is usually compressed before encryption as encrypted data is incompressible (Harding, 2003). Various encryption softwares exist for handheld devices. Examples of these include paolaZip 1.0, ComponentOne Zip and PKZIP.

Furthermore, Liu and Hart (2003) showed that data compression can be achieved on mobile devices in the form mobile agents. The design was made with the consideration for the storage and processing constraints of older mobile devices. By evaluating the performance of a set of compression agents on a data set, a proper recommendation was made to a user.

4.2.1.3 Device Wipe

As discussed in section 4.1 authentication can prevent an unauthorized individual from gaining access to sensitive information. However, sometimes the prevention can be achieved only in a matter of time. The amount of time depends on the strength of the password and the speed at which the intruder can attempt various passwords. If there is sufficient time, an attacker or intruder can guess a password. This process is referred to as a brute force attack (Ciampa, 2004).

To prevent the potential for a brute force attack, a device wipe mechanism can be used (Taylor, 2006). A device wipe mechanism can cause all information on the handheld device to be erased if a brute force attack is detected. The detection of a brute force attack is based on the number of failed authentication attempts. If the number of failed authentication attempts crosses a configurable threshold, all information on the device is erased.

If a device is known to be lost or stolen, a device wipe can be instigated remotely over the wireless network (Grote, 2003; Taylor, 2006; Hassell, 2005). However, if the codes to perform the remote device wipe were to become known to an intruder it can be used as a tool for denial of service against an organization. The denial of service is achieved by replaying the device wipe to a number of existing devices that are in use by employees. An example of a third-party product that offers the device wipe functionality includes the "Bluefire Mobile Security Suite" by Bluefire Security Technologies www.bluefiresecurity.com/products.html. The next section looks at some mechanisms that will help protect health information while it is in transit.

4.2.2 Communication Perspective

This section discusses the mechanisms that will help protect health information while it is in transit. The following sub-sections describe such mechanisms. Also, since cryptography also play a vital role in this section, Appendix C will be referred to often as witnessed in the previous section.

4.2.2.1 Transmission encryption

Encryption is not only required for data stored on a mobile device, but to also secure data and communication that moves through networks (Karygiannis & Owens, 2003). Focusing on the privacy of wireless communications, sensitive health information should be encrypted during wireless transmission. According to Chapman and Zwicky, (1995), Blount (2004, p.59), Glenn and Kent, (1998) and Lindstrom (2001), encrypting network traffic provides possible guarantees of protecting privacy confidentiality. Personal health information should be encrypted and sent over an unsecured network, and then decrypted by the receiving end, and then the data is kept private from observers. Furthermore, by ensuring that no inappropriate or unauthorized third parties access or view the information, confidentiality is assured. Section 4.2.2.4 briefly shows how this is achieved.

End-to-end encryption ensures that even if data is intercepted, it will be useless to the interceptor. In network applications, encryption can be applied either between two hosts, called "link encryption", or between two applications, called "end-to-end encryption" (Pfleeger & Pfleeger, 2003; Chapman & Zwicky, 1995).

On the one hand, link encryption protects the data in transit between two devices, but the data is in plaintext inside the hosts. In link encryption, data is encrypted just before the device places it on the physical communications link, which is at the lower level of the OSI model. Link encryption is very appropriate when the transmission or communication medium is the point of greatest vulnerability, as witnessed in the wireless environment. Link encryption provides sense privacy on the network, even when it is part of a public network, as will be discussed in more detail when looking at virtual private networks (VPNs).

On the other hand, end-to-end encryption is performed at the highest level of the OSI model, the application layer. When end-to-end encryption is used, data sent through several devices is protected. The data content of the message is encrypted while in transit at all times, protecting it against unauthorized disclosure.

Encryption is also implemented in the Wireless Transport Layer security (WTLS) protocols designed for WAP applications in the wireless networks (Ottaway, 2002). These protocols allow the transmission of messages preventing eavesdropping and tampering of messages to preserve integrity.

In addition, many enterprise applications provide encryption and authentication as part of their base product. For example, PGP support is fully integrated in the Research in Motion BlackBerry user interface to provide e-mail encryption, decryption, and digital signature and verification services for e-mail sent from and received on BlackBerry devices. Solutions, such as VPN and SSL provide encryption and authentication capabilities for wireless communication security. The next two sections will discuss this solution in detail.

4.2.2.2 Virtual Private Network (VPN)

A VPN service can be used to provide secure access to caregivers, researchers or partners. Remote access VPNs can extend an organization's network to telecommuters, mobile workers and remote offices, enabling users to connect to the intranets and extranets (Lampsas, Vidalis, Papanikolaou & Vagelatos, 2002). A VPN relies on tunneling to create a secure transmission link between endpoints (Bradley, 2006). The traffic within the VPN tunnel is encrypted so that the public Internet can be viewed privately (Ciampa, 2004; Pfleeger & Pfleeger, 2003). A VPN provides secure access to intranet and extranet resources and data (Bajaj, Barton, Brownhill & Hemsath, 2004). If a VPN is properly implemented, it provides user authentication, encryption, and access control. In effect, a VPN makes it possible to secure exchange of information across a public network, which is crucial when deploying mobile devices in wireless networks (Karygiannis & Owens, 2003; Zeisz, Keil, & Lee, 2005). A variety of tunneling protocols can be used for creating VPNs and include PPTP, IPSec SSH and L2TP (Ciampa, 2004).

Most VPN clients work over virtually any network, including Ethernet LANs, GSM/GPRS, 1xRTT, 802.11, Bluetooth, IrDA and CDMAs (Wiehler, 2004 p. 150; Sadlier, 2003). Furthermore, most VPN solutions support and work with many popular gateways, including Cisco, Lucent and Nortel. For instance, Point-to-Point-Tunneling-Protocol (PPTP) VPN clients are supported by most Cisco and Nortel gateways, as well as many Microsoft and Linux servers. CORINA for example, is a client/server VPN application consisting of client parts that run on laptops, and PDAs with the server running on a Windows or Unix-based remote access server while providing support of different network scenarios. Additionally, user authentication to the VPN gateway can occur using the remote authentication dial-in user service (RADIUS) or one-time passwords (OTP) (Wiehler, 2004, p. 150; Karygiannis & Owens, 2003).

It is important to know that VPNs, while providing very strong IP data encryption, cannot prevent lower-level attacks leaving the wireless network vulnerable to a number of lower-level attacks on the MAC and IP headers, such as wireless session hijacking and rogue AP, or man-in-the-middle attacks (HP, 2003d). 802.1x-based security can be used to prevent unauthorized access to the network, and to prevent the sniffing and stealing of IP and MAC addresses. Thus, it can be used to prevent session hijacking and man-in-the-middle attacks from rogue access points.

4.2.2.3 Secure Socket layer (SSL)

SSL uses a combination of symmetric and asymmetric encryption to ensure message privacy (Syme & Goldie, 2004). During the SSL handshake, the SSL client and SSL server agree an encryption algorithm and a shared secret key to be used for one session only.

SSL (Secure Sockets Layer) is a common protocol, and most Web browsers have SSL capabilities built in (Bradley, 2006). Therefore, it can be argued that almost every computing device is likely already equipped with the necessary “client software” to connect to an SSL VPN. Today’s mobile devices come with a built-in Web browser that features SSL 2.0, SSL 3.0, and 128-bit encryption. SSL VPNs challenge IPSec VPNs (Dedo, 2004b). SSL VPNs take advantage of the SSL built into virtually all Web browsers to authenticate and encrypt transmitted data. The big advantage of many SSL VPNs is that no additional client software is needed other than a standard Web browser, as opposed to IPSec VPNs (Bradley, 2006).

Once a backend SSL server is in place, information is transmitted securely using the browser software already included on the devices. Another advantage is that this technology can be used over virtually any network. One limitation of SSL VPNs is accessing the application(s) through a Web browser, which means that they really only work for Web-based applications. Only browser-based applications can be secured using an SSL VPN without additional client software.

4.2.2.4 Public Key Cryptography

According to Elbaz (2002), public key cryptography is a primary concept in implementing wireless device security. It presents countermeasures by providing encryption, which conceals information to be transmitted between two parties. The application of public key cryptography can protect privacy and confidentiality of information (Simpson, 2005, p. 299). By encrypting a message with a recipient's public key, only the recipient with the corresponding private key can decrypt it, hence assuring confidentiality. Appendix C provides more details on this cryptography type.

4.2.2.5 Access Control Mechanisms

After using authentication to verify that a user requesting access is who he claims to be, the next logical step is to restrict the user to accessing only the resources essential for the user to do his job (Whitman & Mattord, 2003, pp. 143– 144). Access control consists of mechanisms for limiting access to resources, based on user or device identities and their membership in various groups or roles.

An access control will prevent unauthorized users from remotely accessing patient's information; hence, protecting the confidentiality and privacy of the information (Wiehler, 2004, p. 154). Software applications that manage protected health information can address access control. For example, MecuryMD Mdata uses server side, role-based access to prevent unauthorized access to patient information.

4.2.2.6 Compression

As discussed in section 4.2.1.2, data compression strengthens cryptographic security by reducing the redundancy in the plaintext, as such, enhancing resistance to cryptanalysis. This concept is used in PGP (Ciampa, 2004, p. 199). Pretty Good Privacy (PGP) is a program that encrypts e-mails and normally compresses the plaintext before encrypting it to prevent cryptanalysis attack. The Research in Motion “Black Berry” mobile devices implement PGP for e-mail transactions.

4.3 Protecting Integrity

Having data integrity controls ensures that sensitive health information is not tampered with or altered in transit or in storage either in memory or the device. Unauthorized modification can be protected via authentication, encryption and using integrity controls, such as checksums and digital signatures (Microsoft, 2005).

A checksum is a mathematical value that can be assigned to a file. The value is used to test the file at a later date or after synchronization to verify that the data contained in the file has not been altered (Chernicoff, 2001). For instance, a file compare feature in a FolderMatch's software available on notebooks has the ability to perform a bit-for-bit file comparison and cyclical redundancy check (CRC) with a known good copy of the file. This ability determines if a file was corrupt during synchronization.

A cryptographic checksum is created, via a cryptographic algorithm that translates data in a file into a fixed string of digits, called a hash value. The hash value is used as a checksum. Without knowing what cryptographic algorithm was used to create a hash value, it is very unlikely that an unauthorized person would be able to alter the data without inadvertently altering the corresponding checksum (Ciampa, 2004).

Digital signatures allow a recipient of information to verify that a third party has not altered the information in transit (Elbaz, 2002). The public key cryptography is well suited to providing digital signatures. The signature for a document is created by hashing the document with a one-way hash function and encrypting (signing) the hash value with the private key component of a public/private key pair. The verification is done by decrypting the hash with a public key component to expose the hash value. The hash value is compared with a recomputed hash value so that if the two hash values match, the signature is considered valid. Appendix C provides more information on digital signatures.

In addition, and in very much the same way, code signing can ensure the authenticity and integrity of application code. This action prevents the use of malicious applications to compromise critical data and resources of mobile devices (Grimes, 2001; Fleischman, 2002). Authenticity signifies that the code to be installed or launched is indeed from the stated developer or a trusted party. Integrity controls will signify that the code has not been altered since it was signed.

Code signing is achieved by taking a hash of the code, then encrypting that hash with the code signer's private key, or digital signature. This digital signature is then attached to the code. The signed code is then verified prior to installing or launching the applications. The verification is achieved by validating the digital signature, using the signer's public key.

4.4 Protecting Availability

Availability refers to the assurance that the systems responsible for processing, storing and delivering health information are accessible when needed, by authorized individuals who need them.

Malicious codes, such as viruses and worms, use up available device memory and transport themselves across the network. Furthermore, a denial of service attack by a hacker can slow down performance and eventually crash a network. When a network crashes, resources become in accessible. Therefore, by placing anti-virus software both on the network and mobile device levels, malicious code execution or activity can be mitigated. Section 4.4.1 elaborates more on protecting mobile devices and their networks using anti-virus software.

Furthermore, because of the non existence of a physical barrier, the risk of network intrusion is higher in a wireless environment than in fixed networks (See chapter 3 section 3.1). Therefore, having intrusion detection and a firewall system to prevent or mitigate unauthorized intrusion becomes imperative. Sections 4.4.2 and 4.4.3 discuss intrusion detection and firewall systems to curb intrusion and lower the risk of insufficient availability.

4.4.1 Anti-Virus software

There are several types of anti-virus software. These software ranges from solutions that protect user devices, to those that protect files and messaging servers (Wiehler, 2004, p. 127, Symantec, 2006b). These are all necessary in the fight against viruses. Malicious code may execute on a mobile device itself or on any connected system, once an infected file is transferred onto the network. As discussed in chapter 3, most infections are transmitted through e-mail attachments. A messaging server, capable of inspecting attachments before sending them to a mobile device, mitigates the risk of infection (Symamtec, 2006b).

An effective anti-virus strategy includes regular software updates to protect against the latest threats, and scanning of files immediately after receiving data (Slawsby, 2004; Dedo, 2004). Programs with up-to-date signature files are crucial for preventing infection of critical health information. Administrators can have enforceable policies for running virus scans whenever new files are downloaded and for keeping the virus signature files up to date (Symantec, 2006b). Anti-virus software vendors, such as Symantec, McAfee, TrendMicro and Computer Associates, create anti-virus applications for mobile devices.

4.4.2 Intrusion Detection Systems (IDSs)

Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources (Przemyslaw, Kazienko & Piotr Dorosz, 2003). IDSs attempt to identify computer system and network intrusions and misuse by gathering and analyzing data (Farschi, 2003). Basically, the goal of IDS is to provide a near-real-time view of what is happening on an organization’s network. Applications that actively monitor operating systems and network traffic for attacks and breaches are called intrusion Detection Systems (IDSs) (Karygiannis & Owens, 2003). Traditionally developed to detect intrusions and misuse for wired systems and networks, IDSs have been developed for use on wireless networks (Farschi, 2003). IDSs on wireless networks can detect and respond to potential malicious activities.

There are two main approaches to intrusion detection: network based and host based (Karygiannis & Owens, 2003; Farschi, 2003). Network-based systems generate alerts based on comparing live traffic patterns to a list of known attacks or anomalies in traffic (Gerken 1997; Farschi, 2003). These wireless

IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs.

Host-based IDSs (HIDSs) are available for mobile devices (Miettinen & Halonen, 2006). Host-based IDSs monitor devices for misuse and intrusion. A HIDS verifies the integrity of files on a host and compares them to any attack signature within its internal database. Once an attack signature is found, the host then sends an alert to the administrator.

However, both solutions require a regularly updated list of known attacks, just like an anti-virus software. To aid in the defense and detection of these potential threats, WLANs should employ a security solution that includes an intrusion detection system (IDS). Even organizations without a WLAN are at risk of wireless threats and should consider an IDS solution (Farschi, 2003).

4.4.3 Device Firewall

Since a number of mobile devices come equipped with 802.11 wireless local area network, GPRS or CDMA wireless wide area network, or Bluetooth connectivity, they are likely susceptible to attacks or attempted intrusions. In order to prevent access attempts over these networks, all network traffic going in and out from the devices are inspected and placed under policy control by a device or personal firewall (Sadlier, 2003; McAfee, 2006).

The firewall clients can be centrally managed for both configurations as well as security policy. The firewall can be used to generate security event logs that are brought together at a central log reporting and storage system (McAfee, 2006). Central management of policies on devices provides assurance that the devices are, in fact, protected (Sadlier, 2003). An example of a central firewall product is the “PointSec Enterprise Mobile Solution”.

With a device firewall, only authorized ports and protocols are allowed, and all other traffic is blocked (Ciampa, 2004 pp.159– 164). By restricting the communications that a device will participate in, the device can be protected from hostile attacks originating from untrusted networks.

In situations where all connections to an organization’s network pass through a gateway, placing a network firewall on the gateway itself can be the simplest solution, as it avoids the need to place a personal firewall on each mobile device (Dedo, 2004b).

According to Karygiannis and Owens (2003), recent VPN devices have integrated firewalls that work together to protect both the network from unauthorized access and the user data going over the network. Integrated VPNs and firewalls save costs and reduce administrative burden.

4.5 Protecting Non-Repudiation

Digital signatures and time stamps can protect against repudiation (McCullagh & Caelli, 2002; NIST, n.d.). In section 1.2.2 it was stated that non-repudiation provides proof of data transmission or receipt, so that the occurrence of an operation cannot later be denied. A message's recipient can insist that the sender attach a signature in order to make later repudiation more difficult. This prevents the sender of information from claiming at a later time that he or she never sent the information (Lindstrom 2001). Appendix C discusses more on non-repudiation.

Furthermore, based on the NIST's Digital Signature Standard (DSS), an electronic time stamp can be affixed to documents in electronic form and then signed using the Digital Signature Algorithm (DSA) (NIST, n.d.). A DSA is used in computing and verifying digital signatures. Applying a DSA to a document will protect and verify the integrity of the document and its time stamp.

4.6 Secure Administration and Management

As part of network management, one approach to securing a WLANs is to treat it as as an untrusted and unsecure network (Ciampa, 2004, pp. 253 – 254; Zeisz, Keil, & Lee, 2005). This requires that the WLANs be placed outside the secure perimeter of trusted networks and that an access point behind is placed firewall. If a WLANs user must be inside a secure network perimeter, one solution maybe set up a VPN for every user and the other is to use the Wi-Fi Protected Access (WPA).

Furthermore, healthcare organization security cannot be optional, it should be compulsory and enforceable (Stanford, 2002). So the initial step is to take control over the security settings to prevent users and attackers from altering or removing security mechanisms. Schwartz (2004) stated that actively controlling the security state of mobile devices provides the foundation for all other security measures.

Today's mobile devices include a configuration manager facility for easily transferring security settings to mobile devices (Dedo, 2004). This management component offers several benefits, such as configuring devices to connect through the appropriate protocol, e.g., via GPRS or WAP. The management component saves users the time and trouble of trying to configure their own devices. More so**,** mobile operators can configure connectivity settings over the air.

Third-party systems-management products provide functions, such as inventory management for mobile devices, including tracking device settings and software version levels. This information can be used to automate updates or changes to a device the next time it connects to the organization's network. Others offer centralized security systems that enforces how, when, and what a mobile device can access on an organization's network. These tools can enforce such security policies as how many wrong passwords can be entered before a device is locked down or, in some cases, has all its data erased.

In addition, some tools provide back up and data recovery capability. Backing up data regularly enables quick restoration of lost applications and data in order to minimize downtime. When a mobile device is misplaced or stolen, a user account can be disabled temporarily, and the mobile device isolated from the network.

If administrators practice configuration management and conduct regular backups, user data and profiles can be restored immediately. When backups are carried out regularly, the data can be saved within an organization's firewall and can be quickly restored to another device.

Furthermore, some solutions possess audit trail capability, which can record identities, times and circumstances of users accessing information. If it is known by users that these records are kept and reviewed regularly, it will reduce privileges' abuse by users (Rindfleisch, 1997).

Therefore, it can be concluded that central management solutions provide administrators with tools to manage mobile devices, ranging from policy administration, device detection, monitoring to real-time control**.** Some solution product providers include Trust Digital Solutions, Credant Mobile Guardian (CMG), Good Technology, PointSec and iAnywhere**.** Having such solutions can be beneficial to healthcare.

However, the selection of the right solution is dependent on objectives and requirements of an organization. The application of any administrative or any technical countermeasure to protect information requires policies to define what the appropriate use of information is and not (Whitman & Mattord, 2003; Rindfleisch, 1997). Besides that, depending on the nature of the business, government regulations and laws may influence technology selection (Grove, 2003; Nealon & Moreno, 2002).

4.8 Conclusion

In this chapter existing countermeasures to protect the confidentiality, integrity, availability and privacy of health information accessed on mobile devices were discussed. In order to achieve a high level of security, the security mechanisms are used in layers and can be administered from a central point. The existence of the central management and administrative tools provide an administrator with the power to effectively manage and control access to health information.

However, most of the countermeasures discussed are tailored towards IT security and are not enough to provide a mobile computing solution in healthcare. Threats continue to evolve and security and privacy issues are also a people’s problem.

Furthermore, the healthcare industry is required to meet certain regulatory requirements, which may likely influence technology-solution selection. In order to achieve a comprehensive and successful mobile-security solution that will meet healthcare requirements, both technical and operational corrective measures must be combined.

Industry standards and best practices can provide an excellent starting point for formulating sound security guidelines. Standards will help provide a systematic approach to manage sensitive health information that is accessible on mobile devices so that it remains secure at all times. The next chapter introduces and discusses an ISMS management approach that will help define a secure mobile computing profile for healthcare, taking all the required factors into consideration.

Chapter 5

Mobile Computing Security: An Information Security Management Approach

In the previous chapter, mobile computing countermeasures to thwart a wide range of threats and possible vulnerabilities in a system were discussed. Although the countermeasures provide promising results for achieving a successful mobile deployment in healthcare, they are limited. The limitation is based on the fact that the solutions discussed are technically oriented and do not take into account factors like healthcare's specific legal requirements, the continuous evolution of threats and the threats and vulnerabilities associated with users and operations.

In an effort to provide a mobile solution that will span these factors, this chapter attempts to incorporate a mobile security solution into an Information Security Management System (ISMS). It begins by looking at a general ISMS, based on the ISO/IEC 27001:2005 standard in comparison to other standards. It discusses the components that makes up the system and shows how they work. The chapter goes on to look at how compliance can be achieved when different standard references are involved. The chapter then identifies some standards and regulatory requirements that may influence mobile security solutions. Eventually, the chapter sets up an ISMS baseline for mobile security by selecting two suitable standards that the mobile security profile will fit. Finally, a conclusion will be drawn. The chapter begins by looking at ISMS standards.

5.1 An Information Security Management System (ISMS)

An Information Security Management System (ISMS) will help provide a systematic approach to managing sensitive health information, accessible on mobile devices, so that it remains secure at all times (Whitman & Mattord, 2003, p. 210; Treek, 2003). It encompasses people, processes and IT systems (Fiedler, 2003; Whitman & Mattord, 2003, pp. 16 - 17)

According to Wiehler (2004, p. 130), an ISMS consists of a documentation set defining and supporting the business and various information security procedures and processes in different categories, for example, access control and personal security. The procedures and processes provide guidance to staff and information to senior management on the ongoing effectiveness of the ISMS. To be effective, the ISMS must be of manageable size, and its boundaries should be clearly defined.

Focusing on the need for an over all risk management system and an internationally acceptable practical standards for oganizations, (ISO) came up with a set of standards that will allow organizations establish a successful security management system (Calder, 2006). These standards have evolved overtime, each time with sound improvement. The current versions of the standards are referred to as ISO/IEC 17799:2005 (BS 7799-1:2005) “Code of Practice for Information Security Management” and ISO/IEC 27001:2005 (BS 7799-2:2005) “Information Security Management System. Figure 5.1 below shows the evolution timeline for these standards.

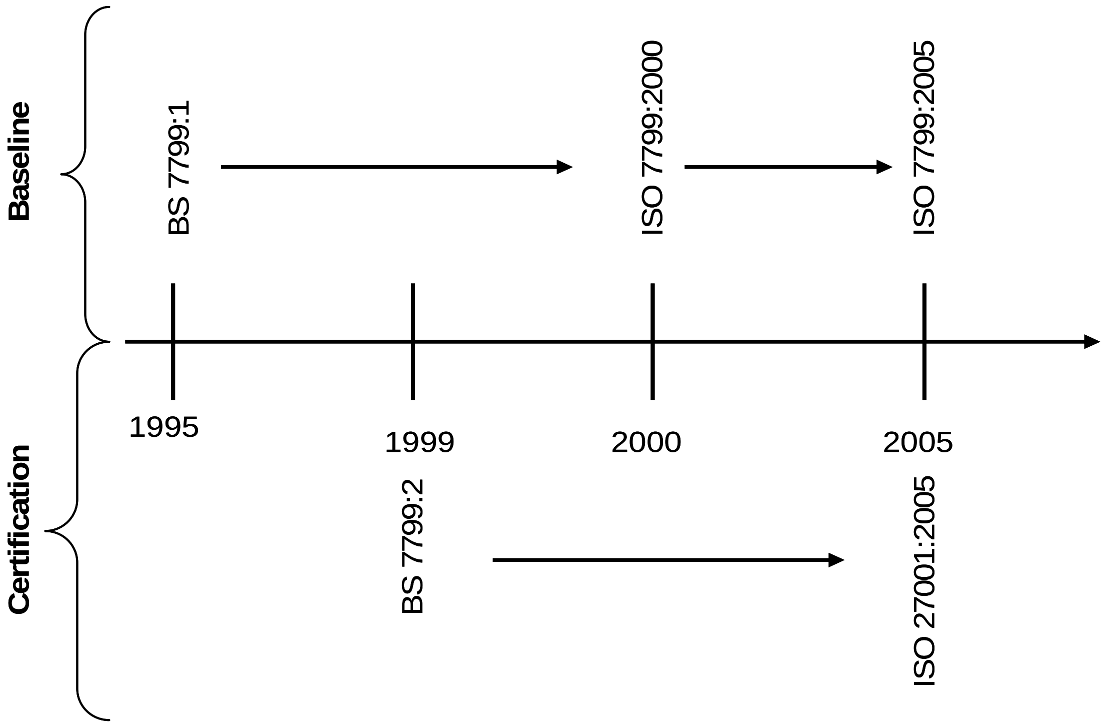

Figure 5.1 ISO standards evolution timeline

The ISO standards have gained worldwide acceptance and are almost universally recognized as quality information management systems. Nonetheless, there exist several standards and best practices, which advise on how to manage the function of various organizations. Many organizations including ISO, have published suggested frameworks on management. However, each of these standards addresses a certain aspect of Information technology (IT) specifically, such as IT governance, information security management or strictly focuses on the technical aspects. None of these frameworks however, are in competition with each other, in fact, it is best if they are used together (Harris, 2005). Von Solms (2005) stated that because of the convergences that exist between these standard frameworks, using them together can provide a synergy which can be beneficial to organizations.

According to Saint-Germain (2005) complying with ISO 17799 standard or obtaining ISO/IEC 27001 certification does not prove that an organization is totally 100% secure. The ISO 17799 is described as a starting point for developing an organization's information security programme. This means that meeting ISO standards is not enough to provide a total security solution for an organization; therefore, other standard controls or guidelines may be required to compliment ISO 17799.

Standards like Common Criteria (CC)/ ISO/IEC 15408, GMITS, NIST 800-14, IT Infrastructure Library (ITIL), ISO 13335 and COBIT can be used to compliment ISO. Although they may seem at first to have overlaps, they do have distinct differences. Table 5-1 shows a summarized comparison between these standards.

Table 5-1 Summarized security standards comparison

ISO 17799	**ITIL**	**COBIT**	**NIST 800-14**	**ISO 13335**	**ISO 15408**
Provides security controls.	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: (Saint-Germain, 2005).

For example, a combination of ISO 17799, ITIL and COBIT can provide a good over all management approach (Harris, 2005). COBIT can be used to determine if an organization's needs, including security, are being properly supported by

IT. ITIL can be used to improve IT processes to meet the organization's goals, including security. Finally, ISO 17799 can be used to determine and improve upon an organization's security posture, which makes it suitable for this research. The subsequent section discus the ISO standards in more details beginning with the code of practice standard.

5.1.1 ISO/IEC 17799:2005

The ISO/IEC 17799:2005 Code of Practice is intended to provide a framework for international best practice in information security management and systems interoperability which depends on ISO 27001 for certification by external auditors (Calder, 2006). It provides substantial implementation guidance on how individual controls should be approached. In addition, its controls cover all aspects of Information Security ranging from organizational, physical and technical aspects (Saint-Germain, 2005).

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).

Healthcare organizations implementing ISO 17799 can guarantee customers and stakeholders that the organization is doing its utmost to ensure the security of their health information (BS 7799, 1999). ISO 17799 can 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. The ISO framework provides a code of practice that encourages organizations to consider all factors when developing their security programme.

Furthermore, ISO/IEC 17799:2005 is consistent with the international Organization for Economic Cooperation and Development (OECD) guidelines on privacy, information security and cryptography. Although, it does not particularly prescribe solutions to personal data privacy, it does specify the security objectives that need to be achieved in whatever implementation circumstances (BSI, 2006). The ISO/IEC 17799 best practice controls are described in a way that can be implemented in a variety of legal and cultural environments.

Nevertheless, as mentioned earlier, 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 each organization (ISO17799, 2005). Therefore, it becomes imperative to consider integrating controls from other security standards or regulations, dealing with healthcare specific requirements, or better still, perform a mapping exercise.

A mapping exercise will provide an interpretive guidance on an intended scope and will show whether or not ISO security scope correlates with a legal or regulatory requirement. The next section discuses the management standard of ISO.

5.1.2 ISO/IEC 27001:2005

Many organizations have active quality management systems which are regularly audited against standards, such as ISO 9001. It is the same principle that has been extended as ISO/IEC 27001:2005 by ISO17799. The ISO/IEC 27001:2005: entitled "Information technology – Security techniques – Information security management systems – Requirements", specifies the processes to enable a business to establish, implement, review and monitor, manage and maintain an effective ISMS. The review of BS7799-2 to ISO/IEC 27001 was made in consistence with other management standards such as ISO 9001:2000 (Customer needs Quality Management) and ISO 14001:1996 (International Standard for Environmental Management). The synchronization of the standards helps in the integration and operation of an organization's overall management system. Furthermore, it is consistent with the principles of the OECD which is focused on the security in the development of information systems and networks.

Implementing an ISO 27001 ISMS requires ISO 17799 (Calder, 2006). The standard forms a complementary pair with ISO/IEC 17799:2005 (BS 7799-1:2005). It mandates the use of ISO 17799 as a source of guidance on controls, control selection and control implementation. The next section discusses the management model that ISO/IEC 27001 uses.

5.2 The ISO/IEC 27001 Management Model

The ISO/IEC 27001 management system implements the Plan-Do-Check-Act

(PDCA) model to perform the management of information security. In order to understand the PDCA model, the following sub-section looks at the elements that make up an ISMS.

5.2.1 Elements of ISMS

ISO and IEC in 1997 created a report called the ISO/IEC TR 13335 and the aim of this document is to provide guidance on the management of IT security. The ISO/IEC TR 13335 Guidelines for the Management of IT Security (GMITS) is usually referred to as the big brother of ISO 17799 (Bisson & Saint-Germain, 2003).The document consists of five parts (GMITS1-5), with part one providing an overview of the fundamental concepts and models used to describe the management of IT security (ISO/IEC TR13335-1, 1997). In this part, eight major security elements are described that contribute to the ISM process. The elements are Asset, Threat, Vulnerability, Impact, Safeguards, Constraints, Risks, and Residual Risks. These elements, according to Ciampa (2004, pp. 505 - 519) Microsoft (2004), and Whitman and Mattord (2003, pp. 27 - 29), are described as follows:

- **Asset**: This is defined as anything that is of value to an organization and is usually protected. An asset can be intellectual or physical. It is owned by an organization in an information system environment and, usually takes the form of hardware, software or data.

- **Threat**: This is defined as an object, person or any situation or event that has the ability to harm or represent a danger to an asset. For example, a hacker is a threat to an unprotected information system.

- **Vulnerability**: This is a weakness that allows a threat agent to bypass security. Security problems in computing systems normally result from vulnerabilities. For example, a flaw in software is a weakness that can expose a system to attack. It requires a patch download and installation to seal up the weakness.

- **Impact**: This refers to the result of an unwanted event or occurrence, caused either deliberately or accidentally, which affects the assets. The measurement of impacts permits a balance to be made between the results of an unwanted incident and the cost of the controls to protect against such an event.

- **Risk:** This is referred to as the possibility that a given threat will exploit vulnerabilities to cause loss or damage to an asset.

- **Safeguards**: These are controls or countermeasure such as practices, software configurations, hardware, and procedures or mechanisms, which may protect against a threat, reduce vulnerability, limit the impact of an unwanted occurrence, detect unwanted occurrences and facilitate recovery. Effective security usually requires a combination of different controls to provide layers of security for assets. An appropriate selection of controls is essential for a properly implemented security programme.

- **Residual Risk**: Refers to the risk that remains to after a counter-measure has been applied. This type of risk is not controlled by implementing controls, but is normally reduced until it is small enough to be acceptable.

- **Constraints**: These are limitations or restrictions, usually determined by the management of an organization, and are influenced by the environment that the organization operates in. Some examples include: cost, time, environmental, legal, technical and many more constraints.

All eight elements need to be understood and considered when dealing with an information security management system.

5.2.2 The PCDA (Plan-Do-Check-Act) Model

As stated, ISO/IEC 27001:2005 is based on a PCDA (Plan-Do-Check-Act) model, which conforms to other management standards, such as ISO 9001 and ISO 14001. It emphasizes strict process thinking and is well rooted in quality management.

According to Fiedler (2003) and Whitman and Mattord (2003, p. 210), the phases or activities of the PDCA cycle include: Establishing the ISMS (the PLAN phase; Operating the ISMS (the DO phase); Monitoring and Reviewing the ISMS (the CHECK phase); Improving the ISMS (the ACT phase). Figure 5.2 shows the layout process of the PDCA cycle.

The **PLAN** phase is concerned with establishing the ISMS. The primary step is to determine the scope of the ISMS. The scope means specifying what will be controlled, which, in this case, is access to sensitive health information.

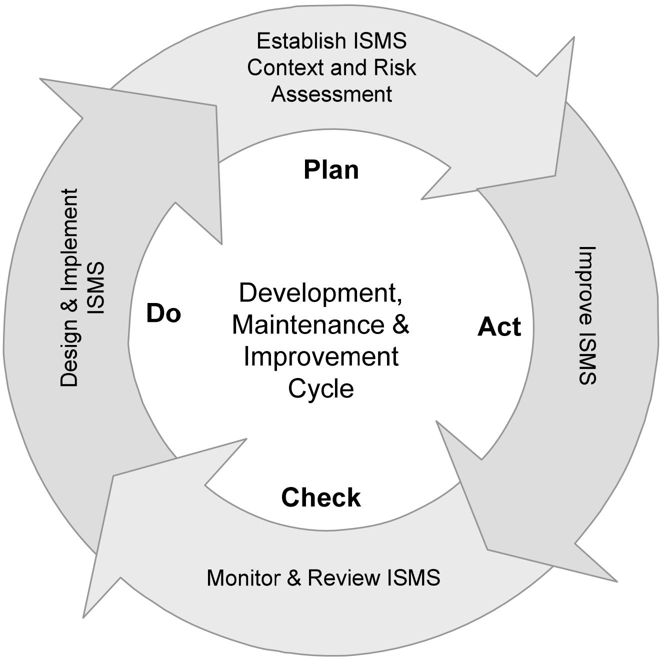
Establish ISMS Context and Risk Assessment
Plan
Design & Implement ISMS
Do
Development, Maintenance & Improvement Cycle
Act
Improve ISMS
Check
Monitor & Review ISMS

Figure 5.2 The PDCA cycle

An ISMS policy has to be defined that includes objectives, legal or regulatory requirements, contractual obligations, the strategic organizational and risk management context and risk assessment criteria. The components of the PLAN phase include:

- **Risk Identification**: This component identifies the assets and prioritizes the assets based on their value. In addition, it identifies threats and vulnerabilities as done in chapter three.

- **Risk Assessment**: Risk assessment looks at the probability or likelihood of risk occurrence and its associated impact on an organization.

- **Risk treatment plan**: This means responding to the risks. The impact on an asset will determine how to manage the risk, i.e., accept the risk, transfer it to other parties, or eliminate or mitigate it. The selection of controls is based on this decision, which is taken during the risk assessment.

- **Statement of Applicability (SoA)**: The SoA is where the organization specifies their ISO 27001 certification scope. The scope can include the whole organization and its security program, or just a specific department within the organization. In other words, the SoA documents the controls wherein implementers must show their compliance, or provide a sound justification if the controls do not apply within the scope of their ISMS. In this case it requires going through all 133 ISO/IEC 27001:2005 controls and justifying which ones have been used and which have not.

- **Management Approval**: Management has to approve the implementation of the ISMS. The responsibility of management is a key success factor for the ISMS.

The **DO** phase implements the steps as planned in the PLAN phase. The phase requires having procedures, to ensure the prompt detection and response to incidents. In addition, to ensures that all members of staff are security aware and are appropriately trained and are competent to carry out their respective security tasks.

The **CHECK** phase monitors and reviews the ISMS by ensuring that the controls are in place and are achieving their objectives. The review of ISMS ensures the effectiveness of the ISMS. Monitoring the operation of the ISMS includes intrusion detection, auditing performance, identifying actions taken to resolve a security breach and following up actions in case of security breaches. Residual and acceptable risk has to be reviewed regularly to determine its current level of impact.

Sometimes, risks are considered acceptable, and no controls are implemented, even if threats are present. Other times, risks can be completely eliminated or mitigated to an acceptable level (residual risk), which is usually associated with constraints, such as costs. Constant monitoring and review should be done to ensure that no new threats develop to exploit known vulnerabilities (Microsoft, 2004).

The **ACT** deals with improvement. In this phase, improvements are implemented, corrective and preventive actions taken, results communicated with all interested parties and improvement actions monitored.

In summary, information security management involves a continuous process of identifying, analyzing and evaluating the risks to a system. The system defines the security policies and controls to be implemented as part of its establishment and implementation. Finally, evaluating how well those controls are fulfilling the requirements specified in the policies is part of maintenance and improvement.

As new vulnerabilities are being identified daily, and new threats are sprouting rapidly to exploit the vulnerabilities and their controls, a risk management process must be in place, and it must be a continuous process (Humpreys, 2000; Ottaway, 2002). The risk management entails the continuous repetition of the risk activities outlined in the plan phase. It is a requirement of ISMS to achieve due diligence in an organization (Robillard, 2001; Whitman and Mattord, 2003; Halliday, Badenhorst, & Von Solms, 1996).

5.3 Achieving Regulatory and Standards' Compliance in Healthcare

According to Wiehler (2004, p. 130), an ISMS is usually implemented by identifying the current gaps in the categories given by ISO 17799 and defining appropriate actions to achieve the described objectives. A corporate policy that gives direction on the objectives of information security within the company is issued, and appropriate bodies are installed with the participation of senior management, to support the ISMS objective throughout the organization.

However, the question is how does the ISMS standard comply as healthcare industries are required to fulfill legislative and regulatory healthcare requirements? The increase of stringent healthcare security standards mean complementing ISO 17799 in a healthcare environment is a necessity. Luckily, the ISO standard set have made space such requirements. In order to determine whether the ISO 17799 controls are sufficient, or whether additional controls are required to meet other requirements, it is appropriate that these other requirements are mapped into the controls given in the an SoA. A first step is to identify those laws or regulations that healthcare organizations are required to show compliance with through their ISMS.

Many countries have developed various privacy and data protection laws with the main objective of ensuring data and privacy protection (SALC, 2003). For instance, the Data Protection Act of 1998, which was implemented into UK law, and the Europe Directives, details how personal data may legally be used. The purpose of the act is to protect the rights of the individual about whom data is obtained, stored, processed or supplied, applying to both computerized and paper records. This is meant to give users the confidence that healthcare is meeting regulatory and ethical obligations when sending out health information. The next sections provide an overview of standards and some specific, regulatory requirements prominent to the healthcare environment.

The healthcare industry has some unique industry-specific requirements in the form of legislation and regulations it must adhere to. Many countries have established laws to ensure that privacy and security of health information is protected. In the event of failure to meet their standards, loss in the legal and financial stakes for organizations is the result (Nicolett, 2003; Wales, 2003; Nealon & Moreno, 2002).

As mentioned in Chapter 1, 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. Hence, adopting security best practices to ensure security of information does not necessarily ensure privacy protection. Adopting a regulatory framework then becomes important for data privacy protection.

Traditionally, the concept of protecting health information was based on an ethical code where physicians pledged to respect confidentiality and privacy of patient health information, even on the event of a patient’s death (Oath of Hippocrates, 1995). This pledge of antiquity was declared as a professional responsibility of physicians to ensure privacy protection (Smith, 2004).Today; the Hippocratic Oath by itself is no longer sufficient in this electronic era and has been extended by international and national legislation.

5.4 Overview of Standards and Regulatory Requirements in Healthcare

Currently, there is an increasing number of international healthcare standards, but most of them are not security related. These standards include the communications standards developed by Institute of Electrical and Electronic Engineers (IEEE) and Digital Imaging and Communications in Medicine (DICOM) and the Content and Structure standards Health Level 7 (HL7), an ANSI accredited standard. The standards which deal with ensuring the privacy and security of health information are ISO/TC 215 and CEN/TC 215 and others are developed by government agencies, public and private security practitioners.

The ISO/TC 215 and CEN/TC 215 standards have very similar scope which largely covers the same ground. The standards both cover 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). The ISO TC 215 consists of 25 participating member countries including 15 from Europe, 4 from Asia, 2 from America, 2 from Oceania and 2 from Africa. More information on these standard guidelines can be found at these sites (www.iso.ch) or ISO/TC 215 (www.iso.ch/sdis).

The development of computer-based patient record systems and healthcare information networks created the need for more definitive confidentiality, data security, and authentication guidelines and standards (Blair, 2002). Among these organizations are; The Computer-based Patient Record Institute (CPRI), is an organization of public and private entities that promotes the use of electronic health records, and The Center for Medicare and Medical Services (CMMS) who published HIPAA regulations standards for the security of electronic health information. Another organization is; NIST, a non regulatory federal agency with a Special Publication (SP) 800-66 document about understanding the HIPAA security rule. There are also many others.

In addition to the ISO TC 215 principle are the international privacy principles. The increasing ease with which personal data can be transmitted outside the borders of a certain country of origin propelled the release of the privacy principles to govern such information.

The privacy principles are the 1981 OECD guidelines, governing the protection of “Privacy and Trans-border Data Flows of Personal Data”, and the Council of Europe’s 1981 Convention for the protection of individuals with regard to the automatic processing of personal data are responsible for these principles (BT, 2004; OECD, n.d). These principles are known as the “Principles of Data Protection” and form the basis of both legislative regulations and self-regulating control.

These important principles have had an intense effect on the enactment of national laws around the world, even outside the OECD member countries. The OECD principles have guided the deliberations, policies and laws of some 30 member countries of the OECD. It is possible that an OECD member country can refuse to transfer personal data internationally to another receiving country that does not have comparable protection laws (OECD, n.d.). Hence, it can be argued that they are considered as universal best practices principles.

The key principles are based on the OECD guidelines. The guidelines however, do not set out requirements as to how these principles are to be enforced by member nations but require that the principles are met. The member countries have chosen a range of differing measures to implement the privacy principles.

As data protection and privacy of personal medical information has become imperative, many countries have adopted different standards and legislative frameworks to ensure their protection. The subsequent section discusses some regulations aimed to ensure the privacy and security of health information in some countries.

5.4.1 SANHA AND ECT Acts

In South Africa (member of ISO TC 215 committee), healthcare organizations are required to 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’ contains a number of requirements aimed at protecting the privacy and security of health information.

SANHA incorporates some of the standards adopted by Health Insurance and Accountability Act (HIPAA) regulations in America to meet its needs for greater standardization of data collection, IT systems and billing practices. This adoption was in effort to a resolve problems experienced by healthcare providers with regard to the payment of claims (Council Medical Schemes, 2002).

This application standard requires all healthcare players to use Health Level Seven (HL7) v.2 standard in conjunction with X12 for passing data between providers and payers. The Health Level Seven (HL7) which was already adopted by HIPAA in America (A ISO TC 215 and OECD member) to achieve this objective. The recommendations finally drawn by SANHA were mostly related to HIPAA standards requirement such as the use of security and accountability safeguards found in HIPAA security standard, the written consent of the patient prior to the disclosure of health information, notice about the use and disclosure of health information and some necessary requirement found in the HIPAA privacy rule. Most of these were incorporated in the South African National Health Act (SANHA).

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 is not specifically aimed at healthcare organizations. However, it 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 using increased electronic communication in healthcare business transactions. Chapter 8 titled, Protection of Personal Information, provides the scope, as well as the principles, for electronically collecting personal information.

5.4.2 Legislation in New Zealand

In New Zealand (member of ISO TC 215 and OECD), the health laws were drawn up in the already enforced, Privacy Act of 1993 ("New Zealand Federation Of…", n.d.). This is referred to as the "Health Information Privacy Code of 1994". The Privacy Act governs the responsibilities towards the collection, storage or disclosure of personal information about individuals, as well as the transparency of activities in this area (Kerr, 2004). This code applies to any organization that provides health or disability services to sick or disabled citizens. This has been interpreted at a policy level through the Health Networking Code of Practice, sponsored by the Ministry of Health and Standards

New Zealand. This is meant to support the Health Intranet and wider health information networking activities for a secure electronic environment within which users throughout the health system can transfer and exchange health information (Kerr, 2004).

The Health Network Code of Practice assists health care providers and consumers who need to communicate securely and with confidence, by electronic means, through a chain of trust where the level of security is maintained across all the participants. The Code of Practice is meant to support the Health Intranet and wider health information networking activities.

5.4.3 HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets standards for the security of medical records for all health plans, healthcare clearinghouses and healthcare providers that transmit health information in electronic format. The HIPAA, Public Law 104-191, was signed into law on August 21, 1996 by the then US President, Bill Clinton. The primary focus of the HIPAA is to mandate that healthcare information become “portable” and “available” by legislating on the use of uniform electronic transactions and other administrative measures (Herrera, 2006).

The haling of the healthcare industry to adopt uniform electronic transaction standards for healthcare information meant that it became 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 sections of the HIPAA law that have impact on IT interests are the sections on Administrative Simplification (Title II, Subtitle F). This section attempts to force uniform standards in the electronic interchange of health information (through the Transaction standard) and mandates guidelines for the security and privacy of that information whether in transit or stored. The US Department of Human Health and Services (HHS) has issued three rules, the Security Rule, the Privacy Rule and the Transaction and Code Set Rule that covered entities must follow to meet HIPAA requirement.

5.4.3.1 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, 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 rule encompasses standard electronic transaction formats mostly derived from the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12.

5.4.3.2 The Privacy Rule

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral protected health information (PHI). The rule mandates that any health information that identifies an individual and is transmitted or maintained by a health care provider must remain confidential, not be altered or accessed without authorization and be readily available to authorized users (HIPAA Administrative Simplification – Privacy Set Rule, 2000).

5.4.3.3 The Security Rule

HIPAA’s Security Final Rule only applies to the security of “electronic” protected health information (ePHI) to be implemented by health plans, healthcare clearinghouses, and certain healthcare providers referred to a Covered Entity (CE). 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 rule mandates the protection of the confidentiality, integrity and availability of electronic personal health information (HIPAA Security Rule, 2003). The final Security Rule is consistent with the Privacy Rule, however it limits its scope only to PHI that is in electronic form. The refinement, however, does not eliminate the requirement for security on non-electronic PHI, since the HIPAA Privacy Rule sections 164.530(c) still requires appropriate security for all PHI, regardless of its format.

The majority of the security standards incorporate implementation specifications to better describe the actions that should be taken to ensure compliance with the standards. The final rule offers high-level guidance, providing what is essentially a model for information security, with less specific guidance on how to implement the model. In other words, the rule is focused more on what needs to be done and less on how it should be accomplished. However, HHS has promised more specifics in future guidance documents.

Section 164.306 provides the statement for the General Rule, which requires covered entities to:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) the covered entity creates, receives, maintains or transmits;

- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and

- Ensure compliance by its workforce.

The HIPAA Security Rule requires safeguards in three main areas of the rule: Administrative, Physical and Technical, which in total contain 42 security-measure specifications that covered entities must implement. However, there is an organizational requirement standard that must be met. The organizational requirement standard includes policies, procedure and documentation requirements (CMS 2005).

Administrative safeguards primarily address the policies and procedures a covered entity must have in place to document its ability to insure the confidentiality, integrity and availability of ePHI. 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 programme (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 an entire information security programme is based. It serves as the central source of documentation for HIPAA compliance reviews.

It is vital to note that for every standard, the Security Rule provides a number of implementation specifications to better describe the actions that should be taken to ensure compliance with the standards. Only 13 of these implementation specifications are required; the majority of the specifications are termed "addressable." The HHS makes a distinction between implementation specifications that are required, and those that are addressable. If a standard is marked Required (R), this 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 to the protection of health information. Should it be appropriate, they must be implemented as written, or else they must document why it is inappropriate and implement an equivalent alternative measure that is reasonable and appropriate. For example, the Rule requires training on security issues for the workforce, but identifies training in password management as an "addressable" specification. In an environment where biometric technology is used to control system access, password training would be irrelevant, and not required. Table 5-2 outlines the required and addressable measures of the Administrative Safeguard Requirements.

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 5-3 shows the standards, section and implementation specifications of physical safeguards. These are marked Required (R) or Addressable (A).

Table 5-2 Administrative Safeguards

Administrative Safeguards (164.308)			
Standards	**Section**	**Implementation specifications**	
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
		Authorization and/or Supervision	A
		Workforce Clearance Procedure	A
		Termination Procedures	A
		Isolating healthcare clearinghouse function	R
		Access authorization	A
		Access establishment and modification	A
		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
		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)

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 5-4 shows the Technical Safeguards Standards.

The organizational requirement (164.314) provides requirements for the contents of business associates contracts or other arrangements and the plan documents of group health plans (CMS, 2005). The Policies and Procedures and

Documentation Requirements (164.316), amongst other things, require a covered entity to implement and maintain written policies, procedures and documentation required to comply with the Security Rule. Table 5-5 shows the organizational requirements.

Table 5-3 Physical Safeguards

Physical Safeguards (164.310)			
Standards	**Section**	**Implementation Specifications**	
		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
		Disposal	R
		Media Re-use	R
		Accountability	A
		Data Backup and Storage	A

Source: (Swindom, 2004)

Table 5-4 Technical Safeguards

Technical Safeguards (164.312)			
Standards	**Section**	**Implementation specifications**	
		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
		Integrity Controls	A
		Encryption	A

Source: (Swindom, 2004)

Table 5-5 Organizational Requirements

Organizational Requirements (164.314)			
Standards	**Section**	**Implementation Specifications**	
Business Associate contracts or other Arrangements	164.314(a)(1)	Business Associate contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	164.314(b)(1)	Implementation Specifications	
		Implement Safeguards	(R)
		Ensure Adequate Separation	(R)
		Ensure Agents Safeguard	(R)
		Report Security Incidents	(R)
Policies and Procedures and Documentation Requirements (164.316)			
Standards	**Section**	**Implementation Specifications**	
Policies and Procedures	164.316(a)		
Documentation	164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

Source: (CMMS, 2005)

Any initiative to send health information via a network requires consideration of the above legislations and principles. While securing the wired network and related infrastructure as a necessary first step to ensure regulatory compliance, mobile devices must be considered, as accessibility to health information is extended to them.

5.5 Setting an ISMS Baseline for Mobile Computing Security in Healthcare

In order to prove to customers, partners and lawmakers that recognized processes, to deal with information security threats and compliance regulations, are in place, it is imperative that an internationally acceptable information security framework, like ISO, and a healthcare industry specific standard requirement, like HIPAA is used to complement ISO. ISO 17799 has earned a reputation as the internationally acceptable *de facto* information security standard (Haworth & Pietron, 2006; Rasmussen, 2005). Furthermore, the ISO/IEC 17799 is consistent with the OECD guidelines on privacy, information security and cryptography (BSI, 2006). The ISO/IEC 17799 best practice controls are described in a way that they can be implemented in a variety of legal and cultural environments.

Although BS ISO/IEC 17799 does not prescribe particular solutions to protection of personal data privacy, it does, however, specify the security objectives that need to be achieved, whatever the implementation circumstances. In addition, ISO17799:2005 Section 11, entitled “Access control”, has a few guidelines on how to deal with a mobile computing and teleworking environment. Furthermore ISO 17799 provides accommodation for legal requirements. ISO 17799 touches on all aspects Information Security ranging from the organizational, physical and technical realms. Each clause deals with a separate topic built around administrative, technical and physical control measures as categorized in the HIPAA security rule. As shown in chapter 3, risks associated with mobile computing cut across these domains making the standards a good choice for setting up a mobile-security baseline.

The HIPAA Security Rule provides a stringent industry standard requirement when dealing with electronic health information in healthcare (Grove, 2003; Anderson, 2005). The HIPAA's rules link privacy and security; one goal of the Security Rule is to create greater coordination between the two. The link between the two shows a clear acknowledgement that the concepts of security and privacy are inextricably linked (Grove, 2003).

According to the Canadian Institute of Health Research (2001), the approach to the HIPAA Privacy Rule accords with those in many countries and with standards in the international community. The HIPAA Privacy Rule outlines general standards on the processing of health data in a manner that parallels those of the OECD Guidelines and the EU Privacy Directive. It can, therefore, be argued that the HIPAA security is well grounded in terms of ensuring the privacy and security of health information, making it an ideal choice for the mapping comparison.

Although, one might ask, why not New Zealand's Health Networking Code of Practice? The New Zealand Networking code of practice is more focused on the transmission security using technical countermeasures discussed in chapter 4 section 4.2.2. It does not cover the administrative, physical and some important aspects of the technical controls pertaining storage. The HIPAA guideline covers a broader perspective and has a level of alignment with the ISO 17799 requirement which makes a mapping exercise easier.

5.6 Conclusion

The chapter depicted that if mobile security is incorporated into ISMS, it will provide a systematic approach to managing sensitive health information that is accessible on mobile devices so that it remains secure. An ISMS policy is defined by objectives, such as legal or regulatory requirements, contractual obligations, strategic organizational and risk management contexts and risk assessment criteria as part of the process.

Since healthcare is required by national and international laws to meet the industry-specific regulatory requirements and provides provision for the security limitation, as outlined in Chapter 4, the ISMS provides the perfect platform for drafting a mobile security framework.

In order to set up a baseline that meets both the information security management requirement, as well as the healthcare-specific requirement, the ISMS should be complemented by the healthcare specific requirement. This is achieved through a mapping exercise. A mapping exercise will provide an interpretive guidance on an intended scope of standard controls, which shows whether or not the security standard scope correlates to a legal or regulatory requirement. This provides an indication whether more controls are required to meet these requirements.

In an effort to set a baseline for defining the mobile security framework model, the chapter selected the ISO/IEC 17799 to be complimented by the HIPAA Security Rule. Clearly a comparative analysis is required between these two standards in order to establish a mobile security framework model that will meet both requirements. The next chapter does a comparative analysis between these two reference standards.

Chapter 6

A Comparative Analysis of HIPAA's Final Security Rule and the ISO/IEC 17799:2005

In effort to create a framework for secure mobile computing in a healthcare environment it is imperative that healthcare regulatory requirements and information security programmes are considered. An internationally acceptable information security framework should be adopted in order to prove to customers, partners and lawmakers that recognized processes to deal with information security threats and compliance regulations are in place.

The previous chapter introduced ISO 17799 as the internationally acceptable, de facto standard for information security management. In addition, the Health Insurance Accountability and Portability Act (HIPAA), was introduced among others, as a regulatory standard capable of complementing ISO controls to meet healthcare specific requirements. As mentioned in the previous chapter, this chapter aims to use these standards together in order to create a baseline for drafting a framework model for secure mobile computing in healthcare.

This chapter, therefore, studies ISO 17799 and HIPAA in more depth. This is reported in the form of a comparison of these two standards. The comparison identifies where the standards' controls or requirements meet and discusses how they differ in strength and focus. Particular attention is paid as to how they pertain to a mobile computing environment. This will serve as input when creating the mobile security framework model in the next chapter. The chapter will begin with a section providing a brief background and structural information on the standards to be compared, before the comparison and analysis are initiated.

6.1 Structure and Format of ISO 17799:2005

ISO/IEC 17799:2005 is the latest version of the ISO standard "Information technology - Security techniques - **Code of practice for information security**

management". ISO 17799:2000 was revised and reissued in June 2005 as ISO/IEC 17799:2005. It is an internationally accepted standard of good practice for information security, serving as a starting point for organizations to begin an effective information security strategy (BS 7799, 1999; Walsh, 2001; Rasmussen, 2005). ISO 17799 is a general, advisory document. It lays out a well-structured set of controls to address information security risks, covering confidentiality, integrity and availability aspects. Organizations that adopt ISO 17799 must assess their own information security risks and apply suitable controls, using the standard for guidance.

ISO 17799:2000, adopted from the British Standard BS 7799 part 1, offered information security advice, based on ten broad security control categories. The reviewed standard has 11 control categories, with advice on risk management and incident management consolidated into one new section. The section below discusses the structure of the ISO 17799:2005 standard. ISO/IEC 17799:2005 defines information security controls in the following eleven areas as depicted in Table 6-1:

Table 6-1 ISO 17799: 2005 major areas

Security Control Clauses	**Number of Main Control objectives**
Security Policy	1
Organization of Information Security	2
Asset Management	2
Human Resources Security	3
Physical and Environmental Security	2
Communications and Operations Management	10
Access Control	7
Information Systems Acquisition, Development and Maintenance	6
Information Security Incident Management	2
Business Continuity Management	1
Compliance	3
Total	**39**

After the introduction, scope, terminology and structure sections, the remainder of ISO 17799:2005 specifies some 39 control objectives, consisting of 134 specific controls, to protect information assets against threats to confidentiality, integrity and availability. In effect, these control objectives encompass the functional requirements' specification for an organization's information security management architecture.

The sections covering legal and privacy requirements, physical security, access control secure coding and incident response have all been updated. More emphasis has been given to management responsibilities and managing human resources. There is also a new section dealing with security incidents. Also, the security issues around outsourcing and contracting with service providers are better elaborated. The new version of 17799 also provides guidance on a process to help organizations reduce risks from technical vulnerabilities, for example, patch management is now covered.

Furthermore, for the part that most concerns this project, ISO 17799 has expanded its security guidance to tackle increased mobility by adding depth to the guidance of dealing with mobile information and technology security. The section provides implementation guidelines for mobile computing and communication as well as teleworking.

The goal of ISO/IEC 17799:2005 is to provide a security architecture outline for information security management. The next section defines the structure of the HIPAA final security standards.

6.2 Structure of HIPAA Final Security Standards

With the emergence of the Internet to facilitate communications and electronic transactions, this law is intended to ensure the integrity and confidentiality of personal health information (PHI) shared electronically. The Final Security Rule requires safeguards for the protection of "electronic personal health information" (ePHI) in three general areas, with specific implementation requirements in each area. The areas and numbers of implementation requirements are:

- Administrative Safeguards - 23 implementation requirements

- Physical Safeguards - 10 implementation requirements

- Technical Safeguards - 9 implementation requirements

- Organizational Requirements – 4 implementation requirements

- Policies and Procedures and Documentation Requirements-4 implementation requirements

The HIPAA Security Rule has a total of 50 implementation requirements.

The next section compares the controls associated with ISO17799:2005 and HIPAA Final Security Rule to determine how they relate to each other and determine how the controls affect mobile computing.

6.3 Comparison of the HIPAA Final Security Standards to ISO/IEC 17799: 2005

This section compares ISO 17799: 2005 Controls and the HIPAA Security Rule control. The section will also highlight how the security controls influence a mobile computing environment.

The comparison will be initiated with the first area of controls, which is in section four of ISO17799:2005, dealing with risk assessment and treatment, followed by the subsequent sections accordingly. For each ISO control described, the relating HIPAA controls will be described denoted by ***"HIPAA"*** for conciseness and clarity. The verdict on how they affect mobile computing follows. The verdicts will be termed "Required", if controls are deemed necessary to have in a mobile computing environment and "Addressable", if not necessary. However, the addressable controls are subject to the organizational risk assessment needs and are adequately justified when not implemented.

The decisions taken in assessing the controls are influenced by the threats and vulnerabilities associated with mobile computing, discussed in Chapter 3, as well as HIPAA's security requirement specification and the recommendations of the ISMS. The comparison and decisions begin with section 4 of ISO17799: 2005. The designations for the comparison are defined in Table 6-2.

Table 6-2. Designations and meanings

Designation	Meaning
HIPAA #	**Not covered:** For the topic of concern, the ISO 17799 control is not covered at all in the HIPAA requirements
ISO > HIPAA	**Partially covered:** For the topic of concern, the ISO 17799 control exceeds HIPAA requirements
ISO ~ HIPAA	**Similar coverage:** For the topic of concern, the HIPAA requirements and ISO 17799 are approximately the same
HIPAA > ISO	**Exceed:** For the topic of concern, HIPAA includes at least one requirement not included in ISO 17799
MP	Mobile Perspective

To visually distinguish headings in ISO 17799 from headings in this dissertation the ISO 17799 headings are represented as ISO. Appendix "D" has a summary coverage of the comparison.

6.3.1 Section 4: Risk assessment and treatment

Within ISO17799:2005, Section 4 deals with having processes in place to assess security risks and to ensure that a conscious business decision is made with regards to the possible impact and possible solutions thereof.

>>4.1 Assessing Security Risks (ISO ~ HIPAA)

From an ***ISO 17799*** perspective, it is required to "periodically identify, quantify and prioritize risks against criteria for risk acceptance and objectives applicable to the organization." The ***HIPAA*** 164.308(a) (1)ii(A) "Risk Analysis" requirement that "an accurate and thorough assessment" of the risks to the "confidentiality, integrity, and availability" of electronic Personal health Information (ePHI) must be made, can be considered equivalent.

Chapter 3, section 3.1 showed that mobile devices introduce new vulnerabilities. Therefore, it is imperative that mobile devices are specifically considered when assessing security risks. As part of this exercise, the kinds of mobile devices, the services that are accessed and the ePHI that will be manipulated by these mobile devices must be considered. ***MP*** is thus rated "Required".

>>4.2 Treating Security Risks (ISO ~ HIPAA)

ISO 17799 suggests that organizations should decide on criteria that can be used to determine whether or not risk can be accepted, and then apply appropriate controls to avoid, transfer or mitigate the risk. ***HIPAA*** 164.308(a)(1)(ii)(B) "Risk Management", requires implementing security measures to reduce the risk of security breaches. As both deal with conscious decisions as to which risks must be treated, they can be considered equivalent.

Since organizations do not have unlimited resources, a control, such as the above, would definitely prioritize risks and countermeasures in terms of both risk and cost. Introducing mobile solutions into the organization will require the organization to reconsider the likelihood of certain risks.

Mobility can, therefore, result in a reprioritization. Hence ***MP*** is rated as "Required".

In brief then, mobile computing certainly can have an impact on the risks that a business faces. Therefore, the aforementioned controls need to be revisited in the context of mobility, and conscious decisions need to be taken with respect to unwarranted residual risk.

6.3.2 Section 5: Security Policy

Section 5 of *ISO 17799* deal with creating Information security policy document and review of information security policy.

>>5.1 Information Security (IS) Policy

Section 5.1 of ***ISO 17799*** recommends managements define and document policy stating their direction and support for information security.

>>5.1.1 Information security policy document (ISO ~ HIPAA)

This ***ISO 17799*** control recommends that an information security policy document be approved by management, published and communicated to all employees and relevant external parties. The ***HIPAA*** 164.316(a) requires that policies and procedures must be in place to ensure safeguards to ePHI. 164.316(b)(1) "Documentation" requires that policies, procedures, actions and activities are documented. As they both deal with security policy documentation, they can be considered equivalent.

In order to have a successful programme, management must define and document a policy to clarify their direction of and support. This is applicable to mobile security. It is required by HIPAA and it is the foundation of implementing security countermeasures. It enables control over which applications ePHI are granted network access, under what conditions, over which networks, as well as which medical personnel can receive or access them. Thus, ***MP*** is rated "Required".

>>5.1.2 Review of the information security policy (ISO ~ HIPAA)

This ***ISO 17799*** control requires that the information security policy be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness. ***HIPAA*** 164.306(e)

"Maintenance" requires an ongoing review and modification of security measures. 164.308(a)(8) "Evaluation" requires a periodic security evaluation. 164.316(b)(2)(iii) "Updates" requires a periodic review and updates to changing needs. As both deal with continuous review and updates, they can be considered equivalent.

As technology changes, the information security implications also change. As discussed in Chapter 3, mobile devices are susceptible to changes and upgrades, and new threats continue appearing everyday. A periodic review of the policy will ensure an up-to-date security control is in place to protect ePHI. Thus, rating ***MP*** as "Required".

In summary, a policy is a very important part of mobile security. It serves as a foundation of selecting controls and understanding by users and needs to be enforced. The policies must also be reviewed and updated as the technology and mobile environments change.

6.3.3 Section 6: Organization of Information Security

This section of *ISO 17799* aims to provide guidiance on managing an organization's information security.

>>6.1 Internal Organization

This section of ***ISO 17799*** controls suggests that a suitable information security governance structure be designed and implemented to initiate and control the implementation of IS within an organization.

>>6.1.1 Management commitment to information security (ISO > HIPAA)

ISO 17799 recommends that senior management should provide direction and commit their support, for example by approving information security policies, acknowledging and assigning responsibilities. ***HIPAA*** 164.308(a)(2) "Assigned Security Responsibility" requires identifying security officials responsible for policies and procedures. 164.308(a)(8) "Evaluation" requires a periodic security evaluation. 164.308(a)(3)(ii)(A)**,** "Authorization and/or Supervision". Since ISO provides and requires more activity participation by management to show commitment to information security, like ensuring implementation of information security controls is co-coordinated across the organization, and initiating training and awareness programmes, it is rated greater than HIPAA.

As an issue-specific policy relating to mobile computing is necessary, support procedures, training and awareness programmes for employees are necessary. It is also important that management identify an individual or office responsible to be responsible for policy and coordination. HIPAA denotes this control as required. Thus, ***MP*** is "Required".

>>6.1.2 Information security co-ordination (ISO > HIPAA)

This ***ISO 17799*** control suggests that information security activities be coordinated by representatives from different parts of the organization with relevant roles and job responsibilities. ***HIPAA*** 164.308(a)(2) "Assigned Security Responsibility". Since ISO provides more specific implementation guidelines for the type of responsibilities and the activities to be initiated across the organization, it is concluded that ISO is greater than HIPAA.

As mobility spans healthcare, network managers, administrators, application designers, users or caregivers should have the same security goals in mind. This requires all participants' involvement. Thus, ***MP*** is rated "Required".

>>**6.1.3 Allocation of information security responsibilities (HIPAA > ISO)**

This ***ISO 17799*** control suggests all information security roles and responsibilities should be clearly defined. ***HIPAA*** 164.308(a)(2) "Assigned Security Responsibility" requires the same. Although ISO specifies that security responsibility can be allocated to a single person or a group, HIPAA specifically requires that a single person be responsible for both Information and physical security. Hence HIPAA is considered greater than ISO.

It is important that an office or an individual be responsible for a mobile security policy in case questions regarding the policy arise, as well as ensuring adherence to the policy to meet requirements. Furthermore, the HIPAA requirement designates the control as required. Thus, ***MP*** is rated as "Required".

>>6.1.4 Authorization process for information processing facilities (ISO ~ HIPAA)

This ***ISO 17799*** control requires that a management-authorization process for new information processing facilities be defined and implemented. ***HIPAA*** 164.308(a)(1)(i) "Security Management Process" requires the implementation of policies and procedures to prevent, detect, contain and correct security violations. 164.308(a) (1)ii(A)) "Risk Analysis" requires that vulnerability assessment is conducted on the Confidentiality, Integrity and Availability of ePHI. Since both require approval processes before new facility use, they can be considered equivalent.

Mobility attracts and enhances the use of rogue mobile or wireless devices by users. Furthermore, when users provide new or personally owned devices, as discussed in Chapter 3, they are likely to introduce new vulnerabilities. It is necessary to have controls or processes to authorize what devices are allowed to access or process ePHI. Thus, ***MP*** is rated as "Required".

>>6.1.5 Confidentiality agreements (ISO ~ HIPAA)

This ***ISO 17799*** control requires confidential or non-disclosure agreements, reflecting the organization's needs for the protection of information to be clearly defined and regularly reviewed. The ***HIPAA*** 164.308(a)(3)(i) "Workforce Security" requires the implementation of policies and procedures to ensure appropriate PHI access. 164.314(a)(1) "Business Associate Contracts or Other Arrangements" requires that an organization must ensure its business associates safeguard PHI. 164.308(a)(1)(ii)(B) "Risk Management", as discussed in Section 6.4, is required to identify classified information. Since these control areas relate to protecting confidential information through agreement signatures, they can be considered equivalent.

As the information that can be accessed by mobile devices in a healthcare environment is ePHI, users must be tight with secrecy to avoid unauthorized disclosure. It also involves the right to audit and monitor activities that involve confidential information, as discussed in Chapter 4.

Hence ***MP*** is rated as "Required".

>>6.1.6 Contact with authorities (*HIPAA #*)

This ***ISO 17799*** control requires that appropriate procedures to make contact with relevant authorities should be maintained, for example, law enforcement, the fire department or supervisory authorities. It also requires procedure for security incident reporting in a timely manner, if laws are suspected of being broken. Maintaining contacts with regulatory bodies is useful to anticipate upcoming changes in laws or regulations, which have to be followed by an organization. The HIPAA requirement has no such specification, hence, HIPAA can be considered "Null".

One of the problems of mobile computing is that the sizes of the devices involved make them susceptible to theft and loss. Lost or stolen mobile devices are a more likely cause of financial loss than malicious attacks from outside an organization, as discussed in Chapter 3, Section 3.3.1.1. In case of theft or a loss of a mobile device, relevant authorities can be contacted in order to trace or deactivate the device or track down the culprit, although organizations can invest in a remote wipe to prevent unauthorized data from being leaked when a device is lost or stolen. Thus, ***MP*** is termed "Addressable".

>>6.1.7 Contact with special interest groups (ISO > HIPAA)

This ***ISO 17799*** control requires that contacts with special interest groups or other specialist security forums and professional associations should be maintained. The ***HIPAA*** 164.314(b)(2)(iv) "Report Security Incidents" requires health plan sponsors report breaches to health plans. Since ISO requires contacts with professionals and other security forums by a covered entity, ISO can be considered greater than HIPAA.

Today's mobile devices come with operating systems and are able to run enterprise-wide applications. These devices require security update patches or operating system or applications vulnerability patches, as well as warnings pertaining to attacks or vulnerabilities. Also, when organizations discover new vulnerabilities, they should be reported to the SIGs to accelerate solutions. Thus, ***MP*** is rated "Required".

>>6.1.8 Independent review of information security (ISO ~ HIPAA)

The ***ISO 17799*** control states that an organization approach to managing information security and its implementation should be reviewed independently at planned intervals, or when a significant change to the security implementation occurs. The ***HIPAA*** 164.308(a)(8) "Evaluation" states that there must be periodic security evaluations. Since both controls require periodic evaluation of information security, they can be considered equivalent.

As stated above, because mobility in healthcare concerns ePHI, surely such an exercise will ensure appropriate mobile security implementation compliance to policy as well as identification of flaws that need to be fixed. Hence ***MP*** is rated as "Required".

In brief, mobile devices and wireless networks have infiltrated health organizations. Ensuring security within an organization is as important as security from external intruders. As discussed in Chapter 3, authorized users with access to the facility can pose the biggest threats to an organization.

>>6.2 External Parties

Section 6.2 of ***ISO 17799*** aims to maintain the security of the organization's information and information facilities that are accessed, processed, communicated to, or managed to external parties.

>>6.2.1 Identification of risks related to external parties (ISO ~ HIPAA)

This ***ISO 17799*** control recommends that risks to an organization's information and information processing facilities from business processing involving external parties be identified, and appropriate controls implemented before granting access. The ***HIPAA*** 164.308(b)(1) "Business Associate Contracts (BACs) and Other Arrangements" and 164.308(a)(1)(ii)(A) "Risk Analysis" require risk assessment of third parties. Since they both refer to risk assessment pertaining to third parties, they can be considered equivalent.

Mobility enables anywhere, anytime access which means easy collaboration with partners such as health plans and healthcare providers and easier access to ePHI. It is important that third-party security is as good as the covered entity. Security is only as strong as its weakest link. Hence ***MP*** is rated as "Required".

>>6.2.2 Addressing security when dealing with customers (ISO > HIPAA)

This ***ISO 17799*** control requires that all identified security requirements be addressed before giving customers access to an organization's information asset. ***HIPAA*** 164.308(b)(1) (Business Associate Contracts (BACs) and Other Arrangements) requires that a covered entity must implement BACs to ensure safeguards. Since HIPAA requires security in place, but does not specifically specify that security requirement be addressed before granting access to customers, ISO is considered greater than HIPAA.

Mobile devices and wireless telecommunication networks enhance customer's access to information. It is vital that security is in place to avoid compromise, which can lead to legal liabilities, before access is established. Hence, ***MP*** is rated as "Required".

>>6.2.3 Addressing security in third-party agreements (ISO ~ HIPAA)

This ***ISO 17799*** control requires that agreements with third parties involving accessing, processing, communicating or managing an organization's information or information processing facilities should cover relevant security requirement. The ***HIPAA*** 164.308(b)(1) "Business Associate Contracts (BACs)" and Other Arrangements and164.308(b)(4) "Written Contract and Other Arrangements" require compliance to BACs. 164.314(b)(2)(iii) "Ensure Agents Safeguard" ensures subcontractors safeguard PHI. 164.314(b)(2)(i)" Implement Safeguards" requires plan sponsors to implement safeguards as appropriate. Since all the controls require third-party agreement safeguards in all the factors, the controls can be considered equivalent.

Providing quality healthcare usually involves collaborators and researchers dependent on remote access to a covered entity. Mobile computing fosters access to services and ePHI. It is imperative that they follow the same security measures. In the event of a loophole, in a third-party's security, it can be used as a platform for an attack, in this case, access to ePHI through clearing houses or heath plans. Hence ***MP*** is rated "Required".

In brief, it is important that information accessed, processed, transmitted and stored by third parties is protected. As mobile computing enhances such processes, it is imperative that third-party security is looked into.

6.3.4 Section 7 Asset Management

This section of ***ISO 17799*** aims to manage an organization's assets.

>>7.1 Responsibility for Assets

Section 7.1 of ***ISO 17799*** recommends that an organization should be in a position to understand what information assets it holds and manage its security appropriately.

>>7.1.1 Inventory of assets (ISO > HIPAA)

This ***ISO 17799*** control requires that all assets be clearly identified, and an inventory of all important assets drawn up and maintained. ***HIPAA*** 164.308(a)(7)(ii)(E) "Applications and Data Criticality Analysis" requires prioritizing data and system criticality for contingency planning. 164.310(d)(2)(iii) "Accountability" requires documenting hardware and any electronic media movement and the persons responsible. Since ISO requires all inventories of assets to be identified and documented, and HIPAA requires that the documentation is based on the movement of hardware and media only, ISO can be considered greater than HPAA.

An inventory of assets is necessary to detect theft and misappropriation and to establish IT general controls. It serves as a starting point to develop the more focused documentation needed to identify points of vulnerability. Devices, people, facilities and many more are considered as assets to an organization. In this case, mobile devices, the backend systems that support them and the ePHI information they access should be considered as assets and, therefore, must be protected. Hence, MP is rated as "Required".

>>7.1.2 Ownership of assets (HIPAA > ISO)

This ***ISO 17799*** control requires that all Information and assets associated with information processing facilities should be owned by a designated part of an organization. ***HIPAA*** 164.308(a)(2) "Assigned Security Responsibility" requires single individual to be designated as having overall responsibility for the security of a covered entity's ePHI. Since the HIPAA requirement provides a more stringent requirement that an individual be responsible for security of EPHI, HIPAA can be considered greater than ISO.

An owner, and the custodian of the data, lets one identify the appropriate access policies and security measures that should be applied. To fully achieve mobile security, it is important that a group or an individual is responsible, in order to properly classify the information (ePHI), review access restriction and access control policies. Hence, ***MP*** is rated as "Required".

>>7.1.3 Acceptable use of assets (HIPAA > ISO)

This ***ISO 17799*** control requires that rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented and implemented. This rule must be followed by employees, contractors and third-party users. ***HIPAA*** 164.308(b)(1) "Business Associate Contracts and Other Arrangements", 164.308(b)(4) "Written Contract", and 164.314(a)(1) "Business Associate Contracts or Other Arrangements" require obligations by employees, third parties and contractors. Since HIPAA clearly states what actions need to be taken in an event of violation, it can be considered greater than ISO.

It is important that guidelines for the use of mobile devices, within and outside the organization, are adhered to, as well as the rules for electronic mail and Internet usage, such as access to a clinical database online and access ePHI to achieve mobile security. Hence, ***MP*** is rated as "Required".

In brief, by understanding what information assets, physical assets, such as mobile devices, and the users that are directly responsible for them, can help in managing security appropriately. Usually this information is useful in logging any security relevant event, which will map to a user.

>>7.2 Information Classification

This section of ***ISO 17799*** controls ensures that information receives an appropriate level of protection.

>>7.2.1 Classification guidelines (ISO > HIPAA)

This ***ISO 17799*** control requires that Information should be classified in terms of its value, legal requirement, sensitivity and criticality to the organization. ***HIPAA*** 164.308(a)(7)(ii)(E) "Applications and Data Criticality Analysis" requires prioritizing data and system criticality analysis for contingency planning. Since HIPAA requires only criticality analysis for contingency planning, ISO can be considered greater than HIPAA.

The classification will ensure access control and provide security guidelines for handling ePHI on a mobile device. Besides, not all information or applications in healthcare are considered critical; they may not require the same level of security. Hence, ***MP*** is stated as "Required".

>>7.2.2 Information labeling and handling (ISO > HIPAA)

This ***ISO 17799*** control requires that appropriate sets of procedures be defined for information labeling and handling, in accordance with the classification scheme adopted by the organization. ***HIPAA*** 164.308(a)(4) "Information Access Management" requires implementing policies and procedures for authorizing access to protected information. HIPAA does not specifically specify anything about labeling information. It only has a procedure's requirement set out for only access control of information, which is nearly like the "handling" required by ISO. ISO requires procedures in place for information labeling and handling, as such, ISO can be considered greater than HIPAA.

Labeling of information can determine handling procedures for access, secure processing, storage, and transmission of information on mobile devices. Hence, ***MP*** is rated as "Required".

In brief, by classifying information, establishing labeling and handling procedures can ensure that information or relevant applications receive an appropriate level of protection. This will also help in specifying certain types of mobile devices to access sensitive information, because the processing capacities of the devices are known to handle security algorithms.

6.3.5 Section 8: Human Resources Security

This section of ISO 17799 aims to manage employees, contractors and third parties users.

>>8.1 Prior to Employment

This ***ISO 17799*** control ensures that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and reduces the risk of theft, fraud or misuse of facilities.

>>8.1.1 Roles and responsibilities (ISO > HIPAA)

This ***ISO 17799*** control recommends that security roles and responsibilities of employees, contractors and third-party users should be defined and documented in accordance with an organization's information security policy. ***HIPAA*** 164.308(a)(3)(ii)(A), "Authorization and/or Supervision" requires authorization or supervision for PHI access. Since HIPAA does not specify prior definition and documentation of third-parties' responsibilities and focuses mainly on the authorization and supervision, ISO can be considered greater than HIPAA.

Defining and documenting roles and responsibilities of employees and other third parties will surely keep mobile users abreast of meeting policy requirements. This will help in the authorization process and tracking of activities, as well as controlling users' misuse of information. Since any user requires management authorization before access to ePHI can be granted, ***MP*** can be rated as "Addressable".

>>8.1.2 Screening (ISO > HIPAA)

This ***ISO 17799*** control requires that background verification checks on all candidates for employment, contractors, and third-party users, which should be carried out in accordance with laws, regulations and ethics. ***HIPAA*** *164.308(a)(3)(ii)(B)* "Workforce Clearance Procedure" is a dimly-worded requirement that relates to the process for deciding that a particular worker can be trusted with ePHI. Since ISO outlines specifically the kinds of reference and appropriate credit checks which should be required, ISO rates greater than HIPAA.

Since only confirmed practicing caregivers should have access to ePHI, and it is assumed that only already evaluated third parties and personnel will be authorized certain privileges to information, MP is rated "Addressable".

>>8.1.3 Terms and conditions of employment (ISO ~ HIPAA)

This ***ISO 17799*** control requires that employees, contractors, and third-party users agree to sign the terms and conditions of employment contracts. This states their obligation to information security. ***HIPAA*** 164.308(a)(1)(ii)(C) "Sanction Policy" requires workers' sanctions for policies and procedures violations. Since they both require obligations from employees or third parties, they can be considered equivalent.

Following safe computing procedures is an important aspect of mobile computing security. Commitment by users to extend responsibilities to outside the organization premises while practicing remote access reduces security risks. Hence ***MP*** is rated as "Required".

In brief, contractors, and third party users of information processing facilities like mobile devices and WLANs should sign agreement on their security roles and responsibility.

>>8.2 During Employment

This ***ISO 17799*** control suggests that managements' responsibilities regarding information security should be defined. Employees, contractors and third-party users are made aware, educated and trained in security procedures. Also, a formal disciplinary process is established to handle security breaches.

>> 8.2.1 Management responsibilities (ISO ~ HIPAA)

This section of ***ISO 17799*** control recommends that management should require employees, contractors and third-party users to apply security in accordance with established policies and procedures of an organization. ***HIPAA*** 164.308(a)(2) "Assigned Security Responsibility" 164.308(b)(1), 164.308(b)(4) "Written Contract", and 164.314(a)(1) "Business Associate Contracts or Other Arrangements". Since all the controls add up to require user commitment in compliance with organizational policies, they can be considered equivalent.

Mobile users both within and outside the organization must work in accordance to the organizational policy to show their commitment to compliance and reduce potential risks. Hence ***MP*** is rated "Required".

>>8.2.2 Information security awareness, education and training (ISO ~ HIPAA)

This ***ISO 17799*** control requires that all employees of the organizations receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. ***HIPAA*** 164.308(a)(5)(i) "Security Awareness Training" requires implementing a security awareness and training programmes for all members of the workforce, including management and executives". Since both require security awareness and training, they can be considered equivalent.

Understanding the possible threats and vulnerabilities of mobile computing by users is important for building successful mobile security. Training is required for personnel using mobile computing to raise their awareness on the additional risks resulting from working with mobile devices. At the same time it provides them with knowledge about incident reporting. Security reminders are very much required to inform users of new threats and also to remind them of the importance of securing devices. It is important to note that mobile devices can serve as security reminder platforms for users, creating a wider awareness. Hence, ***MP*** is rated "Required".

>>8.2.3 Disciplinary processes (ISO ~ HIPAA)

This ***ISO 17799*** control requires that organizations have formal disciplinary processes for employees who have committed security breaches. ***HIPAA***, 164.308(a)(1)(ii)(C) "Sanction Policy" requires workers' sanctions for violations of policies and procedures. Both controls deal with outing actions in place to deal with security breaches, and therefore, can be considered equivalent.

Revocation of access rights and privileges, as well as the return of organization mobile device(s), should in part of a mobile security policy as actions to be taken in an event of misconduct. Such a process will remind users to follow the safe computing procedures provided. Monitoring user activity is an important part of the process to align responsibility of an action. Hence, ***MP*** is rated as "Required".

In brief, an adequate level of awareness, education and training in security procedures and correct use of mobile devices should be provided to employess, contractors and third party users to minimize risks. A formal disciplinary process for handling security breaches should be in place.

>>8.3 Termination or Change of Employment

This section of ***ISO 17799*** ensures that employees, contractors and third-party users exit an organization or change employment in an orderly manner.

>>8.3.1 Termination responsibilities (HIPAA #)

This ***ISO 17799*** control requires that responsibilities for performing employment terminations or changes of employment be clearly defined and assigned. HIPAA does not specify that such responsibility be assigned. Hence, making HIPAA "Null".

Having a process for terminating responsibilities in place will help identify which parties are in possession of organizations' mobile devices or can access sensitive information remotely. This will ensure all rights and access to assets are revoked appropriately. Hence, ***MP*** is rated as "Required".

>>8.3.2 Return of Assets (HIPAA #)

This ***ISO 17799*** control requires that all employees, contractors and third-party users should return all of an organization's assets in their possession upon termination of their employment, contract or agreement. HIPAA has no such specification, and, as such, HIPAA is "Null".

Since mobile devices and the information that they may contain are classified as assets, they should be returned in an event of termination or change of employment or contract. However, if users are allowed to keep such devices, in that situation a proper "wipe clean device memory" strategy should be in place. Hence, ***MP*** is rated as

"Addressable".

>>8.3.3 Removal of access rights (ISO ~ HIPAA)

This ***ISO 17799*** control requires that all user access rights to information and information processing facilities be removed upon termination of their employment, contract or agreement, or adjusted to change***. HIPAA*** 164.308(a)(3)(ii)(C) "Termination Procedures" requires procedures to end PHI access upon termination of employment. Since they both require removal of access rights to leaving employees or contractors, they can be considered equivalent.

The mobile workforce usually has remote access to critical information or ePHI via their devices. They can serve as potential threats to an organization once they have left it. Hence, ***MP*** is rated as "Required".

In brief, at the point of employment or after employment, managements should ensure that there are processes in place to ensure that users understand organizations' security objectives as well as the repercussions for violating any of them. Also, at the point of termination of appointment, there should be in place processes to ensure users do not have any affiliation with the organization's information or assets. This will mitigate potential threats and vulnerabilities. This is certainly important to control the mobile workforce.

6.3.6 Section 9: Physical and Environmental Security

This section of *ISO 17799* aims to provide guidiace on physical and environmental security.

>>9.1 Secure areas

Section 9.1 of ***ISO 17799*** aims to prevent unauthorized physical access, damage and interference to an organization's premises and information

>>9.1.1 Physical security perimeters (ISO ~ HIPAA)

This ***ISO 17799*** control requires security perimeters. Barriers, such as walls, card-controlled entry gates or manned reception desks, should be used to protect areas that contain information and information processing facilities. ***HIPAA*** 164.310(a)(2)(ii) "Facility Security Plan" requires policies and procedures to safeguard equipment and facilities. Since the two require setting up measures to protect equipment and facilities, they can be considered equivalent.

It is the absence of physical access controls that make risk profiles of mobile devices different from desktop ones. A malicious user can physically insert a rogue AP into hidden area within a building, allowing unauthorized individuals to gain access to a network. Proper physical countermeasures mitigate some of the biggest risks, such as theft of equipment (mostly mobile devices) and insertion of rogue access points, handhelds or wireless network monitoring devices. Hence, ***MP*** is rated "Required".

>>9.1.2 Physical entry controls (ISO ~ HIPAA)

This ***ISO 17799*** control requires that secure areas be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. ***HIPAA*** 164.310(a)(2)(iii) "Access Control & Validation Procedures" requires facility access procedures in place for personnel. Here is also 164.310(a)(2)(ii) "Facility Security Plan". The two standards, controls are referred to as personnel access security, therefore, they can be considered equivalent.

Acess to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only. Personnel area communication might be fully wireless in close proximity. (See 9.1.1.) Hence, ***MP*** is rated as "Required".

>>9.1.3 Securing offices, rooms and facilities (ISO ~ HIPAA)

This ***ISO 17799*** control requires physical security for offices, rooms and facilities to be designed and applied. **HIPAA** 164.310(a)(2)(iii) "Access Control & Validation Procedures", 164.310(a)(2)(ii) "Facility Security Plan" and 164.310(b) "Workstation Use" require policies and procedures to specify workstation environment and use. 164.310(c) "Workstation Security" requires physical safeguards for workstation access. Since they both require physical security plans, they can be considered equivalent.

Designing and applying physical security plans for restricted areas is important. There should be some distance limitation associated with the wireless access technology that needs to be considered. There should be in place policies and procedures to specify the use of hot spots or the use of ad-hoc wireless networks. Hence, ***MP*** is rated as “Required”.

>>9.1.4 Protecting against external and environmental threats (ISO ~ HIPAA)

This ***ISO 17799*** control requires that physical protection against damage from fires, floods, earthquakes, explosions, civil unrest and other forms of natural or man-made disasters should be designed and applied. **HIPAA** 164.308(a)(1)(ii)(B) “Risk Management” requires implementing security measures to reduce risk of security breaches. Since they both refer to reducing risks, they can be considered equivalent.

While the backend system offering support to the mobile workforce resides at the organization premises, it is important that it is protected. A risk analysis will determine how protecting against these factors will be implemented to protect mobile facilities. Hence, ***MP*** is rated “Required”.

>>9.1.5 Working in secure areas (ISO ~ HIPAA)

This ***ISO 17799*** control requires that physical protection and guidelines for working in secure areas should be designed and applied. ***HIPAA*** 164.310(a)(2)(iii) “Access Control & Validation Procedures”, 164.310(a)(2)(ii) “Facility Security Plan” ,164.310(b) “Workstation Use” and 164.310(c) “Workstation Security” Since the controls all require that procedures for working in secure areas be in place, they can be considered equivalent.

To have a safe computing process in place, mobile or wireless users must understand how to perform their activities in a secure way and in the right physical location to use to avoid unnecessary risks. Wireless signals might travel beyond certain proximity (secure area) making them susceptible to attack. Hence, ***MP*** is rated “Required”.

>>9.1.6 Public access, delivery and loading areas (ISO ~ HIPAA)

This ***ISO 17799*** control recommends that areas where unauthorized persons may enter the premises should be controlled. ***HIPAA*** 164.310(a)(2)(iii) "Access Control & Validation Procedures" and 164.310(a)(2)(ii) "Facility Security Plan" both require illegal access to organizations' facilities be checked, so they can be considered equivalent.

As mentioned, physical access is an important aspect of mobile security. Hence, ***MP*** is rated "Required".

In brief, one of the important aspects of mobile computing security is physical security. Access to the organization's wireless networks can be detrimental. When there is an open access entry to facilities, theft of devices, imposter or rogue access point deployment can be very easy.

>>9.2 Equipment Security

The objective of Section 9.2 of ***ISO 17799*** is to prevent loss, damage, theft or compromise of assets and the interruption to an organization's activities.

>>9.2.1 Equipment siting and protection (ISO > HIPAA)

This ***ISO 17799*** control requires that equipment be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. ***HIPAA*** 164.310(b) "Workstation Use" 164.310(c) "Workstation Security" and 164.310(a)(2)(ii) "Facility Security Plan". Since ISO provides guidelines on reducing the possible environmental threats and hazards, it can be considered greater than HIPAA.

Wireless access points should be situated in secure areas to prevent theft or damage. Predicting access point coverage to avoid unnecessary signal overlap is a necessary step to take. Users should be reminded of safe computing procedures at hotspots or public areas. Hence, ***MP*** is rated "Required".

>>9.2.2 Support utilities (ISO > HIPAA)

This ***ISO 17799*** control requires equipment to be protected from power failures and other disruptions caused by failures in supporting utilities.
HIPAA 164.310(a)(1)(ii) "Facility Access Control". Since HIPAA cautions that continuous access should be provided without interruption for some

users but does not specify the elements, or how that will be achieved, ISO can be considered greater than HIPAA.

Supporting utilities, such as electricity and air conditioning, should be adequate for the systems supporting mobile computing processes to enhance availability. Hence, ***MP*** is rated “Required”.

>>9.2.3 Cabling security (ISO > HIPAA)

This ***ISO 17799*** control requires that the power and telecommunications cable carrying data or supporting information services is protected from interception or damage. ***HIPAA*** 164.310(a)(2)(ii) “Facility Security Plan” requires planning of policies and procedures to prevent "unauthorized physical access, tampering, and theft" from facilities containing or having access to ePHI. Although cables can be related to a processing facility in terms of HIPAA, it does not specifically state cabling security and implementation. ISO can be considered greater than HIPAA.

Cables running from the switch to a wireless access point or to a mast radio can be susceptible to attack. Hence, ***MP*** is rated “Required”.

>>9.2.4 Equipment maintenance (HIPAA > ISO)

This ***ISO 17799*** control ensures that equipment is correctly maintained to ensure its continued availability and integrity. ***HIPAA*** 164.310(a)(2)(ii) “Facility Security Plan”, 164.310(a)(2)(iii) “Access Control & Validation Procedures” and 164.310(a)(1) “Facility Access Controls” require policies and procedures to limit access to systems and facilities. 164.310(d)(2)(iii) “Device and Media Controls” requires policies and procedures to govern receipt and removal of hardware and media. 164.310(d)(2)(iv) “Data Backup and Storage” requires backup of PHI before moving equipment. 164.306(e) “Maintenance” although similar in many aspects, HIPAA does require that information is backed up before equipment is moved, in this case before maintenance activity takes place; it can be considered greater than ISO.

Facility equipment providing wireless and mobile services, such as the backend systems and mobile devices and their applications need to be maintained to ensure availability and integrity. Hence, ***MP*** is rated

"Required".

>>9.2.5 Security of equipment off premises (ISO ~ HIPAA)

This ***ISO 17799*** control requires that security be applied to off-site equipment, taking into account the different risks of working outside of organizations' premises. ***HIPAA*** 164.310(a)(2)(ii) "Facility Security Plan" and 164.310(d)(2)(iii) "Accountability" require documentation for hardware and media movement. Since both ISO and HIPAA require that the security of internal or external equipment accessing the network be kept at all times, ISO and HIPAA can be considered equivalent.

Mostly, mobile devices operate outside an organization perimeter and continually access corporate information, In this case, ePHI. It is imperative that on-device protection is enabled and care taken when using mobile devices in public areas. Mobile device use must be authorized. Another from of mobility is home access. Hence, ***MP*** is rated "Required".

>>9.2.6 Secure disposal or re-use of equipment (ISO ~ HIPAA)

This ***ISO 17799*** control requires that equipment containing storage media be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. ***HIPAA*** 164.310(d)(2) "Media Re-use" requires policies and procedures to remove PHI from media and equipment before reuse. 164.310(a)(2)(ii) "Facility Security Plan" and 164.310(d)(2)(i) "Disposal" require policies to manage media and equipment disposal . Since ISO and HIPAA both require secure disposal policies and procedures in place, they can be considered equivalent.

As mobile devices are capable of storing sensitive Information (ePHI), they should be successfully wiped or overwritten before disposal or reuse. Unwiped or cleared disposed disks can be susceptible to dumpster driving. Hence, MP is rated "Required".

>>9.2.7 Removal of property (ISO ~ HIPAA)

This ***ISO 17799*** control requires that equipment, information or software should not be take off-site without prior authorization. ***HIPAA*** 164.310(d)(2)(iii) "Accountability" requires the maintenance of records, including the responsible party for the movements of hardware and electronic media. Since they both require proper authorization to move assets, they can be considered equivalent.

Information copied onto a mobile device and taken off-site needs to be authorized. Authorization processes for the type of information to be copied to a device and what personnel should be in place, to maintain access control. Hence, ***MP*** is rated as "Required".

In brief, securing mobile devices is an important part of achieving overall mobile computing security. It is important that proper authorization is given on the type of information being stored on mobile devices, and users must be aware of the possible threats to these devices. It is vital that procedures and processes are in place to prevent unauthorized physical access, damage and interference to an organization's premises and information, especially with the challenges of wireless networks.

6.3.7 Section 10 Communications and Operating Management

This section of ***ISO 17799*** aims to provide guidance on communication and operational management.

>>10.1 Operational Procedures and Responsibilities

This section of ***ISO 17799*** aims to ensure the correct and secure operation of information processing facilities.

>>10.1.1 Documented operating procedures (ISO ~ HIPAA)

This ***ISO 17799*** control requires that operating procedures should be documented, maintained and made available to all users who need them. ***HIPAA*** 164.316(b)(2)(ii) "Availability" requires that documented procedures be available to users and administrators.

Mobile users sometimes do not follow safe mobile computing procedures. Procedures should be in place to guide users on how to securely handle organizational resource or access. It is important that these procedures are made available to users. Hence, ***MP*** is rated "Required".

>>10.1.2 Change management (HIPAA #)

This ***ISO 17799*** control requires that changes to information processing facilities and systems should be controlled. HIPAA has no such control as such it is considered “Null”.

Changes may create vulnerabilities in an organization. For example, the introduction of new devices or changes to mobile applications' development at the operational stage may have a negative impact on reliability and availability of application or information. Hence, ***MP*** is rated “Required”.

>>10.1.3 Segregation of duties (HIPAA #)

This ***ISO 17799*** control requires that duties and areas of responsibility should be separated in order to reduce opportunities for unauthorized modification or misuse of information, or services. HIPAA has no such control; as such, it is considered “Null”.

Separation of responsibilities and duties can help secure information when authorization processes and access controls are in place. For instance, when assigning caregivers to groups of patients for which they will be responsible, this can reduce opportunities for unauthorized modification or misuse of ePHI. Hence, ***MP*** is rated “Addressable”.

>>10.1.4 Separation of development, test and operational facilities (HIPAA #)

This ***ISO 17799*** control requires development, test, and operational facilities be separated to reduce the risks of unauthorised access or changes to operational systems.

Vertical mobile application should be well tested, and the rules for development testing and operational status should be well defined and separated. This will help in tracking vulnerabilities and possible threats. This strategy is most important in a clinical environment. Hence, ***MP*** is rated as “Required”.

In brief, responsibilities and procedures for management and operation of mobile computing should be established. Segregation of duty should be implemented where appropriate, to reduce the risks of negligence or deliberate misuse.

>>10.2 Third-Party Service Delivery Management

Section 10.2 of ***ISO 17799*** aims to implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

>>10.2.1 Service delivery (ISO ~ HIPAA)

This ***ISO 17799*** control requires measures to be taken to ensure that the security controls, service definitions and delivery levels, included in the third-party service delivery agreement, are implemented, operated and maintained by a third party. ***HIPAA*** 164.308(b)(1) "Business Associate Contracts and Other Arrangements", 164.308(b)(4) "Written Contract" and 164.314(b)(1) "Requirements for Group Health Plans". Plan documents must reflect security safeguards. Since they all require measures to check third-party compliance, they can be considered equivalent.

Since third parties are common in the healthcare environment for collaboration and research purposes, they should definitely follow safe mobile computing procedures when dealing with ePHI. The review of third-party, service-delivery security should provide satisfactory assurance that they have measures in place to protect information accessible on mobile devices. Hence, ***MP*** is rated "Required".

>>10.2.2 Monitoring and review of third-party services (ISO > HIPAA)

This ***ISO 17799*** control requires services, reports and records provided by third parties to be regularly monitored and reviewed, and audits should be carried out regularly. ***HIPAA*** 164.308(b)(1) "Business Associate Contracts and Other Arrangements" and 164.314(a)(2) Business Associate Contracts). Since HIPAA requires action to be taken if a third party is not safeguarding the information as required, there must be a way to check if the third party meets requirement. Although HIPAA does not specify what should be monitored or reviewed, it is assumed. Since ISO does have in place what is to be monitored and reviewed, ISO can be considered greater than HIPAA.

As long as third parties are allowed access to privileged information of an organization, they must protect it. Since mobility enhances such broader access capability for health plans, etc, monitoring and reviewing are very important for identifying threats and vulnerabilities associated with third parties. Hence, ***MP*** is rated "Required".

>>10.2.3 Managing changes to third-party services (HIPAA #)

This ***ISO 17799*** control requires changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, so that they are managed, taking into account the criticality of the business process involved, and can be reassessed. ***HIPAA*** does not mention specifically managing changes to third-party services.

Third-party services may require new mobile applications to be deployed, changes and enhancements to networks and adoption of new products. An assessment of such changes should be carried out and should influence the review of security policies, procedures and controls. Hence, ***MP*** is rated "Required".

In brief, healthcare organizations should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that services delivered on mobile devices meet all requirements agreed with the third party.

>>10.3 System Planning and Acceptance

This section of ***ISO 17799*** intends to minimize the risks of system failures. It ensures the availability of adequate capacity and resources to deliver the required system performance.

>>10.3.1Capacity management (HIPAA #)

This ***ISO 17799*** control requires that resources be monitored, and projections of future capacity requirements be made, to ensure system performance. HIPAA does not have any specification covering this requirement, hence, HIPAA is "Null".

Since technology is not foolproof, problems do occur. Questions like, Can the infrastructure handle the load? What happens if a system goes down? Can the system support an increasing number of applications and an increasing population of caregivers as needed? For instance, caregivers could try to submit charges from their PDAs simultaneously. Monitoring and scalability are required, Hence, ***MP*** is rated "Required".

>>10.3.2 System acceptance (HIPAA #)

This ***ISO 17799*** control aims to ensure that system acceptance criteria are established for new information systems, upgrades and new versions, and suitable tests are carried out prior to acceptance. These are not covered by HIPAA, and, as such, are deemed "Null".

When new mobile applications are developed or changes are made in any aspect of the technology; the systems should be checked for security weaknesses before acceptance or deploying the application or solution. Hence, ***MP*** is rated "Required".

>>10.4 Protection against malicious and mobile code

Section 10.4 of ***ISO 17799*** is intended to protect the integrity of software information.

>>10.4.1 Controls against malicious code (ISO ~ HIPAA)

This ***ISO 17799*** control requires detection prevention and recovery controls to protect against malicious codes, and appropriate user awareness procedures should be developed and implemented. ***HIPAA*** 164.308(a)(5)(ii)(b) "Protection Against Malicious Software" requires procedures to guard against malicious software. 164.312(a)(1) "Access Control" requires technical (administrative) policies and procedures to manage PHI access. Since all controls are aimed at malicious codes, they can be considered equivalent.

As malicious codes are becoming rampart on mobile devices and are having the same negative effect as they would in a normal desktop environment, protection is required. User awareness is an important process of educating and reminding mobile users about the flaws. Hence, ***MP*** is rated "Required".

>>10.4.2 Controls against mobile code (HIPAA #)

This ***ISO 17799*** control aims to ensure that only authorized mobile code is used. Configuration should ensure that authorized mobile code operates according to security policy, and unauthorized mobile code (software mobility, commonly known as mobile agents) is prevented. This is not covered in HIPAA, and, as such, it is deemed “Null”.

Mobile code is an important aspect of ubiquitous computing as discussed in Chapter 1. Securing mobile code is an important aspect of secure mobile computing. Hence, ***MP*** is rated “required”.

>>10.5 Back-up

This section of ***ISO 17799*** aims to maintain the integrity and availability of information as well as information processing facilities.

>>10.5.1 Information back-up (HIPAA > ISO)

This ***ISO 17799*** control requires that back-up copies of information and software be taken and tested regularly in accordance with agreed back-up policy. ***HIPAA*** 164.308(a)(7)(ii)(a) “Data Back-Up Plan” requires data back-up planning and procedures. 164.310(d)(2)(iv) “Data Backup and Storage” requires the back-up of ePHI before moving equipment. Since ISO does not specifically spot out considerations for back-ups before the movement of equipment, HIPAA can be considered greater than ISO.

Most often, mobile devices are the first input point of information by mobile users. Information collected should be synchronized to a central back-up facility to prevent loss of information in an event of loss or theft of a device. Hence, ***MP*** is rated “Required”.

>>10.6 Network Security Management

This section of ***ISO 17799*** ensures the protection of information in networks as well as the supporting infrastructure.

>>10.6.1 Network controls (ISO > HIPAA)

This ***ISO 17799*** control requires that networks be adequately managed and controlled to protect from threats and to maintain security for the systems, applications and services using the network, including the information in transit. ***HIPAA*** 164.312(e)(1) “Transmission Security” These requirements deal with the need to protect ePHI in transit over communication networks. Since HIPAA has only transmission security, ISO can be considered greater than HIPAA.

As mobile networks deal with information in transit within and across the boundaries of an organization, they access applications remotely. It is important that a network is managed and controlled to protect from threats. Hence, ***MP*** is rated "Required".

>>10.6.2 Security of network services (ISO > HIPAA)

This ***ISO 17799*** control requires that security features, service levels and management requirements of all network services are identified and included in any network services agreement. Service providers should manage agreed services in secure ways. They should be regularly monitored, and agree to be audited. ***HIPAA*** 164.308(b)(1) "Business Associate Contracts and Other Arrangements" 164.308(b)(4) "Written Contract.". Although HIPAA does not particularly state that service levels and management of all network services be in place, it does require that a third party transmitting ePHI provide assurance of protection. Since ISO states specifically about network services, it can be considered greater than ISO.

Most mobile devices are reliant on mobile wireless network services to provide anytime, anywhere access. Services can include the provision of connections from network service providers and providing intrusion detection systems. It is important that service-level agreements be in place. Hence, ***MP*** is rated "Required".

In brief, secure management of networks spanning organizational boundaries, require careful consideration for the data flow, legal implications, monitoring and protection. Additional controls are required to protect ePHI as mobile computing entails passing data over the public network.

>>10.7 Media Handling

This section of ***ISO 17799*** intends to prevent unauthorized disclosure, modification, removal or destruction of assets and interruptions to business activities.

>>10.7.1 Management of removable media (ISO ~ HIPAA)

This ***ISO 17799*** control requires that there should be procedures in place for managing removable media procedures, such as tapes, disks, cassettes, memory cards, and reports. ***HIPAA*** 164.310(d) "Device and Media Controls" governs the handling of hardware and electronic media containing ePHI, including receipt and removal, both external to the facility and within the facility. Since they both require removable media control, they can be considered equivalent.

Devices mentioned above can be classified as portable storage devices. They can be easily stolen and may contain very sensitive information. They can also be used to carry malware. Hence, ***MP*** is "Required".

>>10.7.2 Disposal of media (ISO ~ HIPAA)

This ***ISO 17799*** control requires that media devices that are no longer required be disposed of securely and safely, using formal procedures. ***HIPAA*** 164.310(d)(2)(i) "Disposal of Media" and 164.310(d)(2)(iii) "Accountability". Since they both require safe disposal of devices, they can be considered equivalent.

Mobile devices may be disposed of at some point. It is imperative that information, such as contacts and other forms of sensitive information existing on the devices are completely erased before disposal. Existing information might be confidential. Hence, MP is rated "Required".

>>10.7.3 Information handling procedure (ISO ~ HIPAA)

This ***ISO 17799*** control requires that procedures for handling and storing of information be established to protect information from unauthorized disclosure or misuse. ***HIPAA*** 164.312(c)(2) "Mechanisms to Authenticate Electronic Protected Health Information" requires a mechanisms to confirm PHI is not altered 164.310(d)(1) "Device and Media Controls", 164.310(a) "Facility Access Controls", 164.310(a)(2)(iii) "Access Control and Validation Procedures" and 164.310(d)(2)(iii) "Accountability". Since all require that procedures for handling and storing information be in place, they can be considered equivalent.

Since most caregivers receive or transmit ePHI at the point of care, they must follow certain computing procedures to prevent unauthorized disclosure. There should be mechanisms in place to ensure the right people access the correct information. Hence, MP is rated "Required".

>>10.7.4 Security of system documentation (HIPAA #)

This ***ISO 17799*** control requires that system documentation should be protected against unauthorized access. ***HIPAA*** does not have any specification about securing documentation. Hence, HIPAA is considered "Null".

It is most often unavoidable that system documentation may contain descriptions of mobile applications, organizational data structures and authorization processes. Hence, ***MP*** is rated "Required"

In brief, appropriate operating procedures should be established to protect documents, removable media, input/output data, and system documentation from unauthorized disclosure modification removal or destruction.

>>10.8 Exchange of Information

This section of ***ISO 17799*** aims to maintain the security of information and software exchanged within an organization and with any external party.

>>10.8.1 Information exchange policies and procedures (ISO~ HIPAA)

This ***ISO 17799*** control requires that there be formal exchange policies, procedures and controls in place to protect the exchange of information through the use of all types of communication facilities. ***HIPAA*** 164.308(b)(1) "Business Associate Contracts and Other Arrangements" and 164.312(e)(1) "Transmission Security" require measures in place to guard against unauthorized access to transmitted ePHI. Since ISO specifies all types of information, including electronic, ISO can be considered greater. Since both require the protection of information, regardless of the exchange technology, they can be considered equivalent.

The mobile network is an electronic information exchange communication facility. Hence, ***MP*** is rated "Required".

>>10.8.2 Exchange agreements (ISO > HIPAA)

This section requires that agreements be established for the exchange of information and software between an organization and external parties.

HIPAA (164.308(b)(1) "Business Associate Contracts and Other Arrangements". Since HIPAA only requires agreement for the exchange of ePHI, ISO can be considered greater than HIPAA.

As long as sensitive information (ePHI) is exchanged via mobile devices, and networks are between organizations and external parties, ***MP*** is rated "Required".

>>10.8.3 Physical media in transit (ISO > HIPAA)

This ***ISO 17799*** control requires that media containing information be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries. ***HIPAA*** 164.310(d)(1) "Device and Media controls" does not specifically state the protection of medias in transit. Hence ISO is greater than HIPAA.

Media, such as CD Roms might contain vertical applications or information destined for an organization. It can also be information destined for an offsite back-up facility. In this case, ***MP*** is rated "Required".

>>10.8.4 Electronic messaging (ISO ~ HIPAA)

This ***ISO 17799*** control requires that information involved in electronic messaging be appropriately protected. This is Equivalent to ***HIPAA*** (164.312(a)(1) "Access Control" and 164.312(e)(1) "Transmission Security" Since ISO and HIPAA deal with electronic information exchange, they can be considered equivalent.

The art of mobile computing depends on electronic messaging. Hence, ***MP*** is rated "Required".

>>10.8.5 Business information systems (ISO~ HIPAA)

This ***ISO 17799*** control requires that policies and procedures be developed and enforced to protect information associated with the interconnection of business information systems. ***HIPAA*** 164.308(b)(1) "Business Associate Contracts and Other Arrangements", 164.308(b)(4) "Written Contracts" and 164.314(b)(1) "Requirements for Group Health Plans". Plan documents must reflect security safeguards. ePHI in healthcare, which is accessed by health plans and clearing houses can be considered interconnected. Hence, ISO and HIPAA can be considered equivalent.

Mobile technology enhances the interconnection of business partners, especially to collaborate. Information exchanged should be protected. Hence, ***MP*** is rated "Required".

In brief, procedures and standards should be established to protect ePHI and physical media containing information in transit.

>>10.9 Electronic Commerce Services

This section of ***ISO 17799*** aims to ensure the security of electronic commerce services and their secure use.

>>10.9.1 Electronic Commerce (ISO ~ HIPAA)

This ***ISO 17799*** control requires that Information involved in electronic commerce passing over the public network is protected from fraudulent activity, contract disputes, and any unauthorized access or modification. (***HIPAA*** 164.312(e) "Transmission Security" Since both require the protection of information in transit, they can be considered equivalent.

A mobile operator's network can be classified as a public network, and is susceptible to attacks. ePHI involves a patient's personal information, which might as well be his payment details for the services rendered. Hence, ***MP*** is rated "Required".

>>10.9.2 Online transactions (ISO ~ HIPAA)

This ***ISO 17799*** control requires that Information involved in online transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. This is equivalent to (HIPAA 164.312(a)(1) "Access control" and 164.312(e)(1) "Transmission Security".

Mobile devices are suitable for online transaction use. Customers order and pay for services, for example, health services or drug purchases. Patients can use their cell phones to send physicians their medical and insurance information. Wireless network devices are susceptible to the above mentioned threats. Hence, *MP* is rated "Required".

>>10.9.3 Publicly available information (ISO ~ HIPAA)

This ***ISO 17799*** control requires that the integrity of the publicly available information should be protected against any unauthorized modification. ***HIPAA*** 164.312(a)(1) “Access Control” and 164.312(c) “Integrity” require measures to ensure the integrity of PHI during transmission. 164.312(d) “Person or Entity Authentication” requires procedures to verify identities. (164.312(e) “Transmission security”.

Publicly available Information, accessible on mobile devices, must be protected against unauthorized modification to preserve authenticity. Hence, ***MP*** is rated “Required”.

In brief, the security implications associated with mobile commerce, online transactions, and requirement for controls should be considered, as well as the integrity and availability of publicly available information.

>>10.10 Monitoring

This section of ***ISO 17799*** aims to detect unauthorized information processing activities.

>>10.10.1 Audit Logging (ISO ~ HIPAA)

This ***ISO 17799*** control requires that audit logs, recording user activities, exceptions, and information security events, should be produced and kept for an agreed period to assist in future investigations and access control monitoring. Privacy protection measures should be considered in audit log maintenance. ***HIPAA*** 164.312(b) “Audit Controls” requires procedures and mechanisms for monitoring system activity**.**

Users or caregivers can perform activities or manipulate ePHI from their mobile devices. Therefore, the logging of activities of the users is appropriate to fully meet and optimize mobile security objectives, at same time showing due diligence. Hence, ***MP*** is rated “Required”.

>>**10.10.2 Monitoring system use (HIPAA > ISO)**

This ***ISO 17799***, control requires that procedures for monitoring use of information processing facilities be established, and the results of the monitoring activities reviewed regularly. ***HIPAA*** 164.308(a)(1)(ii)(d) “Information Security Activity Review” requires procedures to review system activity, such as audit logs, access reports, and security incident reports. 164.308(a)(5)(ii)(c) "Log-In monitoring" requires procedures and monitoring of log-in attempts. Although ISO provides lots of recommendations on what should be monitored, HIPAA does specifically require that Login monitoring training be carried out if necessary.

Regardless of any access device type, monitoring usage is necessary to ensure that users are only performing activities that have been explicitly authorized. Hence, ***MP*** is rated "Required".

>>10.10.3 Protection of log information (HIPAA #)

This ***ISO 17799*** control requires that logging facilities and log information should be well protected against tampering and unauthorized access. This is not covered in HIPAA.

Regardless of any access device system, logs need to be protected because if the data can be modified or deleted, their existence will create a false sense of security, especially if needed in a court of law. Hence, ***MP*** is rated "Required".

>>10.10.4 Administrator and operator logs (ISO > HIPAA)

This ***ISO 17799*** control requires that system administrators' and system operators' activities be logged. The logged activities should be reviewed on a regular basis. ***HIPAA*** 164.312(b) "Audit Controls" requires the technology and procedures to record and examine information system activity be based upon risk analysis. Since ISO refers more specifically to administrators' and operators' activities, while providing the nature of logs, it is considered greater than HIPAA.

As discussed in Chapter 3, users with authorized access can be the biggest threat to organization assets (ePHI). Hence ***MP*** is "Required".

>>10.10.5 Fault logging (ISO > HIPAA)

This ***ISO 17799*** control requires that faults should be logged, analyzed and appropriate action taken. ***HIPAA*** 164.308(a)(1)(ii)(d) "Information Security Activity Review" requires that items, such as audit logs, access reports, and security incident reports, be reviewed. Since ISO also requires the review of error logs for the compromise of security controls and the review of fault logs and corrective measures, it is considered the greater.

Fault logging of mobile devices can be very useful in discovering vulnerabilities and detecting failures related to data integrity. Fault logging is useful in enhancing the performance of a system. The level of logging should be determined by risk assessment. Hence, ***MP*** is rated "Required".

>>10.10.6 Clock synchronization (HIPAA #)

This ***ISO 17799*** control requires that system clocks in all information processing systems within an organization or security domain be synchronized with an agreed accurate time source. The correct setting of computer clocks is important to ensure the accuracy of audit logs. The HIPAA requirement has no such control, therefore it is considered "Null".
Audit logging is an important aspect of mobile security; it is useful for investigation purposes. Hence, ***MP*** is rated "Required".

In brief, mobile systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure that the information system problems are identified.

6.3.8 Section 11: Access control

This section of ***ISO 17799*** intends to manage and control access to information.

>>11.1 Business requirements for access control

Section 11 of ISO aims to control access to information, its processing facilities and business processes on the basis of business and security requirements.

>>11.1.1 Access Control Policy (HIPAA ~ ISO)

This ***ISO 17799*** control requires that an access control policy be established, documented and reviewed based on the business and security requirements for access. ***HIPAA*** 164.308(a)(3)(i) "Workforce Security". 164.312(a)(1) "Access control" requires technical or administrative policies and procedures to manage PHI access. 164.308(a)(4)(ii)(b) "Access Authorization" requires that policies and procedures be in place to authorize a worker's access to ePHI through a specific mechanism, such as a workstation or program. Since they both refer to physical and logical access, they can be considered equivalent.

Mobile security very much depends on the access control rules and rights for each user or group policies. These will cater for the logical access that will be implemented for the ePHI accessible by mobile devices. The underlying access technology does not affect the access control as specified by the policy. Hence, ***MP*** is rated "Required".

>>11.2 User Access Management

Section 11.2 of ***ISO 17799*** controls aims to ensure authorized user access and to prevent unauthorized access to information systems.

>>11.2.1 User registration (ISO ~ HIPAA)

This ***ISO 17799*** control requires that there be formal user registration and de-registration procedures for granting access to all information systems and services. ***HIPAA*** 164.308(a)(4)(i) "Access Establishment and Modification" requires policies and procedures to grant access to ePHI and regular access review. 164.308(a)(3)(ii)(c) "Workforce Clearance Procedures" requires procedures to ensure appropriate PHI access. 164.308(a)(3) "Access Authorization" requires policies and procedures to authorize access to PHI. 164.308(a)(3) "Termination Procedures" 164.312(a)(2)(i) "Unique User Identification" requires the assignment of unique IDs to support tracking. Since both require procedures in place for granting and revoking access of users, they can be considered equivalent.

Before access is granted to mobile users, such a process must exist to determine who is eligible for what kind of mobility access. This process will determine who is authorized to access what information using their unique IDs for accountability issues. Hence, ***MP*** is rated "Required".

>>11.2.2 Privilege management (HIPAA ~ ISO)

This ***ISO 17799*** control requires that the allocation and use of any privileges in information system environments should be restricted and controlled. ***HIPAA*** 164.308(a)(3) "Access Authorization" and 164(308)(a)(4) "Access Establishment and Modification" Since they both require appropriate steps to get authorization, they can be considered equivalent.

Privileges should be allocated on need-to-use basis; privileges should be allocated only after formal authorization process granting a mobile user access to the privileged information (ePHI). Hence, ***MP*** is rated “Required”.

>>11.2.3 User password management (ISO ~ HIPAA)

This ***ISO 17799*** control requires that the allocation and reallocation of passwords should be controlled through a formal management process. ***HIPAA*** 164.308(a)(5)(ii)(d) “Password Management” requires procedures for password management**.** Since both require a procedure in place for password management, they can be considered equivalent”.

Password or pins, among other access technologies, such as biometrics, are used to access most mobile devices. Organizational resources accessible by mobile devices should be protected with passwords, and users should be asked to sign a statement to keep the password confidential. Hence, ***MP*** is rated “Required”.

>>11.2.4 Review of user access rights (ISO ~ HIPAA)

This ***ISO 17799*** control requires that management should review user access rights at regular intervals using a formal process. ***HIPAA*** 164.308(a)(4)(ii)(c) “Access Establishment and Modification” requires an organization to establish, document and review or modify user access rights. Since both require the review of access rights, they can be considered equivalent.

Regular reviews of access rights are useful in maintaining effective control over access to data and information services. This also includes the access rights associated with mobility. Hence, ***MP*** is rated “Required”.

In brief, access control is an important aspect of secure mobile computing. Procedures should be in place to control the allocation of access rights to mobile information systems. The procedure should cover from the initial registration of a user to the final deregistration of a user.

>>11.3 User responsibilities

This section of ***ISO 17799*** aims to prevent unauthorized user access, and compromise or theft of information and information facilities.

>>11.3.1 Password use *(*ISO ~ HIPAA)

This ***ISO 17799*** control requires that users should be required to follow good security practices in the selection and use of passwords. ***HIPAA*** 164.308(a)(5)(ii)(d) "Password Management". Since both require password management best practice to be followed, they can be considered equivalent.

Mobile devices and networks use pins and passwords, required as users are dealing with sensitive information (ePHI). Hence, ***MP*** is rated "Required".

>>11.3.2 Unattended user equipment (ISO ~ HIPAA)

This ***ISO 17799*** control requires that users should ensure that unattended equipment has appropriate protection. ***HIPAA*** 164.310(b) "Workstation Use" requires policies and procedures on the proper use of workstations and on their proper physical attributes for the siting of workstations. (164.310(c) "Workstation Security", 164.312(a)(2)(iii) "Automatic logoff" Session Termination Mechanisms.

Session termination should be invoked when a user finishes an activity, and should logoff, requiring re-access during the next session to prevent easy intrusion. Mobile on-device security should be kept on unless the user wants to use the mobile. Mobiles should not be kept lying around as they become easy prey for theft. Hence, ***MP*** is rated "Required".

>>11.3.3 Clear desk and clear screen policy (ISO ~ HIPAA)

This section of ***ISO 17799*** control requires organizations to adopt a clear desk policy with regards to papers and removable storage media. They should adopt a clear screen policy with regards to information processing facilities. ***HIPAA*** 164.310(b) "Workstation Uses" and 164.310(c) "Workstation Security", 164.312(a) (2) (iii) "Automatic Logoff." Since both require mobile devices' protection as well as some procedures for safe computing, they can be considered equivalent.

Device users should consider the clear screen policy to protect from shoulder-spoofing attacks, especially in public areas, like hot spots. Storage devices should be well hidden or kept to prevent theft. Hence, ***MP*** is rated "Required".

>>11.4 Network Access Control

The objective of this section is to prevent unauthorized access to networked services, either internally or externally.

>>11.4.1 Policy on the use of network services *(*ISO > HIPAA)

This ***ISO 17799*** control requires that users be provided with access only to the services that they have been specifically authorized to use. (***HIPAA*** 164.312(a)(1) "Access Control" 164.312(d)(2) "Transmission Security" and 164.308(a)(4)(ii)(b) "Access Authorization". Since HIPAA does not specifically identify the use of network services and focuses more on the information requiring security during transmission only, ISO can be considered the greater.

Different categories of users will require access to information or mobile applications that are to be only attributed to them. Some users will work from home and others will choose to have access to resources via the mobile operator wireless network. Hence, ***MP*** is rated "Required".

>>11.4.2 User authentication for external connections (ISO ~ HIPAA)

This ***ISO 17799*** control requires that appropriate authentication mechanisms be used to control access by remote users. ***HIPAA*** 164.312(d) "Person or Entity Authentication" requires procedures to verify identities**.** Since both require user authentication procedures to be in place, they can be considered equivalent.

Most mobile users or third parties access organizational information or resources remotely. All wireless access points should be treated as external networks to boost security. Hence, ***MP*** is rated "Required".

>>11.4.3 Equipment identification in networks (ISO ~ HIPAA)

This ***ISO 17799*** control requires that automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. ***HIPAA*** 164.312(d) "Person or Entity Authentication". Since equipment can be identified as an entity, ISO and HIPAA can be considered equivalent.

Providing device-level authentication can keep track of what devices are accessing network resources and will provide useful information for logging activities, as well identifying specific users. Hence, ***MP*** is rated "Required".

>>11.4.4 Remote diagnostic and configuration port protection (ISO > HIPAA)

This ***ISO 17799*** control require that physical and logical accesses to diagnostic ports be securely controlled, i.e., protected by security mechanisms. ***HIPAA*** 164.312(a)(1) "Access Control", 164.312(a)(2)(i) "Unique User Authentication" and 164.312(d) "Person or Entity Authentication". Although HIPAA does not specifically mention diagnostics and configuration port protection, it does require authentication to access workstations as well as access control. ISO can be considered the greater.

If diagnostic ports are open, mobile devices can be used to remotely gain unauthorized access to a network or devices to aid in an attack, such as denial of service. It is imperative that a secure connection is used for diagnostics and configuration. Hence, ***MP*** is rated "Required".

>>11.4.5 Segregation in networks (ISO > HIPAA)

This ***ISO 17799*** control requires that groups of information services, users and information systems should be segregated on networks. ***HIPAA*** 164.314(b)(2)(ii) "Ensure Adequate Separation" requires health plan security measures to separate PHI from plan sponsors and group health plans. Since they require the separation of information or services, they can be considered equivalent.

Not all information on a healthcare network is PHI. A large portion of the network accessed by healthcare workers may not be HIPAA-sensitive. Healthcare organizations should take appropriate steps to segregate PHI and non-PHI on the network to improve access control. Authorized access will be granted to users belonging to a particular group service that will use mobile devices. Hence, MP is rated "Addressable".

>>11.4.6 Network connection control (HIPAA #)

This ***ISO 17799*** control requires that there should be an access control policy which states network connection control for shared networks, especially for those extending across organizations' boundaries. The capability of users to connect to the network should be restricted. ***HIPAA*** does not have any specification control dealing with network connection control; as such, HIPAA can be considered "Null".

The capability of users' connections to an organizations network via a mobile network should be restricted and monitored. If given full access to resources, they might be targeted by a malicious user, who can gain an edge over the non-suspecting user. Hence, ***MP*** is rated "Required".

>>11.4.7 Network routing control (HIPAA #)

This section ***ISO 17799*** control requires that outing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business application. **HIPAA** does not mention network routing controls, and as such, it is considered "Null".

In an ad hoc network, any node can compromise the routing protocol functionality by disrupting the route discovery process. Also in a mobile IP network, a lot of routing is required between networks; therefore, secure routing is imperative. Hence, ***MP*** is rated "Required".

In brief, to prevent unauthorized access to wireless network services, logical and physical access to both internal and physical networked services should be controlled. The authentication mechanism discussed in chapter 4 plays and important role.

>>11.5 Operating System Access Control

This section of ***ISO 17799*** intends to prevent unauthorized access control.

>>11.5.1 Secure log-on procedures (HIPAA #)

This ***ISO 17799*** control requires access to operating system to be controlled by secure log-on procedure. HIPAA does not specify secure log-on procedures.

As discussed in chapter two, section 2.4, mobile devices now come with operating systems capable of running an organization-sensitive vertical application. Hence, ***MP*** is rated "Required".

>>11.5.2 User identification and authentication (ISO ~ HIPAA)

This ***ISO 17799*** control requires that a unique identifier (user ID) should be provided to every user. And a suitable authentication technique should be chosen to validate the claimed identity of a user. ***HIPAA*** 164.312(a)(2)(i) "Unique User Identification" requires that verification is performed that a person or entity is the one claimed. Since both require unique user identification and authentication, they can be considered equivalent.

Memory tokens or smart cards that users possess can be used for identification and authentication. Mobile devices also provide support for biometrics. Access by users via mobile devices should be interrogated for identification and authentication before accessing sensitive information. Hence, ***MP*** is rated "Required".

>>11.5.3 Password management systems (ISO > HIPAA)

This section of ***ISO 17799*** control requires that systems for managing passwords should be interactive and should ensure quality passwords. ***HIPAA*** 164.308(a)(5)(ii)(d) "Password Management" requires procedures for password management. Although HIPAA acknowledges the importance of password management, it does not provide steps that should be taken to safeguard the passwords. ISO is, therefore, greater than HIPAA.

Password management for mobility is the same as any other system. It must enforce the use of user IDs and password to ensure authentication when accessing an information system. It must enforce password changes and other rules associated with password management to achieve secure mobility. The process is to prevent attacks such as password guessing or brute force. Hence, ***MP*** is rated "Required".

>>11.5.4 Use of system utilities (HIPAA #)

This ***ISO 17799*** control requires that the use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. ***HIPAA*** does not mention the use of utility programs. For organizations' mobile devices, restrictions should be placed on the types of programs that should be installed on the devices. As mentioned, the devices capture important data. Central management of devices should be considered, e.g., for installation, upgrades or configurations to prevent unauthorized utility programs. Hence, ***MP*** is rated "Required".

>>11.5.5 Session time-out (ISO ~ HIPAA)

This ***ISO 17799*** control requires that inactive sessions should be shutdown after a defined period of inactivity. ***HIPAA*** 164.312(a)(2)(iii) "Automatic Logoff" requires time-outs for sessions after a period of inactivity. Since both require time-outs of session, they can be considered equivalent.

Users use mobile devices perhaps to open up sessions with an organization information system. If an attacker takes over or hijacks a session, he can carry out any operation the session privileges permit as discussed in section 3.2.2.1. It is imperative that a session shuts down after a period of inactivity because an open session opens up a window of opportunity for unauthorized access. Hence, ***MP*** is rated "Required".

>>11.5.6 Limitation of connection time (ISO > HIPAA)

This ***ISO 17799*** control requires that restrictions on connection times should be used to provide additional security for high-risk applications. ***HIPAA*** 164.312(a)(2)(iii) "Automatic Logoff" Although HIPAA requires timeouts of inactive sessions, ISO requires more action on restricting connection period of users, or using predetermined time slots for activities.

Limiting the period during which connections to mobile computing services are allowed reduces the window of opportunity for unauthorized access. The process does oppose the concept of mobility of anytime, anywhere access. Hence, ***MP*** is rated "Addressable".

In brief, to restrict access to critical application on devices and backend servers to unauthorized user, authentication, session/user monitoring and control should be in place.

>>11.6 Application and Information Access Control

This section ***ISO 17799*** aims to prevent unauthorized access to information held in application systems.

>>11.6.1 Information access restrictions (ISO ~ HIPAA)

This ***ISO 17799*** control requires that access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. ***HIPAA*** 164.312(a)(1)

"Access Control", 164.308(a)(4)(ii)(b) "Access authorization" and 164.308(a)(4)(ii)(c) "Access Establishment and Modification". Since they all require information access restrictions, they can be considered equivalent.
Access restrictions to information and application functions accessible on mobile devices are important in achieving mobile security. Hence, ***MP*** is rated "Required".

>>11.6.2 Sensitive system isolation (HIPAA > ISO)

This ***ISO 17799*** control requires that sensitive systems should have dedicated (isolated) computing environments. ***HIPAA*** 164.308(a)(4)(ii)(A) "Isolating Health Clearinghouse Functions" requires policies and procedures to separate PHI from other operations. While ISO requires the isolation of sensitive application system, HIPAA isolates healthcare clearinghouse operations at a policy level and requires procedures in place. As such, HIPAA is greater than ISO.

Since HIPAA states that the control is required, any mobile activity within the premises must be trusted to that area or application. The wireless signal at this point must taken into consideration. Hence, ***MP*** is rated "Required".

In brief, logical access to information and application systems (local or remote) should be restricted to authorized mobile workers.

>>11.7 Mobile Computing and Teleworking

This section ***ISO 17799*** aims to ensure information security when using mobile computing and teleworking facilities.

11.7.1 Mobile computing and communication (ISO > HIPAA)

This ***ISO 17799*** control requires that a formal policy be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. ***HIPAA*** 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" and 164.312(e)(1) "Transmission Security" require the need to protect ePHI on devices and in transit over communication networks.

Although HIPAA does provide the necessary controls that will be required in a mobile computing environment, it does not provide additional guidelines specific to the mobile environment. Therefore, ISO can be considered greater than HIPAA. Hence, ***MP*** can be rated "Required".

>>11.7.2 Teleworking (ISO ~ HIPAA)

This ***ISO 17799*** control requires that a policy, operational plan and procedures should be developed and implemented for teleworking activities. ***HIPAA*** 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" and 164.312(e)(1) "Transmission Security". Although teleworking is another form of mobility, it is more static. Since ISO and HIPAA both require procedures for secure remote access they can be considered equivalent. Hence, ***MP*** is rated "Required".

In brief, to ensure information security when using mobile computing and teleworking facilities, protection required should align with the risk these specific working ways cause. In addition, teleworking sites should be well protected.

6.3.9 Section 12: Information Systems Acquisition, Development and Maintenance

This section of ***ISO 17799*** aims to ensure security, in information system acquisition, development and maintenance.

>>**12.1 Security Requirements of Information Systems**

This ***ISO 17799 control*** aims to ensure that security is an integral part of information systems.

>>12.1.1 Security requirements analysis and specification (*HIPAA #*)

Statement of business requirements for new information systems, or enhancements to existing information systems, should specify the requirements for security controls. ***HIPAA*** does not have such a requirement.

Most organizations' mobile computing constitutes part of the enhancement programme of a current information system. Hence, ***MP*** is rated

"Required".

In brief, all security requirements should be identified prior to extending the information an information system to include mobile technology as part of the overall business case.

>>12.2 Correct Processing in Applications

This section of ***ISO 17799*** aims to prevent errors, loss, unauthorized modification or misuse of information in applications.

>>12.2.1 Input data validation (ISO > HIPAA)

This ***ISO 17799*** control requires that data input to application systems is validated to ensure that it is correct and appropriate. ***HIPAA*** 164.312(c)(2) "Mechanism to Authenticate Electronic Protected Health Information" simply requires a mechanism be in place to authenticate ePHI, while ISO details specifically where the data be validated at the point of input at the application. Therefore, ISO can be considered greater than HIPAA.

As vertical mobile applications accept data and store this information before synchronization to a database, perhaps the data entered should be validated. At the point of care in healthcare, if a patient's drug information is entered wrongly, it will lead to mistreatment. Also, it is important to verify that application inputs traveling across a network are safe to process. Hence, ***MP*** is rated "Required".

>>12.2.2 Control of internal processing (ISO ~ HIPAA)

This ***ISO 17799*** control requires that validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. ***HIPAA*** 164.312(c)(2) "Mechanism to Authenticate Electronic Protected Health Information". Since both require that a mechanism is present to check for validation. ISO and HIPAA can be considered equivalent.

As mentioned for critical vertical applications, like in healthcare, it is important to have such validation checks as applications run on mobile devices. Hence, ***MP*** is rated "Required".

>>12.2.3 Message integrity (ISO ~ HIPAA)

This section states that requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented. ***HIPAA*** 164.312(c)(1) "Integrity". This requirement is to assure that ePHI is not altered or destroyed in an unauthorized manner. 164.312(d)(2) "Integrity Controls" requires measures to ensure integrity of PHI on transmission "Encryption". Since the two require a system in place to protect the integrity of a message, ISO and HIPAA can be considered equivalent.

Since healthcare organizations often deal with sensitive information, the integrity of the information accessed and processed on the mobile devices need to be kept. Hence, ***MP*** is rated "Required".

>>12.2.4 Output data validation (ISO ~ HIPAA)

This ***ISO 17799*** control requires that data output of application systems should be validated to ensure that the processing of stored information is correct and appropriate to circumstances. ***HIPAA*** 164.312(c)(2) "Mechanisms to Authenticate Electronic Protected Health Information". Since at this point the processed data is information and requires to be checked for authenticity, ISO and HIPAA can be considered equivalent.

As mobile computing deals with very sensitive data, in this case, authenticity of information is required**.** Hence, ***MP*** is rated "Required".

In brief, appropriate controls should be designed into mobile applications, including user developed applications to ensure correct processing.

>>12.3_Cryptographic controls

This section of *ISO 17799* aims to protect the confidentiality, authenticity or integrity of information by cryptographic means.

>>12.3.1 Policy on use of cryptographic controls (ISO > HIPAA)

This ***ISO 17799*** control requires that a policy on the use of cryptographic controls for the protection of information should be developed and implemented. ***HIPAA*** 164.308(a)(1)(i) "Security management process" requires the implementation of policies and procedures to prevent, detect, contain and correct security violations.

164.312(a)(2)(iv) "Encryption and Decryption" Encryption is a mechanism for encryption of stored PHI. Since HIPAA does not specifically require policy on the use of cryptographic controls, ISO can be considered greater than HIPAA.

Weaknesses associated with a wireless network require cryptographic solutions to protect the confidentiality integrity and non-repudiation of information. Hence, ***MP*** is rated "Required".

>>12.3.2 Key management (HIPAA #)

This ***ISO 17799*** control requires that key management should be in place to support the organization's use of cryptographic techniques. Although some HIPAA controls require the use of keys, it does not mention anything about key management; as such it is considered, "Null".

Cryptographic keys should be protected against modification, loss, and destruction. Secret keys and private keys should be protected against unauthorized disclosure. Hence, ***MP*** is rated "Required".

In brief, as shown in chapter 4, to protect the confidentiality, authenticity or integrity of information associated with mobile computing, cryptographic means are required. In addition, key management is also required.

>>12.4 Security of system files

This section of ***ISO 17799*** aims to ensure the security of system files.

12.4.1 Control of operational software (HIPAA #)

This ***ISO 17799*** control requires that there should be procedures in place to control the installation of software on operational systems. ***HIPAA*** does not specifically require procedures in place to control installations of software. Hence HIPAA can be considered "Null".

Central software Update management service should be available for application on corporate devices. This is to ensure same level of security among devices. Patch management or configuration of mobile devices can be an example. Hence, ***MP*** is rated "Required".

>>12.4.2 Protection of system test data (HIPAA #)

This ***ISO 17799*** control requires that Test data should be selected carefully and protected and controlled. ***HIPAA*** does not mention anything about test data. Therefore HIPAA is considered “Null”.

Where personal information is involved for test purposes on a mobile network, it should be modified beyond recognition. Hence, ***MP*** is rated “Required”.

>>12.4.3 Access Control to program source code (HIPAA #)

This ***ISO 17799*** control requires that access to program source code be restricted. ***HIPAA*** does not mention program source code restriction in it requirement, as such it is considered “Null”.

Access to mobile application source code should be protected to prevent the introduction of unauthorized functionality and to avoid unintentional changes by malicious users. Hence, ***MP*** is rated “Required”.

In brief, access to mobile programs source code should be controlled. Care should be taken to avoid exposure of sensitive data in test environments.

>>12.5 Security in development and support processes

This section of ***ISO 17799*** aims to maintain the security of application system software and information.

>>12.5.1 Change control procedures (HIPAA #)

This ***ISO 17799*** control requires that the implementation of changes should be controlled by the use of formal change control procedures. ***HIPAA*** does not mention having a change control procedure in place. As a result, HIPAA is considered “Null”.

The implementation of changes must be authorized and a risk assessment and analysis of impacts of change should be conducted. Users may tend to install wireless devices at their desks to make their jobs easier. Hence, MP is rated “Required”.

>>12.5.2 Technical review of applications after operating system changes (HIPAA #)

This ***ISO 17799*** control requires that there should be a process or procedure in place to review and test business critical applications for adverse impact on organizational operations or security, after a change to an operating system. ***HIPAA*** does not mention such controls in its requirement.

Back-end system supporting mobile network applications may require a change in operating systems. More so, new devices, running different operating systems, may be introduced. Compatibility issues should be checked as well as if new threats and vulnerabilities are introduced. Hence ***MP*** is "Required".

>>**12.5.3 Restrictions on changes to software packages (HIPAA #)**

This ***ISO 17799*** control requires that modifications to software packages be discouraged or limited to necessary changes, and all changes should be strictly controlled. ***HIPAA*** has no such control; as such, it is considered "Null".

As it is possible to install a third-party application on a mobile device, there can be chances of modification. As far as is possible and practicable, vendor-supplied software packages should be used without modification to prevent risks. Central management of mobile devices should be employed. Hence, MP is rated "Required".

>>12.5.4 Information leakage (ISO ~ HIPAA)

This ***ISO 17799*** control requires that opportunities for information leakage should be prevented. ***HIPAA*** 164.312(a)(1) "Access Control"l 164.308(a)(1)(i) "Security Management Process" and 164.312(e)(1) Transmission Security and 164.308(a)(1)(ii)(d) "Information System Activity Review". Since both standards aim to prevent information leakage by having processes in place, they can be considered equivalent.

Regardless of the types of device, type of network, information, whether processed, stored and transmitted, must be protected. Monitoring activities performed and resource usage by users, as approved by legislation, as well as masking and modulation can be very useful. Hence, MP is rated "Required".

>>12.5.5 Outsourced software development (HIPAA #)

This ***ISO 17799*** control requires that outsourced software development should be supervised and monitored by an organization. ***HIPAA*** has no such specification.

There should be contractual requirements for quality and security functionality. Mobile applications should be tested before installation of mobile applications on the devices in order to detect malicious and Trojan code. Hence, MP is rated "Required".

In brief, in order to maintain the security of mobile application systems software and information, project and support environment should be strictly controlled.

>>12.6 Technical Vulnerability Management

This section of ***ISO 17799*** aims to reduce risks resulting from exploitation of published technical vulnerabilities.

>>12.6.1 Control of technical vulnerabilities (HIPAA ~ ISO)

This ***ISO 17799*** control requires that timely information about technical vulnerabilities of information systems being used is obtained, the impact of such vulnerabilities evaluated, and appropriate measures taken to mitigate the associated risk. ***HIPAA*** 164.308(a)(1)(ii)(b) "Risk Management" The essence of the risk management process is to achieve the objectives, as mentioned, and it should be periodic. The requirements can be considered equivalent.

A technical-vulnerability management process is critical for mobile security, therefore, should be regularly monitored and corrected. Hence, MP is rated "Required".

6.3.10 Section 13. Information Security Incident Management

This section of *ISO 17799* aims to provide guidance on security incident management.

>>13.1 Reporting Information Security Events and Weaknesses

This ***ISO 17799*** control aims to ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective actions to be taken.

>>13.1.1 Reporting information security events (HIPAA ~ ISO)

This ***ISO 17799*** control requires that information security events be reported through appropriate management channels as quickly as possible. ***HIPAA*** 164.308(a)(6) "Response and Reporting" requires mitigation and documentation of security incidents. The standards both request that report and action be taken; as such they can be considered equivalent.

A formal procedure, called an incident response procedure, should be developed and implemented. This is applicable to mobile devices. This process will help identify flaws for quick isolation until solved. Hence, MP is rated "Required".

>>13.1.2 Reporting security weaknesses (ISO ~ HIPAA)

This ***ISO 17799*** control requires that all employees of information systems and services should be required to note and report any observed or suspected security weakness in the system or services. ***HIPAA*** 164.308(a)(1)(ii)(d) "Information System Activity Review" and 164.308(a)(6) "Response and Reporting". Since both standards expect such reports from employees, they can be considered equivalent.

This process is vital to prevent information security incidents associated with mobile devices by taking actions on reported weaknesses. Users that access ePHI and services on mobile devices should be required to note and report any observed or suspected security weakness in the systems or services. Hence, MP is rated "Required".

In brief, to ensure security events and weaknesses associated with mobile computing are communicated allowing timely corrective action to be taken, event reporting and procedures should be in place. All users should be made aware of reporting procedures.

>>13.2 Management of Information Security Incidents and Improvements

This section ***ISO 17799*** aims to ensure consistent and effective approach is applied to the management of information security incidents.

>>13.2.1 Responsibilities and procedures (ISO ~ HIPAA)

This ***ISO 17799*** control requires that management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. ***HIPAA*** 164.308(a)(6)(i) "Security Incident Procedures" requires policies and procedures to manage security incidents. 164.308(a)(6)(ii) "Response and Reporting". Since both standards require responsibilities and procedures in place, they can be considered equivalent.

Procedures should be in place to quickly respond to security incidents associated with mobile devices in order to seal the opening from further attack. Hence, ***MP*** is rated "Required".

>>13.2.2 Learning from information security incidents (ISO ~ HIPAA)

This ***ISO 17799*** control requires that there should be a mechanism in place to identify and quantify the type, volume and costs of information security incidents. ***HIPAA*** 164.308(a)(6)(ii) "Response and Reporting" and 164.308(a)(1)(ii)(b) "Risk Management", can be considered equivalent.

The information gained from the evaluation of the past information security incidents can be used to identify recurring or high impact incidents to aid in identifying appropriate controls in a mobile computing environment. Hence, ***MP*** is rated "Required".

>>13.2.3 Collection of evidence (HIPAA > ISO)

This ***ISO 17799*** control requires that a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal). Evidence should be collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdictions. ***HIPAA*** 164.316(b)(2)(i) "Time limit" "Policies and Procedures" requires the retention of documentation for 6 years in the event where evidence is needed.

Although both controls require evidence to be collected, HIPAA specifically specifies how long and it is not negotiable, except exceeded by another law. Hence HIPAA is rated greater.

Regardless of technology, in the event of a security breach, there are legal repercussions. Evidence might be required in court to show due diligence. Hence, ***MP*** is "Required".

In brief, a process of continual improvement of monitoring, evaluating, response and overall management of information security incident should be in place.

6.3.11 Section 14: Business Continuity Management

This section of ***ISO 17799*** aims to provide guidance on business continuity management.

>>14.1 Information Security Aspects of Business Continuity Management

This section ***ISO 17799*** controls aims to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of Information systems or disasters and to ensure their timely resumption.

>>14.1.1 Including information security in the business continuity management process (HIPAA > ISO)

This ***ISO 17799*** control requires that there should be a managed process in place that addresses the information security requirements for developing and maintaining business continuity throughout the organization. ***HIPAA*** 164.308(a)(7)(i) "Contingency Plan" requires emergency response policies and procedures. 164.310(a)(2)(i) "Contingency Operations" requires procedures to support emergency operations and recovery. 164.312(a)(2)(ii) "Emergency Access Procedure" requires procedures to support emergency access. 164.308(a)(7)(ii)(C) "Emergency Mode Operation Plan" requires business continuity procedures. Although similar in many aspects, HIPAA does specifically require that access control for contingency operations be addressed. Hence HIPAA can be considered greater than.

As wireless networks are susceptible to interference, both human and natural, a process should be in place to ensure continuity especially where lives are involved. Hence, ***MP*** is rated "Required".

>>14.1.2 Business continuity and risk assessment (ISO ~ HIPAA)

This ***ISO 17799*** control requires that events that cause interruption to business process should be identified along with the probability and impact of such interruptions and their consequence for information security. ***HIPAA*** 164.308(a)(7)(ii)(e) "Applications and Data Criticality Analysis" and 164.308(a)(1)(ii)(a) "Risk Analysis". Since both require a continuous risk management process, they can be considered equivalent.

As mentioned in chapters 3 and 4, threats continue appearing rampantly, and attacks can be expected to become ever more sophisticated as technology improves. Risk analyses and assessment processes are required. Hence, ***MP*** is rated "Required".

>>14.1.3 Developing and implementing continuity plans, including information security (ISO ~ HIPAA)

This ***ISO 17799*** control requires that plans should be developed to maintain and restore business operations and ensure availability of information within the required level in the required time frame, following an interruption or failure to business processes. ***HIPAA*** 164.308(a)(7)(ii)(a) "Data Backup Plan" and 164.308(a)(7)(ii)(b) "Disaster Recovery Plan" require data recovery planning and procedures. (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" and 164.312(a)(2)(ii) "Emergency Access Procedures" As HIPAA does have a combination of controls to restore business operation and ensure availability, they can be considered equivalent.

One of the main objectives of mobile computing is to enhance availability of information and that is critical in healthcare. Hence, ***MP*** is rated "Required".

>>14.1.4 Business continuity planning framework (ISO > HIPAA)

This ***ISO 17799*** control requires that a single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements and to identify priorities for testing and maintenance. ***HIPAA*** 164.310(a)(1)(ii)(d) "Testing and Revision Procedures" requires contingency planning and periodic testing procedures to ensure it works. HIPAA does not specifically require a single business continuity planning framework; as such ISO is considered greater than HIPAA.

To ensure mobile security plans are consistent with the information security requirement plan is very useful in meeting overall business objective. Hence, ***MP*** is rated "Required".

>>14.1.5 Testing, maintaining and re-assessing business continuity plans (ISO ~ HIPAA)

This ***ISO 17799*** control requires that business continuity plans should be tested regularly to ensure that they are up to date and effective. ***HIPAA*** 164.308(a)(7) "Testing and Revision Procedures" requires Contingency planning and periodic testing procedures to be in place. Since both require testing, maintaining and re-assessing business continuity plans, they can be considered equivalent.

While this is true for any system in place, such plans for mobile computing must be tested periodically. Hence, ***MP*** is rated "Required".

In brief, business continuity plans should be developed and implemented to ensure timely resumption of essential operations. The management should include controls to identify risks, limit the consequences of damaging incidents, and ensure information availability at the point of care.

6.3.12 Section 15: Compliance

This section of *ISO 17799* aims to ensure compliance with legal requirements.

>>15.1 Compliance with legal requirements

This ***ISO 17799*** controls aims to avoid breaches of any law, statutory, regulatory or contractual obligation, and of any security requirement.

>>15.1.1 Identification of applicable legislation (HIPAA #)

This ***ISO 17799*** control requires that all relevant statutory, regulatory, contractual requirements and organizational approaches to meet the requirements should be explicitly defined and documented for each information system and organization.

While designing the mobile security policy, it is important that it captures the requirements by legislation or regulatory bodies as well just as mentioned in the previous chapter and illustrated in this chapter. Hence, ***MP*** is "Required".

>>15.1.2 Intellectual property rights (IPR) (HIPAA #)

This ***ISO 17799*** control requires that appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material, in respect of which, there may be intellectual property rights and on the use of proprietary software products.

For instance, some management softwares may require limited number of mobile devices to be managed. Copyright infringement can lead to legal actions, which may involve criminal proceedings. Hence, ***MP*** can be rated "Required".

>>15.1.3 Protection of organizational records (HIPAA > ISO)

This ***ISO 17799*** control requires that important records should be retained and protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual and business obligations. ***HIPAA*** 164.316(b)(1) "Policies and Procedures Documentations". This requires documenting policies and procedure, actions and activities. Although can be considered similar, as ISO allows the adoption of a national law retention time limit, ISO places itself inferior. HIPAA does specify it's documentation retention period to be six years. Hence HIPAA is considered greater.

Important records associated with mobile computing should be documented and protected. Hence, MP is rated "Required".

>>15.1.4 Data protection and privacy of personal information (ISO ~ HIPAA)

This ***ISO 17799*** control requires that data protection and privacy should be ensured as per relevant legislation, regulations and, if applicable, contractual clauses. ***HIPAA*** 164.306(a) "Security Standards: General Requirements". 164.308(a)(2) "Assigned Security Responsibility". Since this section requires data protection and privacy of personal information, they can be considered equivalent.

In the healthcare environment, covered entities must protect the privacy and security of health information. Covered entities are meant to follow the data protection laws, regardless of the technology in place. Hence, ***MP*** is rated “Required”.

>>15.1.5 Prevention of misuse of information processing facilities (ISO ~ HIPAA)

This ***ISO 17799*** control requires that users should be deterred from using information processing facilities for unauthorized purposes. ***HIPAA*** 164.310(a)(1) “Facility Access Control” describes the required controls on facilities containing ePHI or systems with access to ePHI. 164.310(b) “Workstation Use” requires policies and procedures on the proper use of workstations and proper physical attributes for siting of workstations. 164.308(a)(3)”Workforce Security” covers personnel management requirements relevant to the protection of ePHI. Since both deal with processing facilities and the users, they can be considered equivalent.

Using organizations’ mobile devices for personal purposes should be deterred, for instance, installing games, as it creates avenues for more risk to an organizational information system. Users should follow proper computing procedures in public areas. Hence, ***MP*** is rated “Required”.

>>15.1.6 Regulation of cryptographic controls (HIPAA #)

This ***ISO 17799*** control requires that cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. HIPAA does not specifically state such a requirement.

Because of the level of processing requirement of cryptographic controls, and the need to provide availability of information in time when dealing with ePHI in healthcare, ***MP*** can be rated “Required”.

In brief, Mobile computing in healthcare is very well subject to legislative requirement and must be considered when employing a solution.

>>15.2_Compliance with security policies and standards, and technical compliance

This section of ***ISO 17799*** aims to ensure compliance of systems with organizational security policies and standards.

>>15.2.1 Compliance with security policies and standards (ISO ~ HIPAA)

This ***ISO 17799*** control requires that managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. ***HIPAA*** 164.308(a)(8) "Evaluation" requires periodic evaluation. Since a periodic evaluation is required to measure compliance to policies and standards, they can be considered equivalent.

As a required process of security and the fact that all security controls should align with policies and standards, ***MP*** is rated "Required".

>>15.2.2 Technical compliance checking (ISO ~ HIPAA)

This ***ISO 17799*** control requires that information systems be regularly checked for compliance with security implementation standards. ***HIPAA*** 164.308(a)(8) "Evaluation" requires periodic assessment of technical and non-technical measures in place to achieve compliance. Since both require constant evaluation of technical controls in line with compliance, they can be considered equivalent.

Mobile computing security involves a lot of technical controls and they continuously evolve, as mentioned in chapter 4. Hence, ***MP*** is rated "Required".

In brief, Mobile computing security should be regularly reviewed, against appropriate security policies and technical platforms. In addition, it should be audited for compliance with applicable implementation standards and documented controls.

>>15.3 Information systems audit controls

This section ***ISO 17799*** controls aims to maximize the effectiveness of and to minimize the interference to/from the information system audit process.

>>15.3.1 Information systems' audit controls (HIPAA #)

This ***ISO 17799*** control requires that audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business process. ***HIPAA*** does not state that a plan should be in place.

Access to the mobile network in the healthcare situation should not be interrupted since it deals mostly with emergency cases. Hence, ***MP*** is rated "Required".

>>15.3.2 Protection of information system audit tools (HIPAA #)
This ***ISO 17799*** control requires that access to information system audit tools, such as software or data files, should be protected to prevent any possible misuse or compromise. ***HIPAA*** does not mention such a requirement.

It is important that a true state of a network is realized. In the event of vulnerabilities, the right controls can be implemented. Hence, ***MP*** is rated "Required".

In brief, since mobile computing is subject to audit, there should be controls to protect operational system and audit tools during information system audits. In addition to protect the integrity of audit tools as well as their misuse.

6.4 Analysis of Comparison

Table 6-3 Comparison result

ISO ~ HIPAA	67	(50 %)
ISO> HIPAA	28	(20.9%)
HIPAA > ISO	10	(7.5%)
HIPAA #	29	(21.6%)
Total	**134**	**100%**

Table 6-3 shows how the 134 ISO 17799 controls compare to the specific HIPAA security standards implementation requirements.

The results of the comparison showed that a single, implemented instance of the ISO control satisfies more than one need of HIPAA. In addition, it showed that if ISO 17799 controls are implemented, an organization is well on its way to meeting HIPAA compliance with a very high percentage of exceeding the requirement. ISO17799 has a number of security controls not covered by HIPAA. Having a good Information Security Management System which complies with ISO, would therefore ensure that almost all of the requirements of HIPAA are met. The HIPAA Security rule includes a small number of requirements which are either not included in ISO, or for which HIPAA has a more stringent requirement.

Furthermore, the result of the comparison from a mobile computing perspective showed many of the controls as "required". A similar situation was evident when considering the risks associated with the wired network in section 3.1. It therefore can be argued that mobile computing security needs cannot be completely isolated from the common security requirement associated with the wired environment or the organization as whole. The result showed that mobile computing must be well integrated into the organization security plans as it touches many aspects in the administrative, technical and physical domains of the overall organizational security needs.

6.5 Conclusion

The comparisons in this chapter show all 11 ISO areas, and most of the components of each area, which contribute to the ability of an organization to conform to the requirements of the HIPAA Security Rule. The mapping of the ISO/IEC 17799 and HIPAA confirmed that both standards have in place all the necessary domains of security to be considered on fixed or mobile networks. The control domains encapsulate management, operational, and technical safeguards to protect an organization's assets.

Implementing ISO controls very much overlaps with HIPAA controls, although a few HIPAA controls need to be complemented. However, it is possible that not all controls of the standards may be required in an organization. A risk assessment is necessary to determine the controls needed and ensure that they go inline with the objectives of the organization. A documentation process will be required to provide rationales that will support control measures selected.

Nonetheless, the result of the comparative exercise provides a proactive guideline of what needs to be considered when creating a mobile-security solution that will meet healthcare regulatory requirements, as well as an internationally acceptable information security best practice while taking full advantage of mobile computing.

The next chapter is intended to create a secure mobile computing framework model that will meet healthcare mobile security needs. This will be based on the comparison result achieved in this chapter and the investigations and analysis preformed in the previous chapters.

Chapter 7
The Mobile Security Compliance Framework

Protecting the confidentiality, integrity and availability of patient information is no longer just a best practice for healthcare organizations, but a legal requirement. In the previous chapter, a comparative analysis of ISO 17799 and HIPAA was done to provide a baseline for establishing a mobile computing security solution in healthcare.

The comparison came as a result of the need to compliment ISO 17799 with the health specific regulatory standard in order to have a compliant mobile computing security strategy for healthcare. The comparison aimed at identifying the gaps in the ISO standard that need to be filled. The result of the comparison showed that although there is a major overlap between the standards controls a few gaps exist that have to be filled to meet the HIPAA requirement.

This chapter uses the comparative analysis discussed in the previous chapters to provide a security framework for mobile computing in healthcare in the form of a model. This will ensure that international Information Security best practice and healthcare specific legislative requirements are met. The framework model which is a three-step process will categorize the ISO 17799 controls in three different phases alongside the HIPAA controls to highlight the gaps. These gaps will be considered in each phase. The phases include the “Assess and Design” phase, “Implementation” phase and the “Management and Support” phase. The model is built on the Plan-Do-Check-Act (PDCA) model implemented by the ISO/IEC 27001 management system, the technical countermeasures discussed in Chapter 4 and the threats and analysis in Chapter 3.

The framework model will help identify and analyze gaps in an existing security state compared to requirements for security best practices and legal requirements. Furthermore, it designs and implements solutions to close those gaps, as well as ensure ongoing consistency and compliance.

7.1 Phase of the Model: An Overview

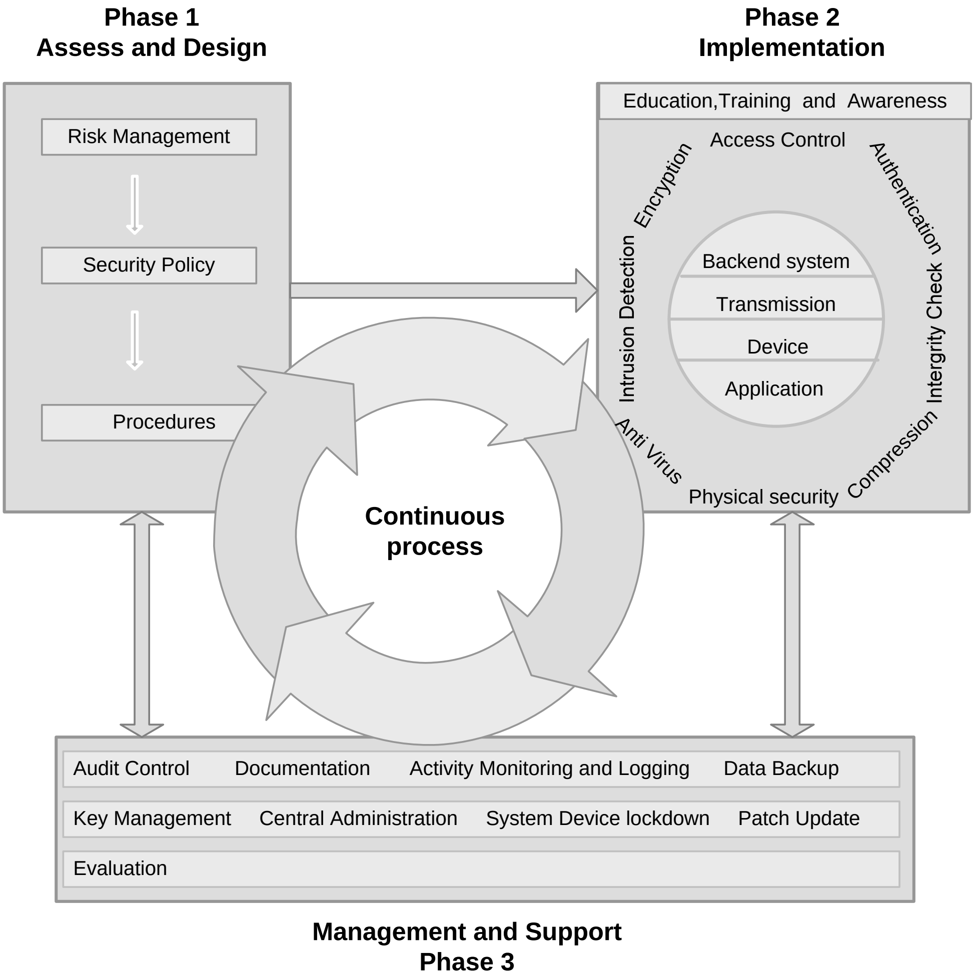

Figure 7.1 The framework model for mobile computing security in Healthcare

Phase 1 (Assess and Design Phase) strives to meet ISO management and operational requirement as well as the HIPAA administrative requirement. Phase 1 assesses the current level of information security to identify the gap between the current state and the standards requirement. The phase designs and documents policies, procedures and solutions to ensure protection, hence, creating a gap closure plan.

Phase 2 (Implementation Phase) strives to meet the ISO technical and physical security requirement as well as the HIPAA technical and physical safeguards. The section handles implementation of protection technology and services to help execute gap closure. The section also involves the Security

Education, Awareness and Training (SETA) plan. The SETA plan involves educating the organization on the security best practices and the use of technology. The education ensures that caregivers understand their responsibilities towards meeting the standards requirements.

Phase 3 (Management and Support phase) strives to meet the ISO management and operational requirement as well as the HIPAA administrative requirement. The section involves managing the security program to serve the organizational objectives. The section ensures that gaps remain closed and new gaps are not opened. Figure 7.1 depicts the mobile security model, showing the different phases and the content of their activities and how they relate to each other.

7.2 Phase 1 (The Assess and Design Phase)

This phase initiates the security process; it sets the tone that is supported in the other subsequent phases introduced in the previous section. This phase incorporates **Plan** (identify, analyse and evaluate the risks) and part of the **Do** (selecting controls and implementation of policies) section of the ISMS model. Table 7-1 shows a list of ISO 17799 controls that needs to be considered in this phase, along with the complementing HIPAA controls required in the phase. The controls appear in the order they appear in the standard documentation handbook. The tags associated with each control, categorises the control as will be discussed afterwards.

The controls listed in table 7-1 below can be categorized into three profile categories namely; “Risk Management”, “Security polices” and “Procedures”. These profiles are discussed in the following sub-sections.

7.2.1 Risk Management

The risk management profile encapsulates the controls tagged as “**Analysis”** “**Assessment”** and **“Treatment”.** Risk management, as discussed in section 5.2.2, typically includes, critical asset identification and classification, risk assessment (overall risk analysis and evaluation), risk treatment, risk acceptance and communication. This section of ISO very well meets the HIPAA requirement in this regard.

Table 7-1 ISO and HIPAA controls in phase 1

ISO 17799 Controls	
4.1 Assessing security risks **(Assessment)**	
4.2 Treating security risks **(Treatment)**	
5.1.1 Information Security Policy Document **(Policy)**	
6.1.1 Management Commitment to information security **(Policy)**	
6.1.2 Information security Co-ordination **(Policy/procedure)**	
6.1.3 Allocation of Information Security responsibilities **(Policy/Assignment)**	
	HIPAA 164.308 (a) (2) Assigned security responsibilities
6.1.4 Authorization process for information Processing facilities **(Policy/Assignment)**	
6.1.5 Confidentiality Agreements **(Policy/Contracts)**	
6.1.6 Contact with Authorities **(Policy/procedures)**	
6.2.1 Identification of risks related to External parties **(Analysis)**	
6.2.2 Addressing Security when dealing with customers **(Policy/procedures)**	
6.2.3 Addressing security in Third Party agreements **(Policies/contracts)**	
7.1.1 Inventory of Assets **(Analysis)**	
7.1.2 Ownership of Asset **(Policy/Assignment)**	
	HIPAA 164.308 (a) (2) Assigned security responsibilities
7.1.3 Acceptable use of Assets **(Policy/contracts)**	
	HIPAA 164.308(b)(1) (Business Associate Contracts and Other Arrangements), 164.308(b)(4) (Written Contract), and 164.314(a)(1) (Business Associate Contracts or Other Arrangements electronic)
7.2 .1 Classification guidelines **(Analysis)**	
7.2.2 Information labeling and handling **(Procedures)**	
8.1.1 Roles and Responsibilities **(Policy)**	
8.1.2 Screening **(Assessment)**	
8.1.3 Terms and Conditions of Employment **(Policy)**	
8.2.1 Management Responsibilities **(Policy)**	
8.2.3 Disciplinary Process **(Policy/Procedure)**	
8.3.1 Termination responsibilities **(Policy)**	
8.3.2 Return of Assets **(Policy)**	
8.3.3 Removal of access rights **(Policy/Procedure)**	
9.1.4 Protecting against external and environmental threats **(Analysis and treatment)**	
9.1.5 Working in Secure areas **(Policy/Procedures)**	
9.2.5 Security of equipment off premises **(Analysis and treatment)**	
9.2.6 Secure disposal or re-use of equipment **(Policy)**	
9.2.7 Removal of Property **(Policy)**	
10.1.4 Separation of development, test and operational facilities **(Policy/Procedures)**	
10.3.2 System Acceptance **(Policy/procedures)**	
10.5.1 Information back-up (**Policy/procedures)**	
	HIPAA 164.310(d)(2)(iv) (Data Backup and Storage) requires the back-up of ePHI before moving equipment
10.7.1 Management of removable media **(Procedures)**	
10.7.2 Disposal of Media **(Procedures)**	

ISO 17799 Controls	
Table 7-1 Continued…	
10.7.3 Information Handling Procedure **(Procedure)**	
10.8.2 Exchange Agreements **(Policy/Procedures/contracts)**	
10.8.1 Information exchange policies and procedures **(Policy/Procedures)**	
10.8.5 Business Information System **(Policy/Procedures)**	
11.1.1 Access Control Policy **(Policy)**	
11.2.1 User registration **(Procedure)**	
11.3.1 Password use **(Policy/Procedures)**	
11.3.3 Clear desk and clear screen policy **(Policy)**	
11.4.1 Policy on the use of network services **(Policy)**	
11.5.1 Secure log-on Procedures **(Procedures)**	
11.6.2 Sensitive system isolation **(Policy)**	
	HIPAA 164.308 (a) (4) (a) Isolating health care clearinghouse functions (Required).
11.7.1 Mobile Computing and Communication **(Policy/Procedures)**	
11.7.2 Teleworking **(Policy/Procedures)**	
12.1.1 Security requirements analysis and specification **(Policy)**	
12.3.1 Policy on use of cryptographic controls **(Policy)**	
12.4.2 Protection of system test data **(Procedures)**	
12.5.1 Change control procedures **(Procedures)**	
13.1.1 Reporting information security events **(Procedures)**	
13.1.2 Reporting security weaknesses **(Procedures)**	
13.2.1 Responsibilities and procedures **(Policy/Procedures)**	
14.1.2 Business continuity and risk assessment **(Assessment)**	
14.1.3 Developing and implementing continuity plans including information security **(Analysis/Procedures)**	
14.1.4 Business continuity planning framework **(Planning/Procedures)**	
15.1.2 Intellectual property rights (IPR **(Procedures)**	
15.1.4 Data protection and privacy of personal information **(Policy)**	
15.1.5 Prevention of misuse of information processing facilities **(Policy)**	

Like any other business risks, risk management for mobile devices must be evaluated. The first step to implementing a good mobile security strategy is to assess how mobile devices fit into the organization, how they will be managed and secured. A sound security practice should be dictated by the organization's objectives and the risks the organization faces. Information security planning should begin by understanding the importance and sensitivity of the information that is stored and manipulated.

The process begins by identifying where sensitive data is located, and providing answer to question like: "who controls the data?", "who has access to the data?" and "how it is currently stored and protected?" It is imperative to understand what information can be stored on mobile devices, even if not supported by the organization.

Notwithstanding, to proactively implement a mobile security policy, an organization must identify the likely threats and vulnerabilities as witnessed in Chapter 3, as well as evaluate their severity as suggested in Chapter 6 section 6.3.1. These activities are performed under the risk management function. The answers to the question or derivation from these activities will help the organization draft the mobile security policy.

7.2.2 Establishing a Security Policy for Mobile Computing

Once a risk assessment has been performed, a security policy needs to be implemented. Without a policy, nothing can be enforced. A policy is a guiding principle used to set direction in an organization. It can be a course of action to guide and influence decisions as stated in section 6.3.1 in chapter six. Such a policy will include as minimum a statement of institutional philosophy and goals regarding privacy and security, classification of information assets, standards for administering, controlling, and monitoring information use as mentioned in section 4.6. All statutory, regulatory or contractual security requirements should be recognized in the policy in this case as mentioned in Section 4 of ISO 17799.

These requirements are highlighted in the various ISO 17799 controls listed in Table 7–1. Table 7-1 shows a list of controls that need to be addressed at a policy level to be supported in the later phases. While most HIPAA security controls are in similar lines with ISO17799, HIPAA 164.308 (a) (2) “Assigned security responsibilities” specifically requires that a single person is responsible for ePHI. In addition, 164.308 (a) (4) (a) “Isolating health care clearinghouse functions” requires that policies and procedures be in place to separate PHI from other operations. These requirements should be considered in drafting the security policy.

Most of the ISO 17799 controls contain a procedure policy in the likes of a **mini-mission statement**. This procedure policy is usually an extension of an existing general security policy. The policy is meant to keep malicious threats out, while helping to direct the behavior of users. Employee policies will help deter risks associated with the human factor discussed in Chapter three, section 3.4. Most non technical measures are appropriate to avoid accidental disclosure, curiosity or intentional driven disclosure of health information with the assistance of the audit trail capability discussed in chapter four, section 4.6. The policy should be extended to business partners or external users accessing the organization resources. Handling sensitive health information in confidence requires an effective supervisory and legal structure that provides sanction against detected misuse. More information highlighted in section 5 of ISO 17799.

A policy ensures that appropriate levels of functionality are applied to the diverse groups of users and/or devices. The security policy will assign user responsibility and dictate access control permissions, providing varying levels of access depending on the user, device and data in question. The policy should cover controls that include items such as the types of information that is to be placed on the device, the security configuration of the device, including all software that is to be used to protect the information; and permissible modes of operations, and use of removable media. The policy should force compliance across all devices accessing the organization network and ePHI, regardless of whether the organization or an individual purchased the device.

The policy should be written in an understandable way and procedures need to be in place. The procedure should provide a series of steps to be followed as a consistent and repetitive approach on the appropriate use of mobile devices and solution implementation. Adherence to policies and in implementation procedure for external parties should be enforced by signing an agreement as discussed under the sub section titled contracts.

7.2.2.1 Contracts

Contracts are agreements established for the accessing, processing, communicating or managing information, software or services between the organization and external parties or employees. For instance an agreement can be established to ensure that external parties and employees will abide to the policies set out by the organization. HIPAA 164.308(b)(1) and 164.314(a)(1) “Business Associate Contracts and Other Arrangements”, 164.308(b)(4) “Written Contract” requires contracts of obligations by employees, third parties and contractors.

Furthermore an agreement can be established on the procedures to ensure traceability and non-repudiation of information exchanged. More so, an agreement that will ensure that third parties will protect information once it is in their possession and are willing to take full responsibilities for their actions should be established. In the event of violation, the contract plays a vital role. The controls tagged contracts in Table 7-1 are discussed Chapter 6. The next Phase will discuss how the communication of policies and procedures can be achieved, as well as the implementation of technological controls to support the policies.

7.2.3 Procedures

A procedure is a series of prescribed steps followed in a definite regular order which ensure adherence to the guidelines set forth in the Policy to which the Procedure applies. Procedure manuals should contain instructions, guidelines and parameters for members of the mobile workforce who work with or have access to ePHI. For example, the data back up implementation specification requires that entities have data back procedures. A covered entity will document step-by-step procedures for conducting data back-ups and how often these shall be conducted. HIPAA 164.310(d)(2)(iv). “Data Backup and Storage” specifically requires that PHI is backed up before moving a device.

Furthermore, procedures can be in place to show a user how to achieve data integrity using digital signatures hinted in Chapter 4, section 4.3. Most of the controls in Table 7–1 require that procedures are in place to achieve their various objectives. Most of the requirements encapsulate the HIPAA requirement, however, a HIPAA requirement 164.312 (a) (2) (b) “Emergency Access Procedure” specifically requires emergency access procedure in the event of an incident.

Caregivers handling sensitive health information need to be made aware of the security policy’s importance and understand why they have a responsibility to ensure its correct use. To maximize compliance, the policy should be well communicated.

7.3 Phase 2 (The Implementation Phase)

This particular phase incorporate the **Do** section of the ISMS model, which requires the implementation of controls to mitigate the risks discovered in the first phase of the model. The ISO 17799 controls to be used at this stage are outlined in table 7-2 below.

Table 7-2 ISO and HIPAA controls for Phase 2

8.2.2 Information Security awareness, education and training **(Deterrent)**
9.1.1 Physical security perimeter **(Physical security)**
9.1.2 Physical entry controls(**Physical security)**
9.1.3 Securing offices, rooms and facilities (**Physical security)**
9.1.6 Public access, delivery and loading areas (**Physical security)**
9.2.1 Equipment siting and protection (**Physical security)**
9.2.3 Cabling Security (**Physical security)**
10.4.1 Controls against Malicious codes (**Integrity control)**
10.4.2 Controls against mobile code (**Integrity control)**
10.8.3 Physical Media in Transit (**Transmission security)**
10.8.4 Electronic Messaging (**Transmission security)**
10.9.1 Electronic Commerce (**Transmission security)**
10.9.2 Online Transactions (**Transmission security)**
10.9.3 Publicly available Information (**Transmission security)**
11.4.2 User authentication for external connection *(***Authentication)**
11.4.3 Equipment identification in networks *(***Access control / Authentication)**
11.4.4 Remote diagnostic and configuration port protection (**Access control)**
11.4.6 Network connection Control (**Access control / Authentication)**
11.4.7 Network routing Control (**Access control)**
11.5.2 User identification and Authentication (**Access control / Authentication)**
11.5.4 Use of system utilities (**Access control)**
11.5.5 Session time-out (**Access control)**
11.6.1 Information access restriction (**Access control)**
12.2.1 Input data validation **(Integrity control)**
12.2.2 Control of internal processing **(Integrity control)**
12.2.3 Message Integrity **(Integrity control)**
12.2.4 Output data validation (**Integrity control)**
12.4.3 Access Control to program source code (**Access control)**

The HIPAA controls corresponding to these controls have similar objectives as highlighted in the previous chapter. The controls are tagged like the previous table and will be discussed afterwards. This phase looks at implementation controls from two perspectives namely, the administrative and the technical perspectives. These perspectives are discussed individually in the subsequent sections.

7.3.1 The administrative perspective

Among the implementation measures listed in the table, the first requirement which deals with education, training and awareness is an important part of a mobile security program as stated in section 6.3.5 control >>8.2.2 in Chapter 6. This is discussed in the subsection below.

7.3.1.1 Training, Education and Awareness Program

A security awareness and training program can be defined as one of the key factors for the successful implementation of an organization-wide security policy.

The main aim is to define and outline the specific role each of employee in the effort to secure critical organizational assets, as well as covering in detail each of the core elements in the security policy. Caregivers should be made aware of the vulnerabilities and threats associated with mobile devices and the repercussion to the organization as shown in Chapter 3. Training should include physical security of the device as highlighted in section 6.3.6 in chapter 6, the mobile device security policy as achieved in the previous section, a review of the types of information that can be stored on the device, and the procedure to follow if a device is lost or stolen, infected or compromised.

In addition, the technical measures discussed in Chapter 4 should be well communicated to the appropriate parties. The message should highlight for example caregivers' procedures on the use of digital signatures to achieve integrity and non-repudiation discussed in sections 4.3 and 4.5 respectively. Other important training will be on the user's password management and use of digital certificates as hinted in section 4.1 in Chapter 4. It is important to know that one of HIPAA's controls marked "addressable" suggests that administrators or users responsible are trained on procedures for monitoring of log-in attempts (164.308(a)(5)(2(C) "Log-in Monitoring".

Alerts, reminders, and education of users, can be very effective in reinforcing ethical behavior of users. The mobile devices capabilities discussed in Chapter 2, section 2.10 provide an excellent platform for sending such reminders and users accessing certain operational procedures to avoid mistakes, as discussed in section 3.4 in Chapter 3. The next section looks at some of the technical measures that compliment the human factor measure.

7.3.2 The technical Perspective

Phase 2 also presents the layered-security model and some of the technologies or mechanisms that function at each level. This phase basis its structure based on the threats and vulnerabilities discussed in Chapter 3 and the technical security mechanisms discussed in chapter 4. As analyzed in chapter 6, ISO and most especially HIPAA have a number of key requirements for protecting and securing data (ePHI) accessible on mobile devices.

In order to protect the confidentiality, integrity and availability of health information the HIPAA security rule specified measures such as Authentication, Encryption, data integrity, and Transmission security. These specifications are in similar lines with ISO recommendation as shown if Table 7–2 but even more so. In addition, both standards regard physical security and access control as security aspects that must be considered, which are indeed necessary for a mobile solution in healthcare as discussed in sections 6.3.6 and 6.3.8 in chapter 6 and section 4.2.2.5 in chapter 4 respectively.

Access control limits user access to resources such as applications and data, based on administrative access rights, as stated under the user role and responsibility in the policy. To efficiently manage access rights, the role based access control is most appropriate as it is based on responsibilities. A role based access control can help in audit trail situation as hinted in chapter four section 4.6 and section 6.3.7 in Chapter 6, ISO 17799 control 10.10.1 “Audit Logging”.

As information flows from backend servers out to mobile devices, a blend of technical security measures, as shown in table 7-2, and discussed in Chapter 4, are required to provide the highest level of protection. As shown in Chapter 4, the areas to be protected in order to provide a sound mobile security implementation in healthcare include:

- Backend Systems: Access to the backend servers or the central network
- Transmission: Data traveling across the network
- Device: Data stored on the device
- Application: Remote or device resident vertical applications

These areas are discussed in detail alongside their required security mechanism.

7.3.1 Backend systems and the Central Network

This area assumes that a wired network security is in place, such as a perimeter firewall, a network based antivirus, network based intrusion detection and a vulnerability management system as well as a structured demilitarized zone (DMZ) as mention in Chapter 3, section 3.1. In the event where a WLAN exists, it is assumed that access points are placed behind the firewall. In other words, the WLANs should be subject to the same interrogation associated with the wired network as in Chapter 4 section 4.6.

Mobile computing in healthcare requires that caregivers periodically exchange data with the central network. Frequently they may need to connect over public wide area wireless networks to synchronize or access data. As discussed in Chapter 3, users are likely to unintentionally introduce malware to the central network via infected devices, paving way for hackers. In addition, an upset employee can copy sensitive files from the network to his personal device and leave the building.

Healthcare organizations must protect the network from unwanted outside sources. The use of technologies such as the 802.1x and PKI, as discussed in Chapter 4 becomes prominent to provide strong authentication. VPNs should be used to provide a secure connection over public wireless networks, to the central network. A VPN tunnel can terminate on a VPN-enabled router, firewall, or server within the DMZ. Additionally, PKI can be used to add strong authentication, encryption, digital signing and non repudiation.

As ISO and HIPAA as shown in Table 7-3 and as discussed in section 6.3.8 in chapter six, outline access control to maintain sensitive information (ePHI), the rule applies to the mobile device implementations that retrieve sensitive data from the backend server. For example, the access control will occur at the database or application server that stores and forwards ePHI.

When a user requests ePHI from his/her device, the responding server will first authenticate the user then determine if the user is authorized to access the requested information. The role based access control will prevent access to patient information. The PKI digital certificate can ensure that this is fully achieved. Network authentication needs to be done for all connectivity to the network to prevent rogue attacks at points of entry to the organization’s network. Authorization should be done for all users and devices intending to access the main network locally or via remote VPNs. Devices should have up to date security software before granting then access.

Furthermore, physical access control to network facility will prevent subversion of operating systems. Once an intruder has access to a machine, hence to its operating system, it is possible to download any available number of cracking tools that can used to extract passwords or defeat file level encryption. In addition physical access control will prevent unauthorized users from stationing rogue wireless access points.

Notwithstanding, HIPAA and ISO also require that an inactive session should be shutdown after a defined period of inactivity as shown in Table 7-2 and discussed in Chapter 6 section 6.3.8. It is imperative that a session shuts down after a period of inactivity because an open session opens up a window of opportunity for unauthorized access especially when accessing remotely.

7.3.2 Transmission Security: Protecting Data traveling across the network

An attribute of mobile computing is that data is often in transit. A transmission security plan is imperative as users wirelessly transmit or access ePHI with mobile devices. Data must be protected from interception when traveling across a wireless network. Transmission security protects health information from unauthorized access during transmission over a network. ISO and HIPAA suggest Administrators implement encryption and integrity controls as shown in Table 7-2. Transmission protection requires the use of data encryption or the use of a Virtual Private Network (VPN) as discussed in Chapter 4. VPNs create an encrypted connection between a mobile device and a network and in addition provide integrity controls. SSL VPNs provide end to end encryption for maximum protection of data across the network. IPSEC VPN in use with a PKI solution will provide end to end encryption. A PKI solution will provide data encryption and in addition provide integrity control using digital signatures as well as non repudiation as discussed in chapter 4. Furthermore, as stated discussed in Chapter 4, section 4.2.2.6 another mechanism that can be considered for transmission security is encryption.

7.3.3 Device: Protecting Device and Data stored on the device

HIPAA and ISO require processes in place to safeguard equipment and facilities to prevent loss, damage, theft or compromise of assets and the interruption to the organizations activities. The sections tagged physical security in Table 7-3 provides this protection. Those controls can be found in more detail in Chapter 6. In Chapter 2 it was discussed that mobile devices provide numerous advantages. The advantage of most mobile computing devices rests in their capability to provide multiple applications alongside local processing and data storage. In spite of the advantages, data stored locally on a device is vulnerable to unauthorized access, erroneous usage, and deliberate misuse. In addition the small size and portable nature of mobile devices, their removable memory sources also make them vulnerable to loss or theft.

To protect against vulnerabilities associated with mobile devices, as discussed in Chapter 3, strong access controls and data protection measures should be in place as discussed in Chapter 4. Access control policy can be achieved by forcing authentication at logon. Power-on and user authentication protects data, device functions, applications and network access from unauthorized access. It is also important to enable options that will automatically lock-out access privileges when a user exceeds a certain number of access attempts. Better still; automatically destroy data and application stored on the device as discussed in section 4.2.1.3, but consider the odds that it might be the latest data. An immediate field to a memory module or remote backup can be very helpful at this point. Backups are discussed in Chapter 4, section 4.6 and in section 6.3.11. It is also highlighted phase three.

Encryption policies should be in place to make data unreadable and inaccessible as discussed in Chapter 4. Data encryption, both locally on the device and on removable media should be enforced. Encryption will prevent removable media to be used on unprotected devices to gain access to the data. In addition, compression can assist greatly in the security effort as discussed in chapter 4.

Furthermore, as stated in Chapter 4, virus and spyware protection is imperative. It is important to check for viruses and update antivirus definitions whenever a device attempts to connect to the organization’s network. In addition, a personal firewall should be enabled, to control traffic to the device.

Finally, physical security from the part of the user is important. As mentioned in Chapter 3, physical access does not require any special skill. An organization is likely to suffer more from exposure of sensitive data through loss and theft, than someone monitoring signals in transit. Users must try and observe the clear desk policy, which should include keeping or hiding mobile devices in a safe place. Other best practices will be considered in the management and support phase below.

7.3.4 Application: Remote or device resident applications

Like network and device level authentication, only authorized users should be able to access an application. Applications placed on the Web for access by customers, partners or employees remotely can provide a ready target to individuals with malicious intent.

To protect against threats, an application shield or application-level firewall can be used to ensure that incoming and outgoing requests are permissible for the given application, as discussed in Chapter 4. Applications include: databases, email or any similar applications. In addition, controls like input and output validation, should be part of an application as discussed in Chapter 6, section 6.3.9. Furthermore, a vertical application code should be signed in situation where the building of an application is done externally as discussed in Chapter 4. The controls aimed to provide management and support for phase one and two are discussed in the next section.

7.4 Phase 3 (The Management and Support Phase)

Phase 3 incorporates the **Check** and **Act** phase of the ISMS which is responsible for monitoring and reviewing phases one and two of the model to ensure effectiveness. The **Act** which deals with improvement ensures corrective and preventive actions are taken to meet due diligence.

This phase requires a periodic evaluation and assessment of both technical and non technical measures taken to achieve compliance with regulation and to be prepared to continue to ensure that compliance requirements are met should changes in the environment occur. Table 7-3 shows a list of ISO along with complementing HIPAA controls that will provide management and support for the “assess and design” phase and the “implementation” phase.

The controls contain a whole list of activities to meet their various objectives. At

Table 7-3 ISO and HIPAA controls in phase 3

ISO 17799	
5.1.2 Review of the Information security policy	
6.1.7 Contact with Special Interest group (SIG)	
6.1.8 Independent Review of Information Security	
9.2.2 Support utilities	
9.2.4 Equipment Maintenance	
10.1.1 Documented Operating Procedures	
10.1.2 Change Management	
10.1.3 Segregation of Duties	
10.2 .1 Service Delivery	
10.2 .2 Monitoring and review of third party services	
10.2 .3 Managing changes to third Party services	
10.3.1Capacity Management	
10.5.1 Information back-up	
10.6.1 Network Controls	
10.6.2 Security of Network Services	
10.7.4 Security of System documentation	
10.10.1 Audit Logging	
10.10.2 Monitoring System use	
	HIPAA 164.308(a)(5)(ii)(c)(Log-In monitoring) requires training monitoring of log-in attempts
10.10.3 Protection of log Information	
10.10.4 Administrator and operator log	
10.10.5 Fault Logging	
10.10.6 Clock Synchronization	
11.2.2 Privilege Management	
11.2.3 User password Management	
11.2.4 Review of user access rights	
11.4.6 Network connection Control	
11.5.3 Password management System	
11.5.6 Limitation of connection time	
11.6.2 Sensitive system isolation	
12.3.2 Key management	
12.4.1 Control of operational software	
12.5.2 Technical review of applications after operating system changes	
12.5.3 Restriction on changes to software packages	
12.5.4 Information leakage	
12.5.5 Outsourced software development	
12.6.1 Control of technical Vulnerabilities	
13.2.2 Learning from Information security incidents	
13.2.3 Collection of evidence	
	HIPAA 164.316(b)(1) Policies and Procedures Documentations
14.1.1 Including information security in the business continuity management process	

ISO 17799	
Table 7-3 continued…	
	HIPAA 164.312(a)(2)(ii) (Emergency Access Procedure) requires procedures to support emergency access
14.1.5 Testing, maintaining and re-assessing business continuity plans	
15.1.3 Protection of organizational records .	
	HIPAA 164.316(b)(1) Policies and Procedures Documentations
15.2.1 Compliance with security policies and standards	
15.2.2 Technical compliance checking	
15.3.1 Information systems audit controls	
15.3.2 Protection of information system audit tools	

this point, the ISO controls encapsulate the HIPAA controls, although with a few exceptions. For instance, section 164.310(d)(2)(d) “Data backup and storage’ of Table 7-3 ISO and HIPAA controls in phase 3. HIPAA, as mentioned in section 7.2.3, states that backup of PHI should be made before moving any equipment, in this case, the mobile device. If caregivers synchronize their information with a remote database or external memory module as soon as it is entered into a device, that will solve the problem of the latest data discussed in section 7.3.3. Furthermore, the HIPAA control 164.312(a)(2)(ii) “Emergency Access Procedure” which requires procedures to support emergency access should be considered. In addition, the section of HIPAA tilted “Policies and Procedures Documentations” (164.316(b)(1)) requires that the record retention time limit be six years. As ISO control “15.1.3” stated “an organization should adopt the retention time limit as specified by their national laws or regulations in which the record is to be kept secured. to serve as evidence in future”.

This management and support phase for secure mobile computing employs a variety of tools, applications, and devices to assist IT administrators in monitoring and maintaining security and compliance. Details on management tools can be found in Chapter 4, section 4.6. While security controls management changes to the configuration of devices and the network, management is required to control and update security changes, such as antivirus engines and signature files, personal firewalls, operating system patches, and many more.

In order to enforce policy, organizations should implement policy-based applications to ensure that measures put in place to protect the privacy of sensitive health information are not defeated. The policy administration should be centralized and automated. The policies should be well integrated into an organization's directory, for example the Microsoft Active Directory. Centralized control and automation ensure uniformity of security on all systems and greatly reduce the burden of administering multiple systems each time a new or change in employment status is made.

Furthermore, the security software should be able to monitor, audit and report vital statistics about each user's network access. As mentioned in Chapter 4, section 4.6 this serves as deterrent for user's unethical behavior. Besides that, these activities will validate and ensure compliance with security policies as required by ISO and HIPAA as can be seen in table 7-3.

The information security policy document must be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness. Section 6.3.2 has more details on the review of policies. In addition, information system activity, such as audit logs, access reports, and security tracking reports, must be regularly reviewed. This will identify threats and vulnerabilities that are said to be continuous in Chapter 3, section 3.1.

Furthermore, part of the management strategy should ensure that devices and data are backed up to allow for rapid user recovery after device or data is loss, stolen or corrupted. Sections 4.6 and 6.3.7 discuss more on backup. In addition, key management as recommended by ISO as shown in the table 7-3 above, should be in place. Key management is discussed in more detail in section 6.3.9 in Chapter 6.

Finally, but not the least, documentation is important for maintaining systems and procedures. It plays an important role throughout the lifecycle of the model. Documentation provides administrators with a customized knowledge base of systems configuration data, operational procedures and policy information. It ensures consistency through staff changes and organizational transitions. Documentation assists in the audit process, creates an accurate record of systems design, maintenance, upgrade and replication. It establishes a historical basis for future decisions.

7.5 Conclusion

To have an effective mobile security solution for healthcare, careful planning has to be defined to secure and manage mobile devices used. The activities in the phases outlined in the model need to be considered in order to achieve an effective security solution as well as to ensure up to date compliance with ISO and HIPAA requirements. Using the ISMS model for the mobile security model ensures a proactive and an ongoing security deployment and management. Security and management are mutually dependent and are necessary for the security solution to scale. The implementation of controls should depend on the risk assessment which must be continuous, in order to ensure new vulnerabilities and threats are identified and appropriate actions are taken.

Not withstanding, an existing LAN can be vulnerable, providing another access point for worms, viruses and other malicious attacks on an organization's networks which can in turn infect mobile devices. In order to have a successful mobile security deployment, the LAN must have the proper security in place.

Mobile security should be centralized and automated to ease the burden of administration as well as balance usage and security. Centralized and automated policy base solution controlling devices will allow continuity of business functions, and provide user transparency which in turn enhances user productivity. As users are focused on the tasks necessary to be successful in their roles, trusting security functions to the user will put the whole solution at risk. It is therefore important that security is controlled centrally and management should be automated.

Although all controls in ISO are important and should be considered, the relevance of any control should be determined in the light of the specific risks an organization is facing.

Chapter 8

Conclusion

Chapter 7 provided a mobile computing security model for healthcare in compliance to Information Security Management program ISO 17799:2005 and the healthcare industry specific requirement as presented in the HIPAA security rule. The model ensures that organizations meet privacy regulatory requirements while, at the same time, ensuring customers that international standards for the protecting customer information processed and accessed by mobile devices are used.

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

8.1 Summary and Contribution

As discussed, healthcare organizations are, at present, functioning in an intricate and challenging era of Information Security Management and regulatory compliance requirements. They are required to ensure compliance with multiple regulatory requirements making such compliance a complex issue. Less than obvious is the fact the mobile computing has become a new landscape in today's healthcare organization. Mobile computing has become prevalent in the healthcare industry. The ability to work with information on portable devices regardless of location is appealing and provides many advantages to the healthcare industry. The technology enables greater productivity and efficiency in the industry.

However, mobile devices have to be considered for compliance. The advents of mobile devices and remote systems have made it possible for data to be carried to locations beyond the traditional organization's walls. In addition, new threats to security continue to appear rampantly. It is imperative that organizations protect themselves and their customers from these threats. More so, with the increasing government and industry regulations, protection is no longer just desirable, it is mandatory. Failure to comply with requirements can result in heavy consequences such as, the loss of shareholders trust, a bad reputation for the industry and other legal ramifications for the industry.

The problem addressed in this project is “what security strategy should IT administrators in healthcare follow in order to protect the sensitive information that is continually accessed, processed and stored on mobile devices?” The primary objective of this research was to develop a model that will address the security challenges mobile devices pose to healthcare organizations.

In order to achieve the objective, the dissertation illustrated that the approach of finding the solution was to understand the concept of mobility and how it relates to the healthcare industry. In addition to this finding was to identify the issues investigate the issues surrounding the privacy and security in healthcare. With an intense literature study an understanding of the concept of mobility, how it affects healthcare and the privacy and security issues was achieved.

Further, to answer the question, an understanding of mobile computing technologies along side the factors that make it is what is was required. This was achieved and was followed up by identifying the threats and vulnerabilities associated with the technologies and how they affected the privacy and security of health information. In an effort to provide a solution, an investigation into the existing technological means available was conducted, and the mechanisms found where categorized according to how they solved the privacy and key security components in healthcare which include confidentiality, integrity, availability, authentication and non-repudiation.

Realizing that threats continue to evolve with overall developments and ultimately, security and privacy of health care information were also a peoples’ problem a new security dimension was considered. At that point, an investigation into a suitable ISMS was performed, where the ISO set was selected. Considering the limitation associated with ISO and the need to compliment the controls with more healthcare specific requirements, an investigation on health legal standards was conducted. HIPAA was arguably selected as the complimenting standard. In order to find out to what extent the ISO controls met HIPAA controls, a comparison analysis and mapping had to be performed and the result of each compared result was perceived from a mobile computing standpoint.

Based on the result of the investigations and the comparative analysis performed in the chapters, a compliance model for mobile computing for healthcare was developed. The compliance strategy based on the Plan, Do, Check and Act model provides advantages to an organizations ongoing compliance efforts and successful mobile security deployment.

8.2 Benefits of the framework model

The implementation of the framework model will help healthcare organizations in ensuring due diligence and compliance with the necessary industry requirement while taking advantage of mobile computing. It will increase trust in business partners and patients. The implementation of a well-established compliance program will increase trust with other business partners because they are certain that international best practices are being used. In addition, it will enhance the trust of patients because they can be assured that their information is kept secure and private.

The mapping eliminates redundancy in the auditing process ensuring that no time and cost is wasted on duplicated security controls already implemented when dealing with HIPAA and ISO. Conformance with the proposed framework model will impart that an organization has addressed all the key issues of Information Security. It will ensure continuous vulnerability, threat and solution management, thus reducing breaches associated with mobile computing.

Compliance with the framework will ensure that appropriate assessment is carried out before mobile computing initiatives are carried out in healthcare. The design of the model ensures that controls and cost are part of the assessment. Following the approach will balance usability and cost while providing full mobile computing capability to healthcare.

The framework model provides a security solution that ensures that an up-to-date compliance with standards and regulations is achieved. It streamlines the security requirement with the overall organizational objective. In addition, using the framework ensures a proactive and an ongoing security deployment and management. The framework model incorporates security and management which are necessary for a security solution to scale.

8.3 Chapter overview

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

Chapter 1 introduced mobile computing and its infiltration into the enterprise. In addition the key concepts of Privacy and Security were discussed. The chapter outlined how important these fields are for the healthcare enterprise and how they relate to one another. The problem statement, as well as the objectives, for the dissertation was defined and the methodology used towards the solution to this problem statement was outlined.

Chapter 2 discussed and illustrated the concept mobility and its influence on the healthcare industry. The traditional mobility and the possible role of mobile computing in healthcare were also discussed. Eventually, the challenges associated with mobile computing security in healthcare were highlighted and the possible impact on the privacy and security of health information discussed.

Chapter 3 proceeded to identify the threats and vulnerabilities associated with mobile computing and how they impact on the privacy and security of health information in healthcare. After identifying the threats and vulnerabilities associated with mobile computing, **Chapter 4** investigated the existing measures to thwart the risks associated with the threats and vulnerabilities investigated in Chapter 3. The chapter concluded that the existing counter measures were tailored more towards technical security, and were not enough to meet the mobile computing security requirement. Eventually, the chapter recommended encorporating the countermeasures into an Information security management system.

Chapter 5 introduced and discussed an Information security management. The elements that makeup the ISMS were highlighted and the framework model the concept is based on was discussed. The chapter provided a roadmap for creating the mobile computing security framework model for healthcare organizations. The chapter described an international security standards framework for managing Information Security. ISO 2700 and ISO 17799, the mostly widely used International Security Management standard set were examined in comparison to other standards. The chapter looked at how additional existing healthcare specific standards can be used to complement the ISO 17799 and fill any exposed gaps to overcome some of those criticisms.

In order to achieve that, HIPAA among others was selected to be compared to ISO 17799 to provide a baseline for creating a mobile security solution to meet compliance. The convergence was necessary because HIPAA security rule had more stringent requirements in the protection of electronic based medical information.

Chapter 6 was dedicated to the comparison between an Information Security Management standard (ISO 17799) against the HIPAA security rule. The analysis of the comparison result illustrated that there is quite an overlap between the standards. This confirmed that the strategy would serve to eradicate redundancy while complying with ISO and the HIPAA security rule. The chapter concluded stating the need for a model to ensure compliance with regulatory requirements while ensuring patients that best practices for Information Security Management are being used to ensure the privacy and security of medical information accessible on mobile devices.

Chapter 7 put together a framework model which is based on the ISO/IEC 27000 ISMS Plan Do, Check and Act model. It is formed by the result of the comparative analysis and the technical countermeasures existing to thwart risks associated with mobile computing. Its main intention is to establish a roadmap for healthcare to follow in their endeavors to meet Information security standards and regulatory requirements when dealing with mobile devices. The phases that constitute this compliant framework model were discussed.

The proposed framework model comprises three phases: the “Assess and Design”, the “Implementation” and the “Management and Support” phase. Each phase identifies specific actions and outputs with detail requirement based on the comparison in Chapter 6. The framework model views mobile security as an essential responsibility for all levels and must not be seen as set of technical requirements emanating from the Chief Information Security Officer or Chief Security Officer but must considered as a corporate compliance program.

8.4 Future Research

This project has provided a guideline for healthcare organizations to follow to ensure that mobile devices are considered for compliance of security standard and regulatory requirements. Chapter 7 touched upon on the phases that constitute the proposed mobile security compliance framework model in healthcare. Possible directions for future research include a detailed practical implementation of the proposed framework. Furthermore, how precisely the organizational Information Security Policy should be drafted and communicated to achieve has not been addressed in this dissertation. A proper Security, Education, Training and Awareness (SETA) plan has to be established to ensure proper communication to the users.

In addition, research is also required into the development of a tool or program that will be able to perform a cross reference of standards or regulatory controls to find an overlap in the event that new regulations are to be met. Furthermore, there exist the need for a capable system where controls from different standards can be updated by tools or programs in an organization. This will help in the event where amendments or additions of controls are made and then tools can automatically generate the necessary report to the Information Security Officer. This will assist greatly where transboarder information exchange is necessary to save lives and should not be hindered by non compliance to national or state laws of other countries.

Besides that, research is required in the development of a universally acceptable Information Security Standard. An investigation into national laws and state laws of countries should be engaged and a point of convergence should be found. This will provide a model that will be globally acceptable; hence, it will eliminate boundary issues and make critical healthcare information available to help save lives.

Nonetheless, technology changes everyday and it is continuously accompanied by new threats and vulnerabilities. It is imperative to keep track of changes and be on the lookout for the continuously evolving threats and vulnerabilities that can cripple activities. Adopting such a system will provide a proactive means of preventing loss and damage to an organization. Furthermore, another possible research is to determine what possible combinations of existing security measures can provide the strongest possible security while at the same time balancing usability and cost.

In addition, the area on how to successfully integrate a mobile security solution into the traditional wired infrastructure or an organization’s directory can be investigated. Also, areas like the secure integration of mobile applications with the traditional information systems can be investigated.

8.5 Epilogue

Having proper security measures in place can be a key success factor in the healthcare industry. However, it is unthinkable to impose security constraints so tight that they would prevent emergency caregivers from accessing the record of a seriously ill patient. Care has to be taken to avoid caregivers' frustrations in passing too many security hurdles for frequently accessed records. Usability and security must be well balanced. A risk management process is very important as it plays a vital role in achieving a sound and successful security solution.

References

Ahmad, A., Chandler, R., Dharmadhikari, A. A., & Sengupta, U. (2003). *SIM-Based WLAN Authentication for Open Platforms*. Technology at Intel Magazine. (Retrieved November 5, 2006 from http://www.linuxdevices.com/articles / AT7681519444 . html)

Ahtianen, A., Kaaranen, H., & Naghian, S. (2005). *Evolution from GSM Multi Access. UMTS Networks*. (pp.15 – 24) England: West Sussex, Chichester, Southern Gate. John Wiley and Sons ltd. [ISBN:0470011033]

Antwerpen, S. (2004). The *Role of Audit and Certification in Digital Preservation ERPANET*. (Retrieved May 19, 2006 from http:// www. erpanet .org/events /2004/antwerpen/erpaWorkshop-Antwerpen_TrainingMaterial.pdf)

Anderson, D. (2005). *HIPAA security and compliance*. (Retrieved April 7, 2006 from http://www.tdan.com/i033ht04.htm)

Airespace. (2004). *Improving Patient Care through Wireless Mobility*. Airespace technology. (Retrieved April 16, 2006 from http://www.airespace.com/ technology/improving_patient_care.php)

Ash, R., & Persall, M. (2002). The principal as chief learning officer: The new work for formative leadership. Education World, 22 (8). Boles, KC (1992).

ASM. (2006). EKG or Electrocardiogram. (Retrieved April 26, 2006 from http://www.heartsite.com/html/ekg.html)

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

Ala-Laurila, J., Haverinen, H., Mikkonen, J., & Rinnemaa, J. (2002). *Wireless LAN architecture for mobile operators*. In Wireless Local Area Networks: the New Wireless Revolution, B. Bing, Ed. John Wiley & Sons, New York, NY, 159-176.

Ashley, M. (2006). *Layered Network Security: A best-practices approach*. Still Secure. (Retrieved July 20, from www.stillsecure.com/docs/StillSecure _LayeredSecurity.pdf)

Banerjee, N., Wu, W., Das, S.K., Dawkins, S. & Pathak, J. (2003). *Mobility Support in Wireless Internet*. IEEE Wireless Communications, 10(5), 54-61.

Bajaj, S., Barton, M., & Brownhill, B. (2004). *Providing highly secure access to information across government organizations*. (Retrieved June 30, from http://www-306.ibm.com/software/alliances/verisign/pdf/Secure_Access _to_Government_Information_WP_V1.0.pdf

Beard, M.(2006). *The Challenges of Unwired Freedom*. Wireless Week. (Retrieved August 20, 2006 from http://www.wirelessweek.com/ article/ CA6362711.html

Becker, S., A., Sugumaran, R., & Pannu, K. (2004). *The use of mobile technology for proactive healthcare in tribal communities.* In Proceedings of the 2004 Annual National Conference on Digital Government Research (Seattle, WA, May 24 - 26, 2004). ACM International Conference Proceeding Series.

Beaver, K. (2003). *How secure is the Ultra Wide Band (UWB) wireless technology I'm hearing more about lately?*. Security and UWB. (Retrieved July 23, 2006 fromhttp://searchmobilecomputing.techtarget.com/expert/ Knowledgebase Answer/0,289625,sid40_gci918062_tax299684,00. html?bucket=ETA)

Bialoglowy, M. (2005). *Bluetooth Security review, Part 1.*Secuirty Focus (Retrieved August 4, 2006 from http:// www.securityfocus.com/ infocus/1830)

Bitcon, M. (2003). *Can you begin by outlining the work of Fife Fire & Rescue?*. Electronic Government Magazine. (Retrieved May 03, from http://www. electronic-government.co.uk/archive/index2.cfm?article_id=153)

Bishop, L., & Brown, E.G. (2005). Physicians and Technology Study. Usability holds back MD handheld usage. Forrester Research. (Retrieved March 15, 2006. http://www.forrester.com/Research/Document/Excerpt/0,7211, 36530,00.html)

Bisson, J., Saint-Germain, R. (2003). *The BS 7799 / ISO 17799 Standard For a better approach to Information Security*. (Retrieved, October 10, 2006 from http://www.callio.com/files/wp_iso_en.pdf.)

Blair, J. (n.d.) *An Overview of Healthcare Information Standards*. (Retrieved March 07, 2006 from http://im.med.up.pt/standards/cache/overview.htm.)

Blount, D. (2004). *A Study of Mobile Ad-Hoc Network Architectures and Technologies*. National University of Ireland. (Retrieved July 18, 2006 from http://www.cs.ucc.ie:8080/mccg/common/publications/db5MScSDN2004.pdf)

Borkin, S. (2003). *The HIPAA Final Security Standards and ISO/IEC 17799. SANS Institute 2003*. (Retrieved March 10, 2006 from http://www .sans.org/rr/whitepapers /standards/1193.php).

Boertien, N., & Middelkoop, E. (2002). *Authentication in mobile applications*. (Retrieved September 10, 2006 from https://doc.telin.nl/dscgi/ds.py/Get/ File-23314/VH_authenticatie.pdf)

Budde, P. (2002). *Wireless Technology - Cellular Mobile Networks*. Verizon Learning Centre. (Retrieved April 15, 2006, from http://www22.verizon.com /about/community/learningcenter/articles/displayarticle1/0,1727,1155z1,00 .html)

Bradley, M. (2005). *Infrared*. (Retrieved July 13, 2006 from http://

compnetworking.about.com/od/homenetworking/g/bldef_infrared.htm)

Broder, C. (2006). *Group to push mobile access to health info*. Healthcare IT News, January 2006. (Retrieved April 24, 2006, from http://www. healthcareitnews. com/story.cms?id=4554

Bogdon, C. & Ferguson, M. (2004). Seamless *Mobility. Approaching simple, continuous connectivity*. Wireless Business and Technology. (Retrieved, March 2, 2006 from http://wireless.sys-con.com/read/46646.htm)

Borzo, J. (2005). *A New Physician's Assistant: Handheld devices are becoming critical tools for some doctors and nurses*. The Wall Street Journal, the Journal Report: Personal Health. pp. R5. (Retrieved June 3, from http:// www. patientkeeper.com/wallstreet_10_10_05.html)

British Standard Institute. "BSI" (2006). *Information and Records Management. Information and Communication Technology*. (Retrieved July 10, 2006 from http://www.bsi-global.com/News/Information/index.xalter)

British Journal of Healthcare Computing. (1994). *Nurse Jailed for Hacking into Computerized Prescription System*. British Journal of Healthcare Computing and Information Management 1(94)

Brenner, B. (2006). *Survey exposes lax mobile security*. (Retrieved July16, 2006 from http://searchsecurity.techtarget.com/originalContent/0,289142, sid14_ gci11 78468,00.html)

Brown, E. G., Holmes, B. J., & McEnroe, W. (2006). *Hospital; IT Spending Trends For 2006*.Forrester Research (Retrieved July 20, from http:// www.forrester. com/Research/Document/Excerpt/0,7211, 39174,00. html)

BT Limited. (2004). *Creating a European Identity Management Architecture for eGovernment*. Guide Consortium. (Retrieved November 5, 2006 from: http://istrg.som.surrey.ac.uk/projects/guide/files/documents/D2.1.1.A.pdf)

Burrell, J. (2002). *Wireless Local Area Networking (WLAN) Security Assessment and Countermeasures. IEEE 802.11 Wireless Networks*. (Masters Dissertation, 2002 George Mason University) (Retrieved July 10, 2006 from telecom.gmu.edu/ publications/Jim-Burrell-December-2002.pdf)

Calder, A. (2006). *Information Security based on ISO 27001 and ISO 17799*. A Management Guide (1st ed.) Lk Zaltbommel: Van Heran [ISBN 90 77212 70 1] (Retrieved November 11, from http://www.itfocus.pl/Information ,Security,351.html)

Calif, H. (2002). *Global Physician Survey Reports Mobile Devices Help Doctors Provide Better Patient Care. Survey reports PDAs enhance patient care* (Retrieved July 30, from http://www.rnpalm.com/avantgo_survey.htm)

Canadian Institute of health Research. (2001). *Selected International Legal Norms on the Protection of Personal Information in Health Research*. (Retrieved October 20, from http://www.cihr-irsc.gc.ca/e/documents/

protection_pi_e.pdf)

Caldwell, D., & Koch, J. L. (1998). *Mobile Computing and its Impact on The Changing Nature of Work and Organization*. Leavey School of Business and Administration. (Retrieved April 29, 2006 from sts.scu.edu/research/Mobile Computing.pdf)

Cardelli, L. (1999). *Abstractions for Mobile Computation*. Microsoft Research. 3-9 (Retrieved March 13, 2006 from http://research.microsoft.com/Users/ luca/ Papers/Abstractions%20for%20Mobile%20Computation.A4.pdf

Cassidy, T. (2005). *PDAs Clarify Dictation. Advance for Health Information Professionals*. Advance News magazine, 15(17), 32.

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., & Mickunas, M.D. (2002). *Towards Security and Privacy for Pervasive Computing.* University of Illinois. (Retrieved April, 2006 from www.cyberdudez.com/towards-percomp-security.pdf)

Chernicoff, D. (2001). *Data Synchronization for the Mobile Worker* (Retrieved June 2006, from http://www.windowsitpro.com/Articles/ index.cfm? ArticleID=23590)

Cisco Systems. (2006). *Cisco Wireless Security* (Retrieved May 21, 2006 from http://searchnetworking.techtarget.com/searchNetworking/Downloads/chapter08.pdf

Cisco Systems. (2006a). Demystifying 802.11 (Retrieved May 30, 2006 from http://www. informit.com/articles/article.asp?p=653377&seqNum=7&rl=1)

Cisco Systems. (2005). *Cisco Enterprise Distributed Wireless Solutions*. Reference Network Design. (Retrieved November 3, 20006 from http://www.cisco.com /application /pdf/ en/us/guest/netsol/ns178/c649/ ccmigration_09186a00 800d67eb.pdf)

Cisco Systems. (2004). *Dictionary Attack on Cisco LEAP Vulnerability.Wireless LANs. (Retrieved June 20,2006 from http://www.cisco.com/en/US/tech/ tk722 /tk809/technologies_ security_notice09186a00801aa80f.html*

Ciampa, M. (2005). *Security+ Guide to Network Security Fundamentals* (2nd ed.) Canada. Thomson Learning Inc. [ISBN 0619215666]

Centers for Medicare & Medicaid Services "CMMS". (1996). *The Health Insurance Portability and Accountability Act of 1996* (HIPAA) (Retrieved September 4, 2006 from: http://www.cms.hhs.gov/hipaa).

Centers for Medicare & Medicaid Services "CMMS".(2005). *Security Standards: Organizational, Policies and Procedures and Documentation Requirements*. HIPAA Secuirty series. (Retrieved September 6, 2006 from http://www.cms. hhs.gov/ EducationMaterials/Downloads/SecurityStandardsOrganizational Policies.pdf

Crounse, B. (2006). *Mobile devices usher in new era in healthcare delivery. House calls for health Professionals*. (Retrieved May 23, 2006 from http://www. microsoft.com/industry/healthcare/providers/businessvalue/ housecalls/housecalls_mobility.mspx)

Crumbley, J. (2003). *Trust Us* Access Control and Security systems, Government Security. (Retrieved March 10, 2006 from http:// security solutions.com/ mag/ security_trust_us/index.html)

Chao, C. C., Jen, W. J., Li, Y., Chi, Y.P., Chen, C., & Feng, C.C. (2005). *Using Mobile Technology to Improve Healthcare Service Quality. Student Health Technology Information*. NCBI. (Retrieved April 19, 2006 from http:// www.ncbi. nlm.nih.gov/entrez/query. fcgi?cmd=Retrieve&db= PubMed &list_uids=16160283&dopt =Abstract)

Chapman, B., & Zwicky. (1995). *Building Internet Firewalls*. (1st ed.) [1-56592-124-0] (Retrieved August, 30, 2006 from www.unix.org.ua/orelly/ networking/ firewall/index.htm - 8k)

Coleman Foundation. (2005). *Workplace sabotage: why good employees go bad.*Business and Economic. Western Oregon University (Retrieved July 10, 2006 from http://www.wou.edu/las/business/pdf%20of%202006% 20 newsletter.pdf).

Coiera, E. (1997). *Guide to Medical Informatics the Internet and Telemedicine*. Chapman and Hall Medical, London, p.224

Cotton, D.B. (2005). *Software Defined Radio Isn't Just About Software*. (Retrieved July 28, from: http://www.cotsjournalonline.com/home/article. php?id= 100246&pg=1)

Computer-based Patient Records Institute (CPRI) Toolkit, (1995). *Managing Information Security in Heath Care*. (Retrieved March 10, 2006 from http://www.himss.org/CPRIToolkit/html/3.6.html)

Council Medical Schemes "CMS" (2002). *Draft Recommendations of the Committee on Standardization of Data and billing Practices*. Research and Monitoring.

Creswell, J. W. (1994). *Research design: Qualitative and quantitative approaches*. Thousand Oaks, CA: Sage.

Darwin, C. (2000). *Mobile Information Technology at the Point-Of-Care*: The grass root origin of mobile computing in nursing. (Retrieved March 12, 2006 from http://www.rnpalm.com/mitatpoc.htm)

Data Protection Act.(1998). *The* Data Protection Principles (Retrieved July 20, 2006 from http://www.opsi.gov.uk/acts/acts1998/80029--l.htm)

Dedo, D. (2004). *The Return on Your Mobility Investment: Enterprise opportunities for Windows Powered Pocket PCs and Smartphones*. Microsoft Corporation. (Retrieved March 24, 2006 from http://www.colltech.com/

docs/Return_on_Your_Mobility_Investment.pdf)

Dedo, D. (2004b). *Windows Mobile-Based Devices and security Protecting Sensitive Business Information*. Microsoft Corporation. (Retrieved March 24, 2006, from: www.microsoft.com/windowsmobile/business/ strategy/ security.mspx - 8k -)

Dierks, T., & Allen C. (1999). *The TLS Protocol. RFC 2246*. IETF. (Retrieved August 15, 2006 from http://www.ietf.org/rfc/rfc2246.txt)

Treek D. (2003). *An integral framework for information systems security management*. Computers and Security. 22 (4), 337-360.

Drake, S., & Olofson, C. (2005). *Are you ready? Assessing Enterprise Readiness for Mobility*. IDC Report, Bitpipe IT information. (Retrieved April 15, 2006 from http://www.bitpipe.com/detail/RES/1085682174_387.html)

Department of Defense. (2005). *DOD, Wireless Security Frequently Asked Questions* (FAQs), Information assurance environment. (Retrieved July 15, 2006 from http://iase.disa.mil/wireless/wirelessfaq.html)

Dobson, J., Samarati, P., Jajodia, S., Thuraisingham, B. (1999). *Security and Privacy issues for the World Wide Web: Panel Discussion*. (Retrieved October 6, 2006 from http://mo.co.za/abstract/privpnl.htm)

Dupre la Tour, I., Bochmann, G., Chouinard, J. (2001). *A Secure Authentication Infrastructure For Mobile Communication Service Over The Internet*. (Retrieved August 30, 2006 from http://beethoven.site.uottawa. ca/dsrg /PublicDocuments/ Publications/Dupr01a.pdf)

Eastwood, G. (2006). Protect *and survive: simple rules for the workforce beyond the corporate firewall*. Mobile Computing Technology, Computer weekly (Retrieved June 17, 2006 from http://www. Computerweekly. com/Articles/ Article.aspx?liArticleID= 214983&PrinterFriendly=true

Educause. (2006). *Network and Host Security Implementation. Computer and Security Task Force*. (Retrieved July 14, 2006 from http://www.educause. edu/ NetworkandHostSecurityImplementation(Stage1)/1264

Edlund, A. (2005). *Bluetooth Wireless Technology – 2005 Update. Bluetooth Special Interest Group*. (Retrieved July 24, 2006 from http:// www .touchbriefings. com/pdf/1433/Edlund.pdf)

Eneida, A., M., Chen, E. S., Stetson P.D., Mcknight L. K., Lei, J., & Cimino, J. J. (2004). *Approach to Mobile Information and Communication for healthcare.* Elsevier Int. Journal of Informatics. 73, 631 – 638

Entrust. (2004). *Information Security Governance (ISG)*: An Essential Element of Corporate Governance. (Retrieved August 8, 2006 from, http://itresearch. forbes.com/detail/RES/1082396487 702.html).

Elbaz, L. (2002). *Using Public Key Cryptography in Mobile Phones*. (Retrieved

August 10, 2006 from http://www.discretix.com/white_paper_c3.pdf.)

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

El-Khatib K., Hadibi, N., & Bochmann G. V. (2003). *Support for Personal and Service Mobility in Ubiquitous Computing Environments*. (Retrieved April 4, 2006 from beethoven.site.uottawa.ca/dsrg/ PublicDocuments/Publications/ ElKh03a.pdf)

Ericsson, S. (2006). *McAfee Firewall Mobile*. (Retrieved October 19, 2006 from: http://www.sonyericsson.com/downloads/14_McAfee_Firewall_short.pdf)

EthicSA, (2000). *Chris Hani Baragwanath Hospital Ethics Audit* (Retrieved June 4, 2006 from http://www.ethicsa.org/article.php?story= 2003091908 4251975

European Computer Manufacturing Association "ECMA" (2005). *Corporate Telecommunication Networks – Mobility for Enterprise Communications, Technical Report*. (Retrieved May 25 2006 from http://www.ecma international.org/ publications/techreports/E-TR-092.htm)

Farschi, J. (2003). *Wireless Intrusion Detection Systems* (Retrieved August 10, 2006 from http://www.securityfocus.com/infocus/1742#ref3)

Ferris, M. (2005). *Security in a Networked World. Red Hat Security Solutions*. (Retrieved July 18, 2006 from http://www.redhat.com/whitepapers/security /NetworkedWorld.pdf)

Fieedler, E. A. (2003). The Management System for ISO 17799: The Information Security Management System of BS 7799-2:2002.*(Retrieved May 20, 2006 from http://www.noweco.com/wp_ismse.htm*

Finch, C. (1999). *Mobile Computing in Healthcare*. View Point (Retrieved March 3, 2006, from www.healthmgttech.com/archives/view0499.html - 11k -)

Fleming, R. (2005). *Information Security 101: An Introduction to the Security Essentials*. Digital Defense, Inc. (Retrieved July 6, 2006 from http://www. digitaldefense.net/pdfs/InfoSec.pdf)

Fleischman, E. (2002). *Code Signing.*The Internet protocol Journal, 5(1) (Retrieved July 24, 2006 from http://www.cisco.com/web/about/ac123/ ac147/archived_issues/ipj_5-1/code_signing.html

Fleishman, G. (2003). *Ultrawideband renews high-speed wireless hopes*. InforWorld. (Retrieved July 20, 2006 from http://www.infoworld.com /article/ 03/08/08/31NNwireless_1.html)

Fontelo, P.A., & Chismas, W.G. (2005). *PDAs, handheld devices and wireless healthcare environments: minitrack introduction*. Proceedings of the 38th Hawaii International Conference on System Sciences.

Forman, G. H., & Zahorjan, J. (1994). *The Challenges of Mobile Computing*. IEEE Computer Society, 27(4), 38-47.

Fuggetta, A., Picco, G.P., & Vigna, G. (1998). *Understanding code mobility. Software Engineering*. IEEE Transactions 24(5), 342 – 361

Friedlander, D. (2004). *Managing and Securing Mobile Devices. Analyst Report*, Forester Research, 2004. (Retrieved July 12, 2006 from http://www. csoonline. com/ analyst/report2794.html)

Funk, J. L. (2003). *Mobile Disruption: The Technologies and Applications Driving the Mobile Internet*. (pp.1 -8) Canada, Hoboken New Jersey, John Wiley & sons Inc. [ISBN:0471511226]

Ganz A., Istepanian S. H., & Tonguz, O.K. (2006). *Advanced Mobile Technologies for Health Care Applications*. Journal of Mobile Multimedia, 1(4), 271-272.

Geier, J. (2001). *Swedish ambulance becomes a true mobile platform. Saving lives with roving LANs*. Network World. (Retrieved march 27, 2006 from http://www. networkworld.com/reviews/2001/0205bgside.html)

General Medical Council. (2002). *The Role and Responsibilities of Doctors .Confidentiality – guidance from the General Medical Council London*. (Retrieved August 3, 2006 http://www.gmc-uk.org/guidance /library/research .asp# confidentiality)

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

Gerken, M. (1997). *Statistical-Based Intrusion Detection*. (Retrieved May 3, 2006 from http://www.sei.cmu.edu/str/descriptions/sbid.html)

Giddens, A. (1978). Durkheim. Glasgow: Collins

Glenn, R., & Kent, S. (1998). *The Null Encryption Algorithm and Its Use With IPsec*. NIST 2410 RFC (Retrieved September 4, 2006 from http://www.rfc-archive.org/getrfc.php?rfc=2410)

Groenewald, T. (2004). *A phenomenological research design illustrated*. International Journal of Qualitative Methods, 3(1), 4. Retrieved November 15, from http://www.ualberta.ca/~iiqm/backissues/3_1/html/ groenewald .html

Grove, T. (2003). *Summary Analysis: The Final HIPAA Security Rule. HIPAAdvisory Phoenix Health Systems*. (Retrieved March 24, 2006 from http://www.hipaadvisory.com/REGS/finalsecurity/summaryanalysis.htm

Grote, M. (2003). *Using the ActiveSync Mobile Administration Web Tool*. Windows Security Threats Tips. (Retrieved March 24, 2006 from: http://www.it-training-grote.de/download/searchexchange-mobadmin.pdf)

Grimes, R. A. (2001). *Malicious Mobile Code (book).* Virus Protection for Window (Retrieved April 26, 2006 from http://www.oreilly.com/catalog/ malmobcode/ chapter/ch11.html)

Goede, R. (2003*). A framework for the explicit use of specific systems thinking methodologies in data-driven decision support system development*. (Doctoral Dissertation, 2004 University of Pretoria). (Retrieved November 15, 2006 from upetd.up.ac.za/thesis/available/etd-05132005-080727 /unrestricted/00front.pdf)

Gold, J. (2005). *Managing mobility in the enterprise*. Bitpipe Resource. (Retrieved April 15, 2006 from http://wp.bitpipe.com/resource/org_ 937603713_268/9207_ managed_mobility_edp.pdf?site_cd=itci)

Good. (2005). Mobile *device Security. Securing the handheld, securing the Enterprise*. Good Technologies. (Retrieved July 19, 2006 from http://www.good. com/corp/uploadedFiles/Documentation/WhitePapers/ Mobile_Device_Security_WP.pdf)

Government Accountability Office "GAO". (2005). *Information Security, Federal Agencies Need to Improve Controls over Wireless Networks*. GAO-05-383. (Retrieved August 21, 2006 from http://www.gao.gov/new.items/ d05383.pdf)

Gough, N., & McCulloch, B. (2006). *The Role of Mobile Phone In Increasing Accessibility & Efficiency in Healthcare*. Vodafone Policy Paper series, 4. (Retrieved April 20, 2006 from http://www.vodafone.com/assets/ files/ en/vodafone _policy_paper_4_march06.pdf)

Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Richardson, R. (2005). *Computer Crime and Security Survey.* (Retrieved July 10, 2006 from http:// i.cmpnet.com/ gocsi/db_area/pdfs/fbi/FBI2005.pdf)

Gordon, G. (2002). *Dozens of threats beset your data*. Sunday Times, Business Surveys. (Retrieved August, 2006 from, http://www.suntimes.co.za/2002/ 05/12/ business/surveys/internet/survey10.asp)

Gorlenko, L., & Merrick, R. (2003). *No wires attached: Usability challenges in the connected mobile world*. IBM System Journal, 4, 640

Guidelines for the management of IT security "GMITS". (1998). *Part 2: Managing And Planning IT Security*, TR 13335-2, ISO/IEC, JTC, 1/SC 27.

Gul Y.A, Wan A.C.T., & Darzi (1999). *Use of Telemedicine in Undergraduate teaching of Surgery*. Journal Telemedcine and Telecare. .5 , 202 - 208

Hasan, Jähnert, J., Zander, S., & Stiller, B. (2001). *Authentication, Authorization, Accounting, and Charging for the Mobile Internet*. Computer Engineering and Network Laboratory TIK. (Retrieved March 5, 2006 from http://www.tik.ee.ethz.ch /~ mobydick/papers/MobSum01.pdf

Havenstein, H. (2005). *Health Care: Doctors and PDAs proved a good match, helping give The Industry an Early lead with Wireless*. Cerner Bridge Medical, Computerworld news. (Retrieved March 15, 2006 from http://www. bridgemedical.com/05_16_05.shtml)

Halliday, S., Badenhorst, K., & Von Solms, R. (1996). A *business approach to effective information technology risk analysis and management*. Information Management and Computer Security, 4(1), 19-31Vol.4 No.1 pp.19 – 31.

Harding, T. (2003). *Compressed Data for EDIINT*. IETF. (Retrieved March 15, 2006 from http://www3.ietf.org/proceedings/03mar/I-D/draft-ietf-ediint-compression-01.txt)

Hayes, I. S. (2001). *Upwardly Mobile: A Wireless Primer*. IT Sourcing. (Retrieved August 1, 2006 from http://www.softwaremag.com/L.cfm?Doc= 2001-08/WirelessPrimer)

Hau, S.S. (2001). *Moving to Mobile - five key strategies for managing handheld devices in healthcare settings - Technology Information. Health Management Technology*. (Retrieved, August 10, 2006 from http://findarticles.com/p/articles /mi_m0DUD/is_7_22/ai_76548959/pg_2)

Harris, S. (2005). *How do BS7799 & COBIT differ?* Ask The Security Expert: Questions & Answers. (Retrieved from November 5, 2006 http:// searchsecurity. techtarget.com/expert/KnowledgebaseAnswer/ 0,289625,sid14_gci1140601_tax301709,00.html)

Hassell, J. (2005). Four ways to lock down mobile devices. (Retrieved, August 10, 2006 http://searchwindowssecurity.techtarget. com/tip/1, 289483, sid45_gci1148372,00.html)

Herrera, T. (2006). Solutions *for Health Insurance Portability and Accountability Act (HIPAA) Compliance*. Juniper networks. (Retrieved July 25, 2006 from www.juniper.net/solutions/literature/white_papers/200162.pdf)

Henzell, B. & Watson, E. (2004). *Bluetooth- Security*. M/Cyclopedia of New Media. (Retrieved July 20, 2006 from http://wiki.media-culture.org.au/ index .php/Bluetooth-_Security#Security_Issues)

Herman, W. (2005). *Secure Mobility-Protected Privacy, Defeated Attacks*. Nortel (Retrieved June 15, 2006 from http://www.nortel.com/corporate/ pressroom/feature_article/2005b/04_11_05_secure_mobility.html

Hickey, A.R. (2005). *Loss, theft still No. 1 threat to mobile data*. Search Mobile Computing. (Retrieved July 12, 2006 from http://searchmobilecomputing. techtarget.com/originalContent/0,289142,sid40_gci1143983,00.html

HIPAA Administrative Simplification – Security Final Rule, (2003). *Center of Medical & Medicare Services* (Retrieved June 3, 2006 from http:// www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp.)

HIPAA Administrative Simplification – Privacy Final Rule, (2002). *Center of*

Medical & Medicare Services. (Retrieved June 3, 2006 from http:// www.cms.hhs. gov/hipaa/hipaa2/ regulations/privacy/default.asp.)

HIPAA Administrative Simplification – Transaction and Code Set Rule, (2000). *Center of Medical & Medicare Services*. (Retrieved July 30, 2006 http: //www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/default.asp.)

HIPAA Consortium. (n.d.). *Security*. (Retrieved October 28, 2006 from http:// www.hipaa-consortium.com/Page.html

HP. (2006). *Wireless and mobility - understanding wireless and mobility*. (Retrieved June 24, 2006 from http://www.hp.com/sbso/ wireless/ understanding_wireless.html

HP. (2003). *Executive Briefing: Wireless Network Security*: White Paper. HP T1428-90017. (Retrieved October 5, 2006 from http:// docs .hp.com/en/T1428-90017/index.html)

Hyrkäs, K., & Paunonen, M. (2000). *Patient satisfaction and research-related problems (part 2)*. Is triangulation the answer?. Journal of Nursing Management 8(4), 237-245.

Hoepfl, M.C. (1997). *Choosing qualitative research*: A primer for technology education researchers, Journal of Technology Education, 9(1), 47-63.

Hong, J. I., Boriello, G., Landay, J. A., McDonald, D.W, Schilit, B.N & Tygar, J. D., (2003). *Privacy and Security in the Location-enhanced World Wide Web*. University of California ,Washington. (Retrieved April 13, 2006 from http://guir berkeley.edu/pubs/ubicomp2003/privacyworkshop /papers/ ubicomp2003-privacy-placelab.pdf)

Humphreys, T. (2001). *On Route to a Certified Information Security Management System Environment.* (Retrieved July 12, 2006 from http:// www.itsc.org.sg/ synthesis/2001/itsc-synthesis2001-tedhumphreys-isms-cert.pdf)

Ichiro S. & Niranjan, S. (2002). *Physical Mobility and Logical Mobility in Ubiquitous Computing Environments*. International conference on mobile agents No6, Barcelona , ESPAGNE, (2535), 186-201

International Data Corporation “IDC” (2000). *Nov 2000: IDC projection*. US Telework Scene - stats and facts (Retrieved May 30, 2006 from http:// www.ivc. ca/studies/us.htm)

International Data Corporation “IDC”. (2004*). Mobile Usage Patterns 2004*: An IDC Mobile Advisory Council Survey. (Retrieved June 2006 from http:// www. marketresearch.com/product/display.asp?productid=1058356&g=1)

ISO/IEC 17799. (2005). *Information Technology - Security Techniques - Code of Practice for information security Management* (Edition 2). : SANS.

ISO/IEC TR13335-1. (1997). *Information technology-Guidelines for the*

Management of IT Security Part 1. Switzerland: Case postale 56, CH-1211 Geneve.

Istepanian, R. S. H., Philips, N., Wang, X. H., & Laxminarayn, S. (2004). *The Role of 4G and Emerging Mobile Systems for Future m-Health Systems*, International Congress on Medical and Care Compunetics,. 465-471.

Istepanian, R. S. H., & Lacal, J. (2003). *Emerging Mobile Communication Technologies for Health: Some Imperative notes on m-health*, 25th Annual Int. Conf. IEEE Eng. in Med. and Biol. (EMBS), September, Cancun, Mexico, 1414-1416

Jason, M.B. (2003). *An API for Location Aware Computing*.(Masters Dissertation 2003, Massachusetts Institute of Technology)(Retrieved July 1, 2006 from http://groups.csail.mit.edu/graphics/pubs/thesis_bellj.pdf) .

Johnson, D. (2005). *Best Practices in Information Assurance and Information Technology Networking in Organizations that have two Departments*. Research Report. Bowie State University USA. (Retrieved July 14, 2006 from http://faculty.ed.umuc.edu/~meinkej/inss690/johnson.pdf)

Juha, T. V. (2000). ?Bluetooth Security?, Helsinki University of Technology (Retrieved July 18, 2006 from www.niksula.hut.fi/~jiitv/bluesec.html - 40k)

Kaaranen, H. (2005). *Evolution from GSM Multi Access*. UMTS Networks. (pp.15 – 24) England: West Sussex, Chichester, Southern Gate. John Wiley and Sons ltd. [ISBN:0470011033]

Kapil, S., Emily, Qi H. & Gupta V.G. (2006). *Seamless Platform Mobility Across Wireless Networks*. Technology@Intel Magazine. (Retrieved May 5, 2006 from, http://www.intel.com/technology/magazine/communications/mobility-on-wireless-0905.htm

Karanam, S. (2006). *Secure authentication with the new IEEE 802.1x standard*. Understand the IEEE standard's role in wireless security. (Retrieved October 4, 2006 from www.ibm.com/developerworks/library/wi-8021x/index.html - 53k -)

Kahane, O., & Petrack, S. (1997). *Call Management Agent System: Requirements, Function, Architecture and Protocol*. IMTC Voice over IP Forum Submission VOIP97-010,

Kakihara, M. & Sorensen, C. (2006). *Practising mobile professional work: Tales of locational, operational, and interactional mobility*. Emerald 6(3), 180-187.

Karnik, N.M. & Tripathi, A.R. (1998). *Design issues in mobile agent programming systems*. IEEE Parallel & Distributed Technology 6(3), 52 – 61

Kalakota, R. (2004). *Mobile enterprise applications:Deploying second-generation solutions. Intel Corporation*. (Retrieved May, 2006 from www.sap.com /company/ events/pdf/BWP_EB_Intel-SAP_Mobile.pdf.)

Karygiannis, T. & Owens, L. (2002). *Wireless Network Security 802.11, Bluetooth and Handheld Devices*. NIST. Pub. 800-48 (Retrieved March, 4 2006, from, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_ SP_800-48.pdf)

Karty, S. (2000). *Bluetooth Personal Area Network Technology. Technology and Programs Division,* 7(3) (Retrieved July 9, 2006 from http://www.ncs.gov/ library/tech_notes/tn_vol7n3.pdf)

Kay, R. (2006). *Why Low-Power Radios can have Huge Throughput*. Ultrawideband – the basics, TechWorld. (Retrieved July 21, 2006 from http://www.techworld.com/mobility/features/index.cfm?featureID=2421)

Kay, R. (2005). *QuickStudy: Biometric authentication*. Computerworld. (Retrieved October 12, 2006 from http://www.computerworld.com/ securitytopics /security/ story/0,10801,100772,00.html)

Keay, B. (2004). Microsoft in *Healthcare: Interview with Bill Keay of Microsoft's Healthcare group*. Smart and Pocket PC Magazine. (Retrieved May 20, 2006 from, http://www.pocketpcmag.com/_archives/ may04/MSin Healthcare. aspx

Kerr, K. (2004). *The Electronic Health Record in New Zealand - Part 2*. Creating Quality in Primary Health Care Using Electronic Health Records Journal: Healthcare and Informatics review Online. (Retrieved from http:// hcro.enigma. co.nz/website/index.cfm?fuseaction=articledisplay& FeatureID=040305)

KPMG, (2001). *A new covenant with stakeholders: Managing privacy as a Competitive Advantage*. KPMG's Assurance & Advisory Services Center.

Krausea, A., Hartlb, D., Theisc, F, Stangld, M., Gerauerd, K.E., & Mehlhorne A.T. (2004). *Mobile decision support for transplantation patient data*. International Journal of Medical Informatics, 73(5), 461- 464.

Kyriacou, E., Pavlopoulos, S., Berler, A., Neophytou, M., Bourka, A., Georgoulas, A., et al. (2003). *Multi-purpose HealthCare Telemedicine Systems with mobile communication link support*. Biomedical Engineering Online, 2(7).

Kumar, R. (2006). *Security in Wireless Networks* (Retrieved July, 15, 2006 from http://netlab.cs.iitm.ernet.in/cs650/2006/TermPapers/rajeevkumar.pdf)

1 Kurtz, N. (2004). *Securing A Mobile Telecommunications Network From Internal Fraud.* Wireless Security (Retrieved June 10, 2006 from http://www. securitydocs .com/ library/308

Lamparter, B., & Westhoff, D. (2002). *Security Challenges in the future mobile Internet*. NEC Network Laboratories, Workshop on Requirements for Mobile Privacy & Security PAMPAS'02. (Retrieved May 26, 2006 from http://www. pampas. eu.org/Position_Papers/NEC.pdf)

Langheinrich, M. (2001). *Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems*. ACM UbiComp 2001, Atlanta, GA. (Retrieved February 16, 2006 from www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf)

Lampsas, P., Vidalis, I., Papanikolaou, C., & Vagelatos, A. (2002). Implementation *and Integration of Regional Health Care Data Networks in the Hellenic National Health Service*. J Med Internet Res.4(3),e20

Laurie, A.,& Laurie, B. (2003). *Bluetooth*. The bunker. (Retrieved, July 4, 2006 from http://www.thebunker.net/resources/bluetooth)

Laxminarayan, S., & Istepanian, R.S. (2000). *Unwired E-Med: the next generation of wireless and internet telemedicine systems*. IEEE Transaction Information Technology Biomedical 2000. 3, 189-93.

Layton, J., & Franklin, C. (2006). *How Bluetooth Works: Bluetooth Security*. (Retrieved July 17, 2006 from http://wiki.media-culture.org.au/index.php /Bluetooth-_Security#Security_Issues)

Lee, M. (2003). *Wireless technology: Considering benefits and risks*. (Retrieved July 9, 2006 from http://searchmobilecomputing.techtarget.com /searchMobile Computing/downloads/BTWiFiiWhitePaper.pdf)

Lee, A.S. (1999). *Rethinking management information systems*. Researching MIS. Currie, W.L. & Galliers, R., eds. Oxford: Oxford University Press. p.7-27.

Leggio, S., Manner, J., & Raatikainen, K. (2005). Achieving *Seamless Mobility in IPBased Radio Access Networks*. IEEE Wireless Communications, 12(1), 54-59

Lehrbaum, R. (2000). *Advanced information on a Korean combo cell phone + PDA*. Articles & white papers about Linux based embedded applications. (Retrieved May 24, 2006, from http://www.linuxdevices. com/articles/ AT3334 419107.html)

Linhoff, M. (2002). *Mobile computing in medical and healthcare industry*. Retrieved 13th March, 2006, (Retrieved June 3, 2006 from http://www. mocomed.org/workshop2002/beitraege/Linhoff.pdf)

Lindstrom, P. (2001). Special Report: The Language Of XML Security.*Network Magazine* June 2001, 56-60

Lindow, M. (2004). *How SMS Could Save Your Life*, (Retrieved march 13, 2006 from http://www.wired.com/news/medtech/0,1286,65585,00.html)

Light, J. (2004). *Security, privacy and trust issues raised by the Personal Server Concept*. Intel Research, SPCC Workshop on Security and Privacy in Pervasive Computing. (Retrieved 13, 2006 from http://www. vs.inf.ethz.ch /events/sppc04/ papers /sppc04_light.pdf)

Liu, Y., & Hart, D. (2003). *A Software Monitoring Tool for Data Management on Mobile Devices*. In Proceeding Parallel and Distributed Computing and Systems - 2003, 392-196

Long, M. (2005). *The Mobile Data Poison Pill*. (Retrieved May 4, 2006 from http://www.newsfactor.com/story.xhtml?story_id=010000008CPA)

Luo, J. (2004). *Portable Computing in Psychiatry*. The Canadian Journal of Psychiatry. 49, 24–30

Luukkainen, S. (2003). *Emerging Technologies in Mobile and Wireless Data Network Evolution*. Telecommunications Software and Multimedia Laboratory. Helsinki University of Technology Finland. (Retrieved July 20, 2006 from, http://www.tml.tkk.fi/Studies/T-109.551/2003/Proceedings.pdf)

Maltoni, D., & Jain, A.K (2004). *Biometric Authentication*. (Retrieved June 10, 2006 from http://bias.csr.unibo.it/bioaw2004/)

MacDonald, D. (2003). *A Clinical Reference for Mobile Physicians*. Mobile Imperative.1. (Retrieved May 24, 2006 from http://www.mobileimperative .com/ documents.asp?grID=307&d_ID=1770)

McAfee, (2006). (Retrieved May 24, 2006 from http://www.mcafee.com/us/ enterprise/products/mobile_security/index.html

McCullagh, A., & Caelli, W. (2000). *Non-Repudiation in the Digital Environment*. First Monday peer reviewed journal on the internet (Retrieved October 20, 2006 from http://www.firstmonday.org/issues/issue5_8/mccullagh/)

Meridian healthcare. (2006). The *Practical Application of Handheld and Mobile Computing in Healthcare*. (Retrieved May 1, 2006 from http://www.meridianhc. co.za/article.php?sid=28)

Meyer, S. (2001). *What is means for Privacy and Security*. (Retrieved April 4, 2006 from http://www.giac.org/certified_professionals/ practicals/gsec/ 0609.php)

Microsoft. (2003). *Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard*. Microsoft Security Bulletin MS01-017. (Retrieved May 20, 2006 from:http://www.microsoft.com/technet/security/Bulletin/MS01-017.mspx)

Microsoft. (2004)*. Patch Management Process*. (Retrieved July 15, 2006 from http://www.microsoft.com/technet/security/topics/patchmanagement/secmod193.mspx)

Microsft. (2005). *Service Management Functions. Security Administration*. (Retrieved June 10, 2006 from http://www.microsoft.com/technet/ itsolutions /cits/mo/smf/smfsecad.mspx)

Mitchell, B. (2006). *SSID - Service Set Identifier, Wireless/Networking*. (Retrieved from http://compnetworking.about.com/cs/wireless/g/ bldef_ssid.htm)

Mingqiang, X., Komiya, D., Kawaguchi, S., Rahman, M., Kumar, B., & Shim ,E. (2005). *Extensions of Session Description Protocol (SDP) for Seamless Session Mobility.* (Retrieved March 14, 2006 from http://tools.ietf.org/tools /rfcmarkup/ rfcmarkup.cgi?draft=draft-mingqiang-mmusic-session-mobility-attribute-01.txt

Miettinen, M., & Halonen, P. (2006). *Host-Based Intrusion Detection for Advanced Mobile Devices*. IEEE, 2, 72- 76

Moskop, J.C., Marco, C. A., Larkin, G.L., Geiderman, J.M., & Derse, R. (2005). *From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine Part I: Conceptual, Moral, and Legal Foundations*.58 Annals of Emergency Medicine, 45(1)

Molloy, K. (2003). *Seamless Handoff between 802.11b and CDMA2000 Networks*. University of Canterbury, New Zealand. (Retrieved July 23, 2006 from www. medialab.co.nz/assets/downloads/Seamless%20 Handoff% 20Between%20802.11b%20and%20CDMA2000%20Networks.pdf)–

Moody, D. (2002). *Empirical Research Methods*. (Retrieved November 20, 2006 from.http://www.idi.ntnu.no/~ekaterip/dif8916/Empirical%20Research%20 Methods%20Outline.pdf)

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. (Retrieved June 13, 2006 from http://books.nap.edu/ catalog/5595.html)

National Institute for Standards and technology "NIST". (1997). *Special Pub 800-12 An Introduction to Computer Security*: The NIST Handbook. (Retrieved May 4, 2006 from http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf)

National Institute for Standards and technology "NIST". (n.d.). Digital *Signature Standard*. (Retrieved from http://csrc.nist.gov/publications/nistbul/csl94-11.txt)

Newcombe, T. (2003). Mobile Health. Mobile Government. (Retrieved April 9, 2006 from http://www.govtech.net/magazine/sup_story.php?id= 6865 &magid= 17&issue=1:2003)

New Zealand Federation Of Voluntary Welfare Organisations. (n.d.). (Retrieved March 16, 2006, from www.nzfvwo.org.nz)

News8austin. (2005). *Pitonyak headed to Austin for booking*. News 8. (Retrieved November 3, 2006 from http://www.news8austin.com/content/ top_stories/ default.asp?ArID=143961

Nealon, J., Moreno, A. (2002). The Application of Agent Technology to Healthcare. Proceedings of the Workshop "AgentCities: research in large scale open agent environments", in the 1 International Joint Conference on

Autonomous Agents and Multi-Agent Systems (AAMAS 2002), 169-173.

Nelson, R. (2002). *The Right Choice for TDMA Carriers GSM/GPRS/EDGE/ UMTS*. AT&T Wireless. (Retrieved July 9, 2006 from http://www.gsm world.com /news/media_2002/rightchoice.shtml)

Neethling, J., & Potgieter, J. (1996). *Neethling's Law of Personality*. Recognition of the Right to Privacy. (Retrieved May 3 2006 from wwwserver. law.wits. ac.za/salc/ issue/ip24-03.pdf)

Nikander, .P., Ylitalo, .J., & Wall .J (2003). *Integrating Security, Mobility, and Multi-homing in a HIP Way*. (Retrieved March 5, 2006 from http://www.isoc. org/isoc/conferences/ndss/03/proceedings/papers/6.pdf

Nixon, P. A., Wagealla, W., English, C., & Terzis, S. (2004). *Security, Privacy and Trust Issues in Smart Environments*. The Global and Pervasive Computing Group. (Retrieved May 12, 2006 from smartlab.cis. strath.ac.uk/Publications/techreports/ SPTPaperFinal.pdf) -

Niemi, V., & Kaaranen, H. (2005). *Security in the UMTS Environment*. UMTS Networks (pp.253- 271) England: West Sussex, Chichester, Southern Gate. John Wiley and Sons ltd. [ISBN:0470011033]

Niem, T.C. (2002). Bluetooth and Its Inherent Security Issues. (Retrieved May 16, 2006 from http://www.sans.org/rr/whitepapers/wireless/945.php)

Nicolett, M. (2003). *Managing IT Security Risk in a Dangerous* World. Gartner research. (Retrieved June 10, 2006 from http://www.csoonline.com /analyst/report 1332.html)

Nokia. (2006). The Route to True Competitive Advantage: Today's Evolution of Workforce Mobility. (Retrieved April 15, 2006 from http://www.nokia.com /NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/nokia_es_phase sofmobility.pdf)

Oates, B.J. (2006). Researching Information Systems and Computing. Thousand Oaks, CA: Sage.

Oasis. (2005). *Universal Description, Discovery, and Integration (UDDI).* Technology Reports. (Retrieved April 2006 from, http://www.oasis-open.org/ cover/uddi.html)

O'Brien, N. & McKinnon, N. (2006). *Bungle exposes bank files*. (Retrieved July 15, 2006 from http://australianit.news.com.au/articles/0,7204,19588463% 5E15 306%5E%5Enbv%5E,00.html)

OECD (n.d.). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Information Security and Privacy* (Retrieved November 5, 2006 from http://www.oecd.org/document/20/0,2340, en_2649_34255_ 15589524_1_1_1_1,00.html)

Ottaway, W. (2002). *Mobile Security: Cause for Concern?*. QuinetiQ

Whitepaper, TechRepublic. (Retrieved July 15, 2006 from http:// whitepapers.techrepublic.com. com/whitepaper.aspx?&docid=130237 &promo=100511)

Orlikowski, W., & Baroudi, J. (1991). *Studying information technology in Organizations*: Research approaches and assumptions. Information Systems Research. 2(1), 1–28.

Ou, G. (2005). *Understanding the updated WPA and WPA2 standards*. Security, Mobile/Wireless. (Retrieved November 10, from http://blogs.zdnet.Com /Ou/?p=67)

Parker, D. (2005). *Authentication, Access Control & Encryption:Remote Authentication: Different Types and Uses*. (Retrieved October 20, from: http://www.windowsecurity.com/articles/Remote-Authentication-Different-Types-Uses.html)

Pereira, P. (2002). *Alternatives to WEP security*. (Retrieved November 10, 2006 from http://www.networkmagazineindia.com /200206/inperson.shtml

Peterman, S. (2003). *Security in Pervasive Computing.* Colorado State University Fort Collins. (Retrieved August 10, 2006 from http://www. infosecnews.com /opinion/2003/03/05_04)

Pfleeger, S.L., & Pleeger, C.P. (2003). *Security in Networks*. (Retrieved March 29, from http://www.informit.com/articles/article.asp?p=31339&seq Num=7&rl=1)

Phifer, L. (2006). *Choosing the right flavor of 802.1X. Wireless Security* Lunchtime Learning. (Retrieved September 10, 2006 from http://search netrworking. techtarget.com/generic/0,295582,sid7_gci1174046,00. html#TLS)

Portale, O. (2002). *Healthcare: the mobile opportunity*. Mobile Enterprise, Sun Microsystems. (Retrieved March 17, 2006 from http://www. sun.com/ mobility/ enterprise/feature_story.html)

Pullela, S. (2002). *Security Issues in Mobile Computing*. University of Texas Arlington. (Retrieved September 3, 2006 from http://crystal.uta.edu/ ~kumar/cse6392/termpapers/Srikanth_paper.pdf)

Radack, S. (2003). *Security for Wireless Networks and Devices*. Information Technology Laboratory. NIST. (Retrieved July 24, 2006 from http://www .itl.nist.gov/lab/bulletns/bltnmar03.htm)

Ranger, S. (2005). *Mobile virus epidemic heading this way*. (Retrieved July 25, 2006 from.http://www.vnunet.com/vnunet/news/2126724/mobile-virus-epidemic-heading-way)

Ramanatha, S. (2006). *IT Security Vs Information Security*. (Retrieved July 14, 2006 from http://cio.ittoolbox.com/groups/strategy-planning/info-security-management-sp/it-security-vs-information-security908920#

https://www.atis.org/ docstore/default.aspx)

Ravindran, P. (2005). *IT professionals callous about mobile security*: Survey. Business Line. The HINDU group. (Retrieved July, 16, 2006 from http:// www. blonnet.com/2005/11/24/stories/2005112402630400.htm)

Rasmussen, M. (2005). *Revised ISO 17799 Boosts Information Security Management Relevance*. (Retrieved October 4, 2006 from http:// www.csoonline. com/analyst/report3730.html.)

Result. (2005). *State of Kansas Interim Wireless Local Area Networks Security andTechnical Architecture*. (Retrieved July 24, 2006 www.da.ks.gov/ itec/ Documents/IntrmWrlsSecArch.doc)

Remin, D. G., & Osten, M. (2001). *Information as an Organizational Asset. Creating a culture that values data*. (Retrieved July 10, 2006 from, http://www.techsoup.org/learningcenter/techplan/page2740.cfm)

Research in Motion "RIM" (2005). Making *the Business Case for a Wireless Solution.* Research in Motion Limited. (Retrieved February 5, 2006 from www.blackberry.com)

Rindfleisch, T.C. (1997). *Privacy Information Technology and Healtcare*. ACM Press. 40(8), 92 – 100.

Richardson, R. (2003). *CSI/FBI Computer Crime and Security Survey.* (Retrieved July 29,2006 from http://www.gocsi.com/)

Ritchie, B., & Brindley, C. (2001). *The information-risk conundrum*. Marketing Intelligence and Planning, 19(1), 29–37(9).

Robillard, L. (2001). *Integrated Risk Management Framework*. Treasury Board of Canada. (Retrieved July 10, from http://www.tbssct.gc.ca/pubs_pol/ dcgpubs/ riskmanagement/rmf-cgr01-1_e.asp).

Robinson, P. (2001). *Understanding Digital Certificates and Secure Sockets Layer (SSL)* (Retrieved July 10, 2006 from http://www.entrust.com/ resources/n pdf/understanding_ssl.pdf)

Ross, S. (2006). Seamless Mobility. Mobile Computing. Microsoft Research. (Retrieved April 12, 2006 from http://research.microsoft.com/displayArticle. aspx?id=429)

Sadlier, G. (2003). *Mobile Computing Security.* International Network Services. (Retrieved August 5, 2006 from http://www.ins.com/resources/ whitepapers/)

Saint-Germain, R. (2005).*Information Security Management Best Practice Based on ISO/IEC 17799.*The Information Management Journal. July/August, 2005, 60- 66.

Satyanarayanan, M. (1996). Fundamental challenges in mobile computing. *In Proceedings of the Fifteenth Annual ACM Symposium on Principles of Distributed Computing* (Philadelphia, Pennsylvania, United States, May 23 - 26, 1996). PODC '96. ACM Press, New York, NY, 1-7. DOI.

Sawyer, M. (2006). *Competitive Intelligence in the Healthcare Industry – Part One*. Direction magazine. (Retrieved February 28, 2006 from http://www. directionsmag.com/article.php?article_id=2087&trv=1)

Schneier, B. (2000). *Self-Study Course in Block Cipher Cryptanalysis*. Cryptologia, 24(1), 18-34. (Retrieved May 20, 2006 from http://www .schneier.com/paper-self-study.pdf

Schulzrinne, H. (1996). *Personal Mobility for Multimedia Services in the Internet*. In Proceedings of the European Workshop on interactive Distributed Multimedia Systems and Services (March 04 - 06, 1996). B. Butscher, E. Moeller, and H. Pusch, Eds. Lecture Notes In Computer Science, Vol. 1045, 143-161..

Seleznyov, A. (2001). *A Methodology to Detect Temporal Regularities in User Behavior for Anomaly Detection*. IFIP `2001, July 2002, Plymouth, UK, pp357-364.

Shaw, K. (2003). *NW500 survey: Mobile devices are a necessity*. Network world. (Retrieved May, 28 2006 from http://www.networkworld.com/ newsletters/ mobile/2003/0616mobile1.html?page=1)

Shaw, R. L. (2001). *Why use interpretative phenomenological analysis in Health Psychology?* Health Psychology Update, 10(4), 48-52.

Sheepers, H. (2003). *Emerging trends in mobile technology development*: from healthcare professional to system developer. International Journal of Healthcare Technology and Management. 5 (3/4/5), 179 - 193

Shevchenko, A. (2005). *An overview of mobile device security*. (Retrieved September 10, 2006 from http://www.viruslist.com/en/analysis?pubid= 170773606)

Shiaa, M.M., & Liljeback, L.E (2002). *User and Session Mobility in a Plugand-Play Network Architecture.* NTNU University, Trondheim – Norway (Retrieved 16 May 2006 from, http://tapas.item.ntnu.no/publications/ eunice2002.pdf)

Shinder, D. (2005). *Bluetooth: Is it a Security Threat*?. Wireless security. (Retrieved October 5, 2006 from http://www.windowsecurity.com/articles /Bluetooth SecurityThreat.html?printversion)

Schwartz, M. (2004). *Configuration Management Goes Mobile. New software fixes mobile computers that deviate from corporate standards*. (Retrieved August 12, 2006 from http://esj.com/security/article.aspx?EditorialsID= 947)

Sittampalam, S.R., & Atun, R.A (2006). *The Role of Mobile Phone In Increasing Accessibility & Efficiency in Healthcare*. Vodafone Policy Paper series, No.4. (Retrieved April 20, 2006 from http://www.vodafone.com/assets/files/en/ vodafone_ policy_paper_4_march06.pdf)

Simpson, M.T. (2005). *Hands-On Ethical hacking and Network Defense*. Canada: Thomson Learning Inc. [ISBN: 0619217081]

Siwicki, B. (2003). *Point-of-Care Computing Gets Boost from Mobile Technology*. Health Data Management. (Retrieved from May 6, 2006 http://www.keepmedia. com/pubs/HealthDataManagement/2003/12/01/ 543620?extID= 10037&oliID=229)

Slawsby, A. (2004). *Extending the Corporate Security Infrastructure to Mobile Devices*. IDC Opinion. (Retrieved July 10, 2006 from http://www. bluefiresecurity com/pdf/IDC%20Whitepaper.pdf)

Schroder, C. (2006). *Of Supplicants and Keys: The Lowdown on WiFi Security*. (Retrieved July 12, 2006 from http://www.wi-fiplanet.com /tutorials/article. php/ 3593046)

Sorensen, C. F., Naess, B, Strand, O.S., Inge, A., Wang A. I., & Conradi, R. (2003). *A Survey of Mobile Support Needs in the Home Nursing Care*. Norwegian University of Science and Technology (NTNU). (Retrieved March16, 2006 from www.idi.ntnu.no/grupper/su/publ/carlfrs/apami-survey-2003.pdf

SonicWALL. (2003). *WiFiSec vs. WPA*. (Retrieved July 13, 2006 from http:// www. sonicwall.com/support/pdfs/WiFiSec_vs_WPA.pdf)

South African National Health Act (SANHA) (2003). Vol.469. Government Gazette, Cape Town 23 July 2004.

South African Law Commission "SALC". (2003). *An Investigation of Privacy and Data Protection in South Africa.* (Retrieved from 26 June 2006 http://www server. law.wits.ac.za/salc/salc.html.)

Stanberry, B. (2001). *Legal ethical and risk issues in telemedicine*. Computer Methods and Programs in Biomedcine. (64)(3), 225 – 233

Strode, S.W., Gustke, S. & Allen, A (1999). *Technical and Clinical Progress in Telemedicine*. JAMA. 281(12),1066-1068

Symantec. (2006). *Security Concerns Threaten Enterprise Rollout of Mobile Technology*. (Retrieved July 10, 2006 from http://www.symantec.com/ region/in/press/2006/in_060405.html

Symantec. (2006a). *Symantec Internet Security Threat Report Trends for July 05–December 05 Vol. IX*. (Retrieved July, 11, 2006 from http://www4. symantec.com/Vrt/vrtcontroller)

Symantec. (2006b). *Enterprise Product Catalog*: (Retrieved August 10, from:

http://eval.veritas.com/mktginfo/enterprise/other_resources/ent-enterprise_ products_catalog_07_2006.en-us.pdf)

Symantec. (2005). *Securing the mobile frontier*. (Retrieved, August 7, 2006 from, http://enterprisesecurity.symantec.co.uk/pdf/ Security_Mobile_Frontier.pdf#search=%22Management%20commitment%20to%20mobile%20security%22)

Syme, M. & Goldie, P. (2004). *Understanding Application Layer Protocols: Secure Socket Layer* (Retrieved June 30, from http://www.informit.com /articles/article.asp?p=169578&seqNum=4&rl=1)

Stanford, V. (2002). *Pervasive Health Care Applications Face Tough Security Challenges*. IEEE Pervasive Computing, 1(2), 8-12.

Sun, J. & Sauvola, J. (2002a). *Mobility and mobility management: a conceptual framework*. Networks, 2002. ICON 2002. 10th IEEE International Conference pp. 205- 210 [ISBN: 0-7803-7533-5]

Sun, J. & Sauvola, J. (2002). *On fundamental concept of mobility for mobile communications.* Machine Vision & Media Process. 2, 799- 803

Sutherland, J. & Madrid. G. (2003). *Platform Extends Secure and Auditable Encryption Standards to Mobile Computing. PatientKeeper®* (Retrieve May 3, 2006 from http://www.patientkeeper.com/download/platform/ WP_Encryption _Standards_12_30_03.pdf

Swindom, G., (2004). *HIPAA Final Security Rule Information Security Reference Guide.* Sygate Technologies, Inc

Tachakra, S., Mullett, S.T.H.; Freij R., & Sivakumar, A. (1996). *Confidentiality and ethics in telemedicine*. Journal of Telemedicine and Telecare, (2), 68-71

Taylor, D. (2006). Mobile device management: Part 2 -- Implementation options. *Managing Mobile (Retrieved June 10, 2006 from http:// search mobile computing.techtarget.com/ tip/0,289483,sid40_gci1188268,00.html)*

Teger, S., & Waks, D. (2006). *Ultra Wideband Real Applications Coming Soon (Broadband Home)* (Retrieved May 6, 2006 from http://www.broadband home central.com/report/backissues/Report0604_4.html)

Tuyikeze, T., Pottas, D. (2005). Information Security Management and Regulatory Compliance in the South African Health Sector. *In Proceedings of the 5th Annual Information Security South Africa Conference* (pp. 3-12). 29-01 July 2005, Sandton, South Africa,.

Thornberry, K. (2005). *Handhelds serve healthcare providers across the industry. Managed Health Executive*. (Retrieved March 24, 2006. from http://www.managed healthcareexecutive.com/mhe /article/articleDetail. jsp?id=170612)

Trom, C.H. (2002). *The New World of Communication. Ericsson Publication*.

(Retrieved May 16, 2006. from http://www.ericsson.com/ericsson/corpinfo/publications/onmagazine/pdf/On_102.pdf)

Thayer, G. (2005). *Survey: email is greatest mobile security risk*. Mobile Village. (Retrieved July 24, 2006 from http://www.mobilevillage.com/news/2005. 11.18/good_poll.htm)

“The Times” 1993; February 25. 29. (1999) *Teenager hacked into cancer patient files,*

Thorne, S.(2000).*Data analysis in qualitative research*. EBN online. Evidence-Based Nursing. 3,68-70.

Tsai, Y., Chang, C. (2003). *SIM-based subscriber authentication for wireless local area network*. IEEE. 468- 473 [ISBN: 0-7803-7882-2]

Uday. O., & Pabrai, A. (2003). *Role-Based Access Control (RBAC)*. Certification Magazine. (Retrieved July 10, 2006 from http://www.certmag.com/articles/templates/cmag_department.asp?articleid=370&zoneid=63)

Vilcinskas, M. (2006). *Security Entities Building Block Architecture. Microsoft Solutions Framework*. Best Practices for Enterprise Security. (Retrieved July 6, 2006 from http://www.microsoft.com/technet/Security/bestprac/bpent/sec2/ secentbb.mspx)

Virusoffice. (2005). *Mobile viruses - Are our mobile phones at risk?.* (Retrieved August, 10, 2006 from http://www.virusoffice.com/news/index.cfm?fuseaction =shownewsdetails& NewsID=250)

Wales, J. (2003). *The Pocket PC's Prescription for Health Care.* Smart Phone & Pocket PC Magazine may 2003. (Retrieved April 3, 2006 from http://www.pocketpcmag.com/_archives/may03/e_prescription.asp)

Wang, G. (2005). *Securing Mobile Data. The Proliferation of Wireless Devices and Increased Remote Working means Data Protection is one of the Sectors Growth Drivers*. Mobile Security, iSIGHT, 2005. (Retrieved March 10, 2006 from http:// www.3i.com/us/pdfs/iSight6.pdf)

Walsh, S., Wan, J. & Sadlier, A. (2006). *Bluetooth Security 4BA2*. Technology Survey. (Retrieved July 25, 2006 from http://ntrg.cs.tcd.ie/undergrad/4ba2.05/ group15/index.html)

Weise, J. (2001). *Public Key Infrastructure Overview*. Sun Microsystem Inc. (Retrieved August 14, 2006 from http://www.sun.com/blueprints/0801/publickey.pdf)

Wiehler, G. (2004). *Mobility, Security and Webservices. Technologies and Service-oriented Architrectures for new era of IT Solutions*.Germany. Erlangen, Publicis Corporate Publishing. [ISBN38957822297]

Wipro. (2002). *Software-Defined Radio. Wipro Technologies*. (Retrieved July 4, 2006 from: http://www.wipro.com/pdf_files/sdr_wipro.pdf)

Wright, B. (2001). *Rural Doctors Advance Care with Wireless*. (Retrieved march 30, 2006 from http://news.hst.org.za/view.php3?id=20011026)

Whitman, M.E., & Mattord, H.J. (2003). *Principles of Information Security*. Canada. Course Technology, 25 Thomson Place, Boston, Massachusetts, 02210.[ISBN 0-619-06318-1].

Whittaker, J.(2003). *Why Secure Applications are Difficult to Write*. IEEE Security and Privacy, 1(2), 81-83.

Wu, J., Wang, S., & Lin, L. (2005). What Drives Mobile Health Care? An Empirical Evaluation of Technology Acceptance. IEEE Computer Society. (p. 150a). *Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05) - Track 6*.

Wyatt, A. (2005). *Mobile Workforce for Dummies*. (ed. 2, p13-16) Avaya. (Retrieved April 9, 2006 from www.nyherji.is/media/greinar/Mobile WorkforceForDummies.pdf)

Youngblood. G. (2002). *A Software-Defined Radio for the Masses, Part 1*.(Retrieved April 26, 2006 from http://www.arrl.org/tis/info/pdf/020708 qex013.pdf)

Zachariadis, S., & Mascolo, C. (2003). *Adaptable Mobile Applications through SATIN: Exploiting Logical Mobility in Mobile Computing Middleware*. University College London. (Retrieved July 12, 2006 from http://www.cs.ucl.ac.uk/staff/s. zachariadis/papers/ubinet03.pdf

Zeisz, R., Keil, M., & Lee, J. (2005). *Secure Wireless Networks for Distributed Remote Sites. Introducing the Juniper Networks NetScreen-5GT Wireless*. Juniper Networks, Inc. 200102-001. (Retrieved June 4, 2006 from http:// www.juniper.net/solutions/literature/white_papers/200102.pdf

Zhao, Y., Yagi, Y., Juzoji, H., & Nakajima, I. (2002). *A Study of Wireless IP for Telemedicine*. Nakajima Laboratory, Medical Research Institute. 259-1193

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)*, (pp. 153-162). Chantilly, VA, May 3-4, 2001.

Appendix A
Academic Paper

In addition to this dissertation, an academic paper entitled “MOBILE DEVICE USE IN HEALTHCARE: GUIDANCE FROM HIPAA AND ISO17799” has been prepared. In essence the paper discusses the comparative analysis presented in chapter 6 of the dissertation. The paper will be submitted to a suitable journal. The paper’s abstract is given below.

MOBILE DEVICE USE IN HEALTHCARE:
GUIDANCE FROM HIPAA AND ISO17799

Abstract

The proliferation of mobile computing already has provided many advantages to the healthcare industry. However, mobile technology is not without risk; instead, it poses new threats to the privacy and security of health information. It is therefore imperative that mobile devices are considered within the overall risk management strategy of an organization. As such, it must be ensured that controls implemented to mitigate the risk, comply to international best practices and meet the requirements of legal and regulatory bodies.

The paper, therefore, aims to provide a guideline for secure mobile computing in healthcare using ISO 17799:2005 and HIPAA for guidance. The paper shows the relationship between the standards, particularly how they meet or differ in strength and focus, specifically relating the requirements to mobile computing in a healthcare setting. The paper concludes that healthcare organizations will be far on their way to HIPAA compliance if the ISO 17799:2005 best practice controls are implemented. The paper also identifies the HIPAA requirements that must be considered in addition to ISO 17799:2005 controls.

Appendix B

Summary of Mobile Computing Threats and Attacks

Security Elements	Designation
Privacy	**Pr.**
Confidentiality	**Co.**
Integrity	**In.**
Availability	**Av.**
Authenticity	**Au.**
Non-repudiation	**No.**

The symbol "X" signifies that an attack affects an element

Threat	Attacks Method	Attack Examples	Attack Impact	Pr.	Co.	In.	Av.	Au.	No.
Traditional Wired Network Attacks	Random IP packets -Kiss of Death (KoD) -ActiveSync Flood -Ping Flood -802.11 Deassociate -802.1X Failure	-Random IP packets sent by attacker causes device to lose Internet connectivity, Explorer to crash, and device memory to run critically low. -Deassociate flood from tool like AirJack blocks Wi-Fi stations from reconnecting. -Direct Sequence spread Spectrum (DSSS) cordless	Crashes a system or denies access to service. -Deny device network access -Loss of data if hard reset required				X X X		

Threat	Attacks Method	Attack Examples	Attack Impact	Pr.	Co.	In.	Av.	Au.	No.
	Flood -Wireless Jamming -Wireless Sniffing	phones signals jamming Devices 802.11 and Bluetooth communication -Device using hotspots expose traffic to other LAN users, even when using WEP Unauthorized disclosure of data (including credentials)	-Unauthorized disclosure of data (including credentials)	X	X				
Spoofing Attacks	Desktop Spoofing -AP Spoofing -MAC Spoofing	-Compromised PC uses ActiveSync to quickly copy everything from Device -Rogue AP stores intercepted traffic without notice by PPC or legitimate AP -Rogue 802.11 station uses forged MAC address of handheld to access network	Unauthorized disclosure of data (including credentials) -Unauthorized access to organization's network via device	X	X			X	X
Man-in-the-Middle Attacks	TCP Session Hijacking -802.1X Hijacking	-TCP session hijacker intercepts/modifies data to/from device -When 802.1X Extensible Authentication Protocol exchange is hijacked, 802.11 station is tricked into sending credentials to a rogue AP outside tunnel	-Unauthorized disclosure, modification of data (including credentials) -Unauthorized access to organization's network via device -Modification of transactions to/from device	X	X	X X	X X	X X X	X X X
Rogue Peer-to-Peer Wireless Connections	-Ad Hoc 802.11 -Bluetooth	device configured for any SSID participates in P2P without owner noticing	-Unauthorized disclosure of data -Unauthorized disclosure of	X	X				

Threat	Attacks Method	Attack Examples	Attack Impact	Pr.	Co.	In.	Av.	Au.	No.
	-Infrared Beaming	-Data beamed over IR is also received by attacker intent on corporate espionage	credentials (passwords,keys)	X	X				
			-Delivery of malicious code to device			X	X		
Malicious Codes Pushed to Device	Virus -Worm -Trojan -Spyware -Hostile Java/ActiveX	Devices receives file with virus, then infects desktop during ActiveSync -Device receives mail with worm that uses Outlook contacts to replicate -Spyware installed with shareware program collects and reports usage data from device -Hostile ActiveX copied to device from desktop when synching offline web content -Device infected with remote access trojan while visiting hostile website used as attack platform to penetrate and oranization's network over VPN tunnel	-Inhibit business use of device				X		
			-Unauthorized modification of device configuration			X			
			-Loss of data if malware deletes files				X		
			-Unauthorized disclosure of data (including credentials)	X	X				
			-Distribution of malicious code to organization via device					X	X
			-Unauthorized access to organization's network via device					X	X
Traditional Application Attacks	-Port Scan Discovery -Access Open Servers -Buffer Overflow -Exploit Other common vulnerabilities and exposures	Attacker scans IP blocks, looking for active GPRS Devices -Attacker connects clients to open web or file server ports on device -Attacker invokes hard reset command using IE buffer overflow	-Denies application services				X		
			-Unauthorized modification of device			X			
			-Loss of data if attack overwrites or resets device				X		
			-Unauthorized disclosure of data (including credentials)	X	X				

Threat	Attacks Method	Attack Examples	Attack Impact	Pr.	Co.	In.	Av.	Au.	No.
Malicious Denial of Service (Crashing the System) **(DOS)**	-Hard Reset(entire device halts) -Soft Reset(specific application halts) -Battery Exhaustion	-Attacker injects hard reset code bomb over rogue ad hoc wireless connection, cutting mobile worker off from wireless delivery system -Device is kept busy by rogue Java applet until battery dies and reset required	-Denies services				X		
			-Loss of data since last save [soft] or backup				X		
			-Loss of credentials (passwords, private keys)				X		
			-Loss of programs and program settings				X		
Removable Storage Theft or Loss	Lost or stolen Device or device Card or component. Memory stick	-Thief "borrows" device card, copies data, and returns card without detection	Unauthorized disclosure of data (including credentials)	X	X				
			-Loss of data stored only on missing card or stick				X		
Device Theft or Loss	-Lost device -Stolen device	-Credentials on stolen handheld used for network access before loss is reported -Competitor peeks at files and contacts on lost device found at tradeshow	-Unauthorized disclosure of data (including credentials)	X	X				
			-Unauthorized access to organization's network via device					X	
			-Loss of data not backed up elsewhere				X		
Rogue Device Attacks Against Enterprises	Theft of Service -Server flood -Exploit VPN tunnel	Stolen device with VPN client used by attacker to access Organizations servers -Stolen device used to flood enterprise application server with failed requests	-Increased network usage (cost, performance)				X		
			-Deny legitimate use of enterprise network or servers				X		
			-Unauthorized access to organization's network via device					X	X
			-Distribution of malicious						

Threat	Attacks Method	Attack Examples	Attack Impact	Pr.	Co.	In.	Av.	Au.	No.
			code to organization via device					X	X
			-Unauthorized disclosure of data (including credentials)	X	X				

Appendix C

Cryptography

Cryptography is a science of using mathematics to transform information so that it is secure while it is being transmitted or stored (Whitman & Mattord, 2003 pp. 296 – 297; Ciampa, 2004, p. 272; Simpson, 2005, p. 294). This is achieved by scrambling the data so that it cannot be viewed by unauthorized users. Some cryptography terminologies that will be used in the remaining text are defined as follows:

Encryption: Encryption means changing an original or plain text to a secret message using cryptography.

Decryption: Decryption is the reverse of encryption, when the secret message is changed back to its original form.

Algorithm: An algorithm is a mathematical function or program that works with a key to encrypt and decrypt information.

Key: A value that is used by an algorithm to encrypt or decrypt a message.

Weak Key: A mathematical key that creates a detectable pattern or structure is called weak key.

Cipher: A cipher is an encryption or decryption algorithm tool that is used to create encrypted or decrypted text.

Cipher text: Data that has been encrypted by a cipher is called cipher text.

C.1 How cryptography works

According to Simpson (2005, p. 294) cryptography requires the use of a cipher in the encryption and decryption process. A plaintext is submitted to a cipher that is provided with a key value. The key can either be a word, number, or phrase to encrypt plaintext into a ciphertext. To view the original text again, the ciphertext must be decrypted with the cipher to produce the original text. The security of encrypted data is entirely dependent on the strength of the cipher and the secrecy of the key.

C.2 How cryptography protects.

According to Whitman & Mattord (2003 pp. 305 – 306) and Ciampa, (2004, p. 274) cryptography seeks to fulfill five key security functions described below:

Confidentiality of Information: This means allowing only authorized users to access information. Only authorized users should have the cipher and the key to decrypt encrypted information.

Authentication: This means verifying who the sender was and trusting that the sender is who he claims to be.

Integrity: This means that a receiver of information should be able to trust that the message has not been altered.

Non-repudiation: This means ensuring that a sender or receiver of message cannot deny that a message was sent.

Access control: This means restricting the availability to information.

C.3 Types of Cryptographic algorithms

According to Simpson (2005, p. 296), Ciampa (2004, p. 275) and Sutherland & Madrid (2003), there are three categories of cryptographic algorithms. These algorithms are as follows:

Hashing Algorithms

Hashing is also referred to as one-way hash, and creates a ciphertext from plaintext. However, the message is never intended to be decrypted but instead is used for verification. Hashing algorithms takes a variable length input and converts it to a fixed length output called a hash. If a message is hashed and the content of the message is changed along the way, the hash value changes. It supports integrity by serving as a checksum to verify message content. In addition hashing supports authentication, it can be used to protect passwords or pins, a practical example is an ATM card system when dealing with pin numbers. Examples of hashing algorithms are Message Digest (MD2-5) and SHA, a more secure and widely used hash than MD.

Symmetric Algorithms

The symmetric algorithm uses a single key to encrypt and decrypt data. Both the sender and the receiver must agree on the key before data is transmitted. Symmetric algorithms support confidentiality, but not authentication and non-repudiation. In addition it requires each pair of users to have a unique secret key, so when there are more, key management is a challenge. Furthermore, it is difficult to deliver keys without risks of theft. However, they are faster than asymmetric algorithms. Examples of symmetric algorithms include, Triple DES (3DES), International Data Encryption Algorithm (IDEA), Blowfish, RC5(6) and Advanced Encryption Standard (AES). The AES is known for its impressive combination of security, performance, efficiency and flexibility. This makes it ideal for encrypting data stored on mobile devices.

Asymmetric Cryptography Algorithms

The asymmetric algorithm also known as public key cryptography uses two keys that are mathematically related, the public and the private keys. One is used to encrypt and the other to decrypt. Asymmetric algorithms support authentication, non-repudiation and confidentiality but are slower than symmetric algorithms. The public key is widely known by everyone, while only the key owner knows the private key. The problems of key distribution are solved by public key cryptography.

Asymmetric algorithms include RSA, Diffie Hellman and the Elliptical Curve Cryptography (ECC). The latter has earned respect for combining strength with performance. It is an efficient algorithm requiring few resources such as memory, disk space and bandwidth. The ECC algorithm is a perfect choice, for wireless and mobile devices (Lucent, 2001; Sutherland & Madrid, 2003).

However, most public key algorithms are relatively computationally costly, in comparison with many symmetric key algorithms. In many applications, these methods are complementary, taking advantage of the speed of symmetric to encrypt data and the strength of the asymmetric to encrypt the symmetric keys (Simpson, 2005, pp. 295-296; Ciampa, 2004, pp. 279 – 291; Sutherland & Madrid, 2003).

For example, wireless messaging may use asymmetric keys to establish a session between a client and server, and then use symmetric keys to encrypt the data that is exchanged. It can be argued that using a combination of Advanced

Encryption Standard (AES) and Elliptical Curve Cryptography (ECC) technology can provide the highest possible level of security without sacrificing system performance on mobile devices. Applications that use a combination of both symmetric and asymmetric techniques, are often referred to as “hybrid cryptosystems” (Whitman & Mattord, 2003, p. 307). An example of such a process is the Diffie-Hellman key exchange method of exchanging private keys using public key cryptography.

Digital signatures

Asymmetric algorithms have useful features for multiple types of security functions. This form of cryptography relies on digital signatures (Weise, 2001; Simpsons, 2005, p. 300). A digital signature is an encrypted hash of a message. It helps prove that the person sending a message with a public key is who he/she actually claims to be (Authentication). It also proves that the message was not tampered with (integrity) and that it was sent in the first place (Non-repudiation). Hashing a message is much faster than directly using digital signatures. By first computing a hashcode of a message and subsequently applying a digital signature to the short hashcode security and efficiency is improved.

Digital certificates

Another way authentication can take place over a communication channel is through the use of digital certificates (Ciampa, p. 313; Microsoft, 2003). A certificate is the digital document that verifies two parties exchanging data over the internet ensuring they are who they claim to be. Each certificate contains a unique serial number and must follow the X. 509 standard. It describes how a certificate should look like. Secure Socket layer and Transport Layer security employ the use of certificates and usually require a Public Key Infrastructure (PKI).

C.4 Public key Infrastructure

A PKI manages the keys and identity information required for asymmetric cryptography, integrating digital certificates , public key crytography, and Certificate Authorites. It combines software, encryption technologies and services that an organization needs to deploy asymmetric crytography (Weise, 2001;

Simpsons, 2005, p. 306).

The binding between a public key and its 'owner' must be correct, if not it can become an entirely insecure in practice. Associating a public key with its owner is typically done by protocols implementing a public key infrastructure; these allow the validity of the association to be formally verified by reference to a trusted third party, either in the form of a hierarchical Certificate Authority (e.g., X.509), a local trust model (e.g., SPKI), or a web of trust scheme as used with PGP.

After a user trusts a Certificate Authority (CA) the user can download a digital certificate and public key from the CA and store them on the device (Ciampa, 2004, pp. 321 - 324). A digital certificate only verifies a digital signature; it can't be used to create one. It provides the public key together with information of who owns it, what it can be used for, when it expires, and so forth (Microsoft, 2003). A digital signature is created using the private key that's associated with the digital certificate.

Appendix D

ISO 17799 and HIPAA comparison: Summary

ISO/IEC 17799 Sections	**Comparison**	**HIPAA**
4. Risk Assessment and treatment:		
4.1 Assessing Security Risks	**ISO ~ HIPAA**	164.308(a) (1)ii(A)) (Risk Analysis)
4.2 Assessing Security Risks	**ISO ~ HIPAA**	164.308(a)(1)(ii)(B) (Risk Management)
Section 5 Security policy		
5.1 Information Security (IS) policy:		
5.1.1 Information security policy document	**ISO ~ HIPAA**	164.316(a) policies and procedures 164.316(b)(1) (Documentation)
5.1.2 Review of the Information security policy	**ISO ~ HIPAA**	164.306(e) (Maintenance), 164.308(a)(8) (Evaluation) 164.316(b)(2)(iii) (Updates)
Section 6 Organization of Information Security		
6.1 Internal Organization		
6.1.1 Management commitment to information security	**ISO > HIPAA**	164.308(a)(2) (Assigned Security Responsibility). 164.308(a)(8) (Evaluation) 164.308(a)(3)(ii)(A)**,** (Authorization and/or S upervision)
6.1.2 Information Security co-ordination	**ISO > HIPAA**	164.308(a)(2) (Assigned Security Responsibility)
6.1.3 Allocation of Information Security responsibilities	**HIPAA > ISO**	164.308(a)(2) (Assigned Security Responsibility)
6.1.4 Authorization process for information Processing facilities	**ISO ~ HIPAA**	164.308(a)(1)(i) (Security Management Process), 164.308(a) (1)ii(A)) (Risk Analysis)
6.1.5 Confidentiality Agreements	**ISO ~ HIPAA**	164.308(a)(3)(i) (Workforce Security) 164.314(a)(1) (Business Associate Contracts or Other Arrangements) 164.308(a)(1)(ii)(B) (Risk Management)
6.1.6 Contact with Authorities	**HIPAA #**	Null
6.1.7 Contact with Special Interest group (SIG)	**ISO > HIPAA**	164.314(b)(2)(iv) "Report Security Incidents"
6.1.8 Independent Review of Information Security	**ISO ~ HIPAA**	164.308(a)(8) (Evaluation)
6.2 External Parties:		
6.2.1 Identification of risks related to External parties	**ISO ~ HIPAA**	164.308(b)(1) (Business Associate Contracts (BACs) and Other Arrangements) 164.308(a)(1)(ii)(A) "Risk Analysis"
6.2.2 Addressing Security when dealing with customers	**ISO > HIPAA**	164.308(b)(1) (Business Associate Contracts (BACs) and Other Arrangements)
6.2.3 Addressing security in Third Party agreements	**ISO ~ HIPAA**	164.308(b)(1) (Business Associate Contracts (BACs) and Other Arrangements, 164.308(b)(4) (Written Contract and Other Arrangements) 164.314(b)(2)(iii)(Ensure Agents Safeguard) 164.314(b)(2)(i)
Section 7 Asset Management		
7.1 Responsibility for Assets.		
7.1.1 Inventory of Assets	**ISO > HIPAA**	164.308(a)(7)(ii)(E) "Applications and Data

ISO/IEC 17799 Sections	**Comparison**	**HIPAA**
		Criticality Analysis”. 164.310(d)(2)(iii) “Accountability
7.1.2 Ownership of Asset	**HIPAA > ISO**	164.308(a)(2) (Assigned Security Responsibility)
7.1.3 Acceptable use of Assets	**HIPAA > ISO**	164.308(b)(1) (Business Associate Contracts and Other Arrangements), 164.308(b)(4) (Written Contract), and 164.314(a)(1) (Business Associate Contracts or Other Arrangements)
7.2 Information classification:		
7.2 .1 Classification guidelines	**ISO > HIPAA**	164.308(a)(7)(ii)(E) (Applications and Data Criticality Analysis)
7.2.2 Information labeling and handling	**ISO > HIPAA**	164.308(a)(4) (Information Access Management)
Section 8 Human Resources Security		
8.1 Prior to Employment:		
8.1.1 Roles and Responsibilities	**ISO > HIPAA**	164.308(a)(3)(ii)(A)**,** (Authorization and/or Supervision)
8.1.2 Screening	**ISO > HIPAA**	*164.308(a)(3)(ii)(B)* “Workforce Clearance Procedure”
8.1.3 Terms and Conditions of Employment	**ISO > HIPAA**	164.308(a)(1)(ii)(C) (Sanction Policy)
8.2 During Employment		
8.2.1 Management Responsibilities	**ISO ~ HIPAA**	164.308(a)(2) (Assigned Security Responsibility) 164.308(b)(1), 164.308(b)(4) (Written Contract), and 164.314(a)(1) (Business Associate Contracts or Other Arrangements)
8.2.2 Information Security awareness, education and training	**ISO ~ HIPAA**	164.308(a)(5)(i) (Security Awareness Training)
8.2.3 Disciplinary Process	**ISO ~ HIPAA**	164.308(a)(1)(ii)(C) (Sanction Policy)
8.3 Termination or Change of Employment		
8.3.1 Termination responsibilities	**HIPAA #**	“Null”
8.3.2 Return of Assets	**HIPAA #**	“Null”
8.3.3 Removal of access rights	**ISO ~ HIPAA**	164.308(a)(3)(ii)(C) (Termination Procedures) .
9 Physical and Environmental security		
9.1 Secure areas		
9.1.1 Physical security perimeter	**ISO ~ HIPAA**	164.310(a)(2)(ii) (Facility Security Plan)
9.1.2 Physical entry controls	**ISO ~ HIPAA**	164.310(a)(2)(iii) (Access Control & Validation Procedures) 164.310(a)(2)(ii) (Facility Security Plan)
9.1.3 Securing offices, rooms and facilities	**ISO ~ HIPAA**	164.310(a)(2)(iii) (Access Control & Validation Procedures), 164.310(a)(2)(ii) (Facility Security Plan) and 164.310(b) (Workstation Use) 164.310(c) (Workstation Security)
9.1.4 Protecting against external and environmental threats	**ISO ~ HIPAA**	164.308(a)(1)(ii)(B) “Risk Management”.
9.1.5 Working in Secure areas	**ISO ~ HIPAA**	164.310(a)(2)(iii) (Access Control & Validation Procedures), 164.310(a)(2)(ii) (Facility Security Plan) ,164.310(b) (Workstation Use) and 164.310(c) (Workstation Security)
9.1.6 Public access, delivery and loading areas	**ISO ~ HIPAA**	164.310(a)(2)(iii) (Access Control & Validation Procedures) and 164.310(a)(2)(ii) (Facility Security Plan)
9.2 Equipment Security.		
9.2.1 Equipment siting and	**ISO > HIPAA**	164.310(b) Workstation Use 164.310(c)

ISO/IEC 17799 Sections	Comparison	HIPAA
protection		Workstation Security and 164.310(a)(2)(ii)Facility Security Plan.
9.2.2 Support utilities	**ISO > HIPAA**	164.310(a)(1)(ii)Facility Access Control.
9.2.3 Cabling Security	**ISO > HIPAA**	164.310(a)(2)(ii)Facility Security Plan
9.2.4 Equipment Maintenance	**HIPAA > ISO**	164.310(a)(2)(ii)(Facility Security Plan), 164.310(a)(2)(iii) (Access Control & 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) 164.306(e) (Maintenance)..
9.2.5 Security of equipment off premises	**ISO ~ HIPAA**	164.310(a)(2)(ii)Facility Security Plan and 164.310(d)(2)(iii) (Accountability)
9.2.6 Secure disposal or re-use of equipment	**ISO ~ HIPAA**	164.310(d)(2) (Media Re-use), 164.310(a)(2)(ii)Facility Security Plan and 164.310(d)(2)(i) (Disposal)
9.2.7 Removal of Property	**ISO ~ HIPAA**	164.310(d)(2)(iii) “Accountability”
10 Communications and Operating Management		
10.1 Operational Procedures and responsibilities		
10.1.1 Documented Operating Procedures	**ISO ~ HIPAA**	164.316(b)(2)(ii) “Availability”
10.1.2 Change Management	**HIPAA #**	“Null”
10.1.3 Segregation of Duties	**HIPAA #**	“Null”
10.1.4 Separation of development, test and operational facilities	**HIPAA #**	“Null”
10.2 Third Party service delivery management		
10.2 .1 Service Delivery	**ISO ~ HIPAA**	164.308(b)(1) Business Associate Contracts and Other Arrangements, 164.308(b)(4) Written Contract and 164.314(b)(1)” Requirements for Group Health Plans”.)
10.2 .2 Monitoring and review of third party services	**ISO > HIPAA**	164.308(b) (1) Business Associate Contracts and Other Arrangements and 164.314(a) (2) Business Associate Contracts.)
10.2 .3 Managing changes to third Party services	**HIPAA #**	“Null”
10.3 System Planning and Acceptance:		
10.3.1Capacity Management	**HIPAA #**	“Null”
10.3.2 System Acceptance	**HIPAA #**	“Null”
10.4 Protection against malicious and mobile code:		
10.4.1 Controls against Malicious codes	**ISO ~ HIPAA**	164.308(a)(5)(ii)(b)(Protection Against Malicious Software),. 164.312(a)(1)(Access Control)
10.4.2 Controls against mobile code	**HIPAA #**	“Null”
10.5 Back up		
10.5.1 Information back-up	**HIPAA > ISO**	164.308(a)(7)(ii)(a)(Data Back-Up Plan) requires data back-up planning and procedures. 164.310(d)(2)(iv) (Data Backup and Storage)
10.6 Network Security Management:		
10.6.1 Network Controls	**ISO > HIPAA**	164.312(e)(1)(Transmission Security)
10.6.2 Security of Network Services	**ISO > HIPAA**	164.308(b)(1) Business Associate Contracts and Other Arrangements 164.308(b)(4) Written Contract.)
10.7 Media Handling:		

ISO/IEC 17799 Sections	Comparison	HIPAA
10.7.1 Management of removable media	**ISO ~ HIPAA**	164.310(d) “Device and Media Controls”.
10.7.2 Disposal of Media	**ISO ~ HIPAA**	164.310(d)(2)(i)Disposal of Media and 164.310(d)(2)(iii) Accountability.)
10.7.3 Information Handling Procedure	**ISO ~ HIPAA**	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 and 164.310(d)(2)(iii) Accountability
10.7.4 Security of System documentation	**HIPAA #**	“Null”.
10.8 Exchange of Information:		
10.8.1 Information exchange policies and procedures	**ISO ~ HIPAA**	164.308(b) (1) Business Associate Contracts and Other Arrangements and 164.312(e)(1)(Transmission Security)
10.8.2 Exchange Agreements	**ISO > HIPAA**	164.308(b)(1)Business Associate Contracts and Other Arrangements)
10.8.3 Physical Media in Transit	**ISO > HIPAA**	164.310(d)(1) “Device and Media controls”
10.8.4 Electronic Messaging	**ISO ~ HIPAA**	(164.312(a)(1)Access Control and 164.312(e)(1)Transmission Security.)
10.8.5 Business Information System	**ISO ~ HIPAA**	164.308(b)(1)Business Associate Contracts and Other Arrangements, 164.308(b)(4)Written Contracts and 164.314(b)(1) “Requirements for Group Health Plans”.
10.9 Electronic Commerce Services		
10.9.1 Electronic Commerce	**ISO ~ HIPAA**	164.312(e) Transmission Security
10.9.2 Online Transactions	**ISO ~ HIPAA**	164.312(a)(1)Access control and 164.312(e)(1)Transmission Security
10.9.3 Publicly available Information	**ISO ~ HIPAA**	164.312(a)(1)Access Control and 164.312(c)(Integrity) 164.312(d)(Person or Entity Authentication). (164.312(e) Transmission security.)
10.10 Monitoring:		
10.10.1 Audit Logging	**ISO ~ HIPAA**	164.312(b)(Audit Controls)
10.10.2 Monitoring System use	**HIPAA > ISO**	164.308(a)(1)(ii)(d)(Information Security Activity Review). 164.308(a)(5)(ii)(c)(Log-In monitoring)
10.10.3 Protection of log Information	**HIPAA #**	“Null”
10.10.4 Administrator and operator log	**ISO > HIPAA**	164.312(b) “Audit Controls”
10.10.5 Fault Logging	**ISO > HIPAA**	164.308(a)(1)(ii)(D) “Information Security Activity Review”
10.10.6 Clock Synchronization	**HIPAA #**	“Null”
11 Access Control		
11.1 Business requirement for access control		
11.1.1 Access Control Policy	**HIPAA ~ ISO**	164.308(a)(3)(i)Workforce Security. 164.312(a)(1) “Access control” 164.308(a)(4)(ii)(B) Access Authorization
11.2 User Access Management:		
11.2.1 User registration	**ISO ~ HIPAA**	164.308(a)(4)(i)(Access Establishment and

ISO/IEC 17799 Sections	Comparison	HIPAA
		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 User Identification)
11.2.2 Privilege Management	**HIPAA ~ ISO**	164.308(a)(3)"Access Authorization" and 164(308)(a)(4) Access Establishment and Modification.)
11.2.3 User password Management	**ISO ~ HIPAA**	164.308(a)(5)(ii)(d)(Password Management)
11.2.4 Review of user access rights	**ISO ~ HIPAA**	164.308(a)(4)(ii)(c)Access Establishment and Modification"
11.3 User responsibilities:		
11.3.1 Password use	**ISO ~ HIPAA**	164.308(a)(5)(ii)(d) Password Management.)
11.3.2 Unattended user equipment	**ISO ~ HIPAA**	164.310(b) "Workstation Use" (164.310(c) Workstation Security 164.312(a)(2)(iii)(Automatic logoff) Session Termination Mechanisms.
11.3.3 Clear desk and clear screen policy	**ISO ~ HIPAA**	164.310(b) Workstation Uses and 164.310(c) Workstation Security, 164.312(a) (2) (iii) Automatic Logoff.)
11.4 Network Access Control		
11.4.1 Policy on the use of network services	**ISO > HIPAA**	164.312(a)(1)Access Control, 164.312(d)(2)Transmission Security and 164.308(a)(4)(ii)(b) Access Authorization.)
11.4.2 User authentication for external connection	**ISO ~ HIPAA**	164.312(d)(Person or Entity Authentication)
11.4.3 Equipment identification in networks	**ISO ~ HIPAA**	164.312(d) Person or Entity Authentication)
11.4.4 Remote diagnostic and configuration port protection	**ISO > HIPAA**	164.312(a)(1)Access Control, 164.312(a)(2)(i)Unique User Authentication and 164.312(d) Person or Entity Authentication.
11.4.5 Segregation in networks	**ISO ~ HIPAA**	164.314(b)(2)(ii) 'Ensure Adequate Separation"
11.4.6 Network connection Control	**HIPAA #**	"Null"
11.4.7 Network routing Control	**HIPAA #**	"Null
11.5 Operating system access Control		
11.5.1 Secure log-on Procedures	**HIPAA #**	"Null
11.5.2 User identification and Authentication	**ISO ~ HIPAA**	164.312(a)(2)(i)"Unique User Identification"
11.5.3 Password management System	**ISO > HIPAA**	164.308(a)(5)(ii)(d) "Password Management"
11.5.4 Use of system utilities	**HIPAA #**	"Null"
11.5.5 Session time-out	**ISO ~ HIPAA**	164.312(a)(2)(iii)"Automatic Logoff"
11.5.6 Limitation of connection time	**ISO > HIPAA**	164.312(a)(2)(iii)Automatic Logoff.)
11.6 Application and Information Access Control:		

ISO/IEC 17799 Sections	**Comparison**	**HIPAA**
11.6.1 Information access restriction	**ISO ~ HIPAA**	164.312(a)(1)Access Control, 164.308(a)(4)(ii)(b)Access authorization and 164.308(a)(4)(ii)(c) Access Establishment and Modification
11.6.2 Sensitive system isolation	**HIPAA > ISO**	164.308(a)(4)(ii)(A) (Isolating Health Clearinghouse Functions)
11.7 Mobile Computing and teleworking		
11.7.1 Mobile Computing and Communication	**ISO > HIPAA**	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 and 164.312(e)(1)"Transmission Security"
11.7.2 Teleworking	**ISO ~ HIPAA**	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 and 164.312(e)(1) Transmission Security.)
12 Information systems acquisition, development and maintenance		
12.1 Security requirements of information systems:		
12.1.1 Security requirements analysis and specification	**HIPAA #**	"Null"
12.2 Correct processing in applications		
12.2.1 Input data validation	**ISO > HIPAA**	164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information
12.2.2 Control of internal processing	**ISO ~ HIPAA**	164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information.)
12.2.3 Message Integrity	**ISO ~ HIPAA**	164.312(c)(1)"Integrity".), 164.312(d)(2) (Integrity Controls)
12.2.4 Output data validation	**ISO ~ HIPAA**	164.312(c)(2)(Mechanisms to Authenticate Electronic Protected Health Information).
12.3_Cryptographic controls		
12.3.1 Policy on use of cryptographic controls	**ISO > HIPAA**	164.308(a)(1)(i)"Security management process 164.312(a)(2)(iv) "Encryption and Decryption Encryption"
12.3.2 Key management	**HIPAA #**	"Null"
12.4 Security of system files:		
12.4.1 Control of operational software	**HIPAA #**	"Null"
12.4.2 Protection of system test data	**HIPAA #**	"Null"
12.4.3 Access Control to program source code	**HIPAA #**	"Null"
12.5 Security in development and support processes		
12.5.1 Change control procedures	**HIPAA #**	"Null"
12.5.2 Technical review of applications after operating system changes	**ISO ~ HIPAA**	"Null"

ISO/IEC 17799 Sections	Comparison	HIPAA
12.5.3 Restriction on changes to software packages	**HIPAA #**	“Null”
12.5.4 Information leakage	**ISO ~ HIPAA**	164.312(a)(1)Access Control, 164.308(a)(1)(i)Security Management Process and 164.312(e)(1) Transmission Security and 164.308(a)(1)(ii)(D) Information System Activity Review
12.5.5 Outsourced software development	**HIPAA #**	“Null”
12.6 Technical Vulnerability Management.		
12.6.1 Control of technical Vulnerabilities	**HIPAA ~ ISO**	164.308(a)(1)(ii)(B) Risk Management
13. Information security incident management		
13.1 Reporting information security events and weaknesses:		
13.1.1 Reporting information security events	**HIPAA ~ ISO**	164.308(a)(6)(Response and Reporting
13.1.2 Reporting security weaknesses	**ISO ~ HIPAA**	164.308(a)(1)(ii)(D)Information System Activity Review and 164.308(a)(6)Response and Reporting.
13.2 Management of Information security incidents and improvements:		
13.2.1 Responsibilities and procedures	**ISO ~ HIPAA**	164.308(a)(6)(i) (Security Incident Procedures) 164.308(a)(6)(ii) Response and Reporting
13.2.2 Learning from Information security incidents	**ISO ~ HIPAA**	164.308(a)(6)(ii)Response and Reporting and 164.308(a)(1)(ii)(b) Risk Management,.
13.2.3 Collection of evidence	**HIPAA > ISO**	164.316(b)(2)(i) (Time limit) “Policies and Procedures
14. Business Continuity Management		
14.1 Information security aspects of business continuity management		
14.1.1 Including information security in the business continuity management process	**HIPAA > ISO**	164.308(a)(7)(i)(Contingency Plan). 164.310(a)(2)(i)(Contingency Operations). 164.312(a)(2)(ii) (Emergency Access Procedure). 164.308(a)(7)(ii)(C) (Emergency Mode Operation Plan)
14.1.2 Business continuity and risk assessment	**ISO ~ HIPAA**	164.308(a)(7)(ii)(e)Applications and Data Criticality Analysis and 164.308(a)(1)(ii)(A) Risk Analysis
14.1.3 Developing and implementing continuity plans including information security	**ISO ~ HIPAA**	164.308(a)(7)(ii)(a)Data Backup Plan and 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 and 164.312(a)(2)(ii)Emergency Access Procedures.)
14.1.4 Business continuity planning framework	**ISO > HIPAA**	164.310(a)(1)(ii)(d)(Testing and Revision Procedures)
14.1.5 Testing, maintaining and re-assessing business continuity plans	**ISO ~ HIPAA**	164.308(a)(7)Testing and Revision Procedures
15. Compliance		
15.1 Compliance with legal requirements		
15.1.1 Identification of applicable legislation	**HIPAA #**	“Null’
15.1.2 Intellectual property rights (IPR)	**HIPAA #**	“Null”
15.1.3 Protection of	**HIPAA > ISO**	164.316(b)(1) Policies and Procedures

ISO/IEC 17799 Sections	**Comparison**	**HIPAA**
organizational records		Documentations
15.1.4 Data protection and privacy of personal information	**ISO ~ HIPAA**	164.306(a) Security Standards: General Requirements. 164.308(a)(2)Assigned Security Responsibility
15.1.5 Prevention of misuse of information processing facilities	**ISO ~ HIPAA**	164.310(a)(1)Facility Access Control, 164.310(b) “Workstation Use”, 164.308(a)(3)”Workforce Security”
15.1.6 Regulation of cryptographic controls	**HIPAA #**	“Null”
15.2_Compliance with security policies and standards, and technical compliance		
15.2.1 Compliance with security policies and standards	**ISO ~ HIPAA**	164.308(a)(8)(Evaluation)
15.2.2 Technical compliance checking	**ISO ~ HIPAA**	164.308(a)(8)Evaluation
15.3 Information systems audit controls		
15.3.1 Information systems audit controls	**HIPAA #**	“Null”
15.3.2 Protection of information system audit tools	**HIPAA #**	“Null”