A STANDARDS-BASED SECURITY MODEL FOR HEALTH INFORMATION SYSTEMS

Steven Thomson

A STANDARDS-BASED SECURITY MODEL FOR HEALTH INFORMATION SYSTEMS

by

Steven M. Thomson

DISSERTATION

Submitted in fulfillment of the requirements for the degree

Magistar Technologiae

in

Information Technology

at the

School of Information and Communication Technology

in the

FACULTY OF ENGINEERING, THE BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

of the

NELSON MANDELA METROPOLITAN UNIVERSITY

Supervisor: Dr. Dalenca Pottas

January, 2008

Acknowledgments

My deepest gratitude and appreciation are extended to:

- Our **Heavenly Father**, without whom nothing is possible;
- My parents, **Sandra and Lloyd Thomson**, for all their encouragement and always believing in me;
- My supervisor, **Dr Dalenca Pottas**, for her advice and always keeping me on track;
- My sister, **Kerry-Lynn Thomson**, for all her help and guidance;
- **Bronwyn Kaplan**, for the time taken to proofread my paper

Abstract

In the healthcare environment, various types of patient information are stored in electronic format. This prevents the re-entering of information that was captured previously. In the past this information was stored on paper and kept in large filing cabinets. However, with the technology advancements that have occurred over the years, the idea of storing patient information in electronic systems arose. This led to a number of electronic health information systems being created, which in turn led to an increase in possible security risks.

Any organization that stores information of a sensitive nature must apply information security principles in order to ensure that the stored information is kept secure. At a basic level, this entails ensuring the confidentiality, integrity and availability of the information, which is not an easy feat in today's distributed and networked environments. This paved the way for organized standardization activities in the areas of information security and information security management.

Throughout history, there have been practices that were created to help "standardize" industries of all areas, to the extent that there are professional organizations whose main objective it is to create such standards to help connect industries all over the world. This applies equally to the healthcare environment, where standardization took off in the late eighties. Healthcare organizations must follow standardized security measures to ensure that patient information stored in health information systems is kept secure. However, the proliferation in standards makes it difficult to understand, adopt and deploy these standards in a coherent manner. This research, therefore, proposes a standards-based security model for health information systems to ensure that such standards are applied in a manner that contributes to securing the healthcare environment as a whole, rather than in a piecemeal fashion.

DEPARTMENT OF ACADEMIC ADMINISTRATION
EXAMINATION SECTION – NORTH CAMPUS
PO Box 77000
Nelson Mandela Metropolitan University
Port Elizabeth 6013
Tel. +27 (0) 41 504 3206 / 504 3392
Fax. +27 (0) 41 504 9206 / 504 3064

DECLARATION BY STUDENT

NAME: ……………Steven Michael Thomson………………………………

STUDENT NUMBER: …20208166…………………………..………………

QUALIFICATION: MAGISTER TECHNOLOGIE: Information Technology

TITLE: …… A Standards-Based Security Model for Health Information

……………………Systems…………………………………….…………………

…………………………………………………………………………..………

DECLARATION:

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

SIGNATURE: ………………………………..

DATE: ………………………………..

Table of Contents

List of Figures

List of Tables

List of Acronyms

AFRO - Regional Office for Africa

ANSI - American National Standards Institute

ASTM - American Society for Testing and Materials

BS – British Standard

CCIS - Critical Care Information System

CCOW - Clinical Context Object Workgroup

CCR - Continuity of Care Record

CDMS - Clinical Data Management System

CEN - European Committee for Standardization

CENELEC - European Committee for Electrotechnical Standardization

CEO – Chief Executive Officer

C.I.A. – Confidentiality. Integrity. Availability

COSTAR - Computer-Stored Ambulatory Record

CPR - Computer-based Patient Records

CCR - Continuity of Care Record

CPRI - Computer-based Patient Record Institute

CWA – CEN Workshop Agreements

DHHS - Department of Health and Human Services

DICOM - Digital Imaging and Communications in Medicine

DOD – Department of Defense

E1987 - Electronic

ECC - European Economic Community

ECG – Electrocardiogram

ECHI – European Community Health Indicators

EEG – Electroencephalogram

EFTA - European Free Trade Association

EHR – Electronic Health Record

EMR - Electronic Medical Record

EN – European standards

ENV - European pre-standard

EPR – Electronic Patient Record

ETSI - European Telecommunications Standards Institute

EU – European Union

EU ISIS – European Union's Information Society Initiative in Standardization

HCE - Health-care Equipment & Supplies Co. Ltd

HDF – HL7 Development Framework

HELP - Health Insurance, Equalization, Legislative Adjustments, and Preservation of the Retirement System

HHS - Health and Human Services

HIBCC - Health Industry Business Communications Council

HIN - Health Industry Number

HIPAA - Healthcare Information Portability and Accountability Act

HIS - Health Information Systems

HL7 - Health Level-7

ICT - Information and Communication Technology

IHE - Integrating the Healthcare Enterprise

ISM – Information Security Management

ISMS - Information Security Management System

ISO – International Organization for Standardization

ISO/DIS – ISO/Draft International Standard

ISO/IEC – ISO/International Electrotechnical Commission

ISO/TR – ISO/Technical Report

ISO/TS – ISO/Technical Standard

JAMI - Japan Association of Medical Informatics

LDAP - Lightweight Directory Access Protocol

LDS – Latter-Day Saints

MEDSEC – Healthcare Security and Privacy in the Information Society

MLLP - Minimum Lower Layer Protocol

NCCLS - National Council for Clinical Laboratory Standards

NCPDP - National Council for Prescription Drug Programs

OMG - Object Management Group

P1157 - Project

PACS - Picture Archiving and Communication Systems

PC – Personal Computer

PDMS - Patient Data Management System

PHR – Personal Health Record

PII - Personal Identity Information

PKI – Public Key Infrastructure

SCHIP - State Children’s Health Insurance Program

SEMRIC - Secure Medical Record Information Communication

SHA-1 - Secure Hash Algorithm

SNOMED-CT - Systematized Nomenclature of Medicine-Clinical Terminology

Triple-DES – Triple - Data Encryption Standard

UCLA - University of California, Los Angeles

VHA - Veterans Health Administration

WEDI - Workgroup for Electronic Data Interchange

WHO - World Health Organization

XML – Extensible Markup Language

Chapter 1: Introduction

1.1 Introduction

This dissertation starts with a discussion on the healthcare environment, which comprises the focus area of this research, together with organized standardization activities in information security. A discussion on security in healthcare and an introduction to standardization in healthcare follow thereafter. The last part of the chapter covers the problem statement, the objectives, the methodology and the layout of this research. The chapter concludes with a brief summary.

1.2 The Healthcare Environment

1.2.1 Healthcare and the Role of Governments

Since the focus of this research takes place within a healthcare environment, a definition is needed of what exactly healthcare is. The Oxford Dictionary of Current English defines health as: “state of being well in body or mind” (Thompson, 1993, p. 405). According to The Free Dictionary website, healthcare is defined as a noun that entails, “The prevention, treatment and management of illness and the preservation of mental and physical well-being through the services offered by the medical and allied health professionals” (Farlex, 2008, para. 1). Furthermore, health information is defined as “the data which is produced and collected nearly exclusively within medical settings” (Wagener & Alkerwi, n.d). From both the health and healthcare definitions, a common thread can be seen. This thread is to ensure that an individual is kept both physically and mentally fit. However, health is linked to other non-medical factors such as socio-economic, environmental, political, behavioural factors, lifestyle, etc

(Wagener & Alkerwi, n.d). Therefore information about health does not only cover clinical data, but could also include related data about the social, economic, educational and environmental context of the population.

According to a project named “Design for a Set of European Community Health Indicators/ECHI”, there are four categories of health indicators to help develop a large network for sharing/comparing health data (ECHI Project, 2001). These four indicators are (ECHI Project, 2001):

1. Health systems;
2. Health status;
3. Demographic and socio-economic factors; and
4. Determinants of health.

These health indicators help display a global picture of the health situation. This list can also help describe, evaluate and monitor the health status of an entire population (Wagener & Alkerwi, n.d).

Typically, in democratic countries, a law that may be used to help implement healthcare is usually elaborated as a bill by government (Allaert & Barber, 2000). Healthcare systems all over the world are subject to government intervention (Peacott, 2003). Typically, those healthcare systems that are state funded and regulated are called ‘private’ systems, while there is also a more ‘socialized’ model that the government is also apart of (Peacott, 2003). The motivation for governments to involve themselves in healthcare systems is because of two different reasons (Peacott, 2003, p. 1):

- Government is often seen as the best protector of consumers, through such methods as compulsory licensure and accreditation of healthcare providers and institutions, as well as regulation of what medicines can be prescribed and distributed, and under what conditions; and

- In a world where healthcare can quickly become prohibitively expensive and private insurance is not always available or reasonably priced, government funding, either to individual consumers or the healthcare system as a whole, can often appear to be the only means by which people can afford to utilize modern healthcare providers and technologies.

State governments have also made efforts to affect health changes by providing meaningful data, disseminating collected information, coordinating services delivered and creating transaction systems for both public and private sectors amongst others (Mendelson & Salinsky, 1997). Through implementing information systems, the dissemination of information has become streamlined and provides enhanced analytical flexibility. The government could also aid the provision of data by implementing “executive information systems”, which could allow users to access large amounts of health data through a simple interface integrating historically maintained data (Mendelson & Salinsky, 1997).

Electronic communication between private and public stakeholders has helped to facilitate health transactions. Government has supported this communication by sponsoring health information infrastructures, developing standards for data content and transmission and encouraging integrated health information systems (Mendelson & Salinsky, 1997). In some instances, government has done more than just support public programmes and have rather chosen to take a more active role in improving information system capabilities (Bazzoli, 1996). However, it should be pointed out that there have been very few successful developments of a broad-based, community-focused system (Mendelson & Salinsky, 1997).

Another way that government can help the healthcare industry is by providing government-sponsored public healthcare programmes. The table below shows a few government healthcare programmes that have been implemented in the USA (Daniels, n.d).

Table 1.1: Government Healthcare Programs

Programme	**Beneficiaries**	**Expenditure**
Medicare	40.0 million aged and disabled	$242.4 billion
Medicaid	42.3 million low-income, mostly children, pregnant woman, disabled, and aged	$227.9 billion (joint Federal and State)
SCHIP	4.6 million low-income children	$4.6 billion (Federal/State)
VHA	4.0 million veterans	$20.9 billion
DOD TRICARE	8.4 million active duty military, families, and retirees	$14.2 billion
HIS	1.4 million American Indians and Alaskan Natives	$2.6 billion
Total	**About 100 million people**	**$512.6 billion**

The US government has shown that it is serious about healthcare as evident from President Bush's State of the Union address in January last year, although this did raise negative voices from the public, stating his objective to enhance the number of Americans with health insurance. This has led to the programme, the Affordable Choices Initiative, being implemented (Health Management Systems, Inc, 2007). This programme is a "voluntary programme that provides states with incentives to increase the number of citizens receiving private insurance, primarily by subsidizing access to private insurances" (Health Management

Systems, Inc, 2007, para. 2). It should be noted, however, that President Bush's address elicited rather negative voices from the public with regard to the health insurance issue.

1.2.2 Health Information Systems

The World Health Organization's (WHO) mission statement states that "the WHO has the responsibility to collaborate with member states in the generation and the use of appropriate health information to support decision-making, healthcare delivery and management of health services at both the national and sub-national levels" (WHO & AFRO, n.d.).

Together, the WHO and AFRO have created a programme of Development of Health Information Systems (HIS). This programme's functions include:

- Supporting the strengthening of national health information systems based on an explicit analysis of the needs of information;
- Contributing to the strengthening of monitoring and evaluation functions and their integration into the national managerial process through the implementation of effective information systems;
- Co-ordinating the efforts of partners and countries in the field of health indicators measurement and use, health data management and evaluation of health information systems.

These functions show how the WHO is involved with the development, evaluation and strengthening of health information systems, but what exactly is a health information system?

When healthcare information systems originated in the 1980s, these systems were program-specific, stove-pipe systems more than likely based on old mainframe or early standalone personal computer technologies (Arzt, 2007).

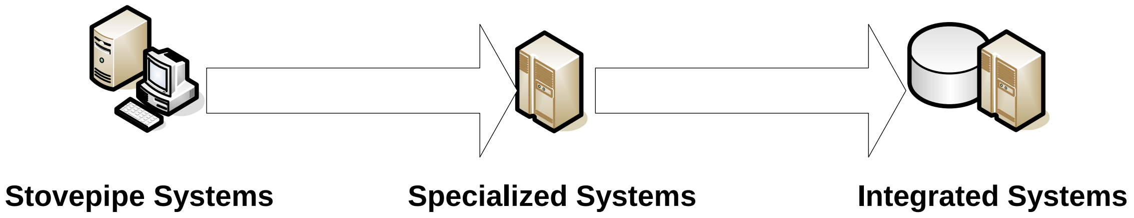
These early systems were often used by epidemiologists and others with public health analytical skills.

As technologies evolved, public health agencies soon realized that information technology was a justifiable target for investment in order to help improve the ability to perform core public health functions. Therefore, these agencies began upgrading, replacing or creating newer systems on their own (Arzt, 2007). These new systems were more robust and specialized and used modern database management systems and tools with more reliable platforms (Arzt, 2007).

The third step in healthcare information system evolution occurred when some agencies realized that deploying systems purely within individual programs caused serious limitations (Arzt, 2007). As networks grew, more applications became network-aware and network-dependant. This led to the need to leverage network investments becoming critical (Arzt, 2007). Thus, integrated systems were born. There are two types of integrated systems. Firstly there are those systems that provide data integration, which forms valid relationships between data sources and those systems that deal with application integration. The second type makes data available from different sources through a unified view of a computer application (Arzt, 2007).

Figure 1.1 summarizes this evolutionary process (Arzt, 2007).

Figure 1.1: Evolution of Health Information Systems



For health information systems, there are four types of integration models that can be used.

Information-orientated integration approaches operate through information exchange and databases and APIs that produce information (Mykkanen, et al., 2004). An example of this type of approach includes the use of HL7. The advantages of this type of integration are that (Mykkanen, et al, 2004):

- Source and target systems need only a few changes;
- State, logic and sequence do not need to be considered; and
- The approach is simple and widely used.

The process-orientated integration approach provides a layer of defined and centrally managed processes on top of existing processes. This type of integration hopes to combine relevant processes to support the flow of information and control logic between them (Mykkanen, et al, 2004). An example of this type of approach is IHE integration profiles.

On the other hand, service-orientated integration helps share business logic or methods. Shared methods are defined and the infrastructure for such sharing is provided (Mykkanen, et al, 2004). An example of this type of approach is the Object Management Group (OMG) Healthcare specifications.

Finally, the user-orientated integration approach provides a user with a consistent view of a multitude of systems (Mykkanen, et al, 2004). By using a unifying front-end, system this can be achieved. An example of this type of approach is the CCOW context management standard from HL7.

While the use of health information systems has various benefits, for example, effective medical decision-making and improved administrative systems, it has also contributed to an increased need to protect the data stored in those systems.

1.3 The Importance of Security in Healthcare

Over the years, there has been much technological advancement that has led to the healthcare industry leaning towards the use of electronic systems and leaning away from the old paper-based systems (Department of Health and Human Services [a], 2007). While this does mean that the medical workforce is more mobile and efficient, the use of these technological systems creates an increase of possible security risks (Department of Health and Human Services [a], 2007).

As more electronic health records are being used and the possibility of larger health networks increases, it is critical for the confidentiality, integrity and availability of electronic patient information to be guaranteed (Department of Health and Human Services, 2007 [a]). This criticality has translated into various laws which hold healthcare organizations legally liable if they do not protect the information that is in their care. The Health Insurance Portability and Accountability Act (HIPAA) is one well-known example of such a law in the healthcare industry. Before HIPAA, there was no set of accepted security standards for protecting health information in the healthcare industry (Department of Health and Human Services [a], 2007). The creation of these types of laws underscores the importance of security in healthcare.

Towards understanding the meaning of security, it is necessary to consider what the definition(s) of confidentiality, integrity and availability mean.

According to a paper written by Roy Schoenberg, confidentiality is defined as a situation in which some access to personal data is deemed appropriate, and the system or user qualifies for such access. Availability is defined as the consistency with which a system is ready to perform its function (Schoenberg, 2005). Finally, the definition of data integrity refers to the system's ability to ensure that once information has been entered into it, an attempt to retrieve that information will produce the same data that was entered or their intended compilation (Schoenberg, 2005). Another paper dealing with information security addresses the same three security components and defines them as follows (Cooper & Collman [b], 2005, p. 100):

- Confidentiality is the property that data or information is not made available or disclosed to unauthorized persons or processes.
- Integrity is the property that data or information has not been altered or destroyed in an unauthorized manner.
- Availability is the property that data or information is accessible and useable upon demand by an authorized person.

According to HIPAA, electronic patient information must (Department of Health and Human Services [a], 2007, p. 3):

- Be accessible only by authorized people and processes (confidentiality);
- Not be altered or destroyed in an unauthorized manner (integrity); and
- Be accessed as needed by an authorized person (availability).

Although the definitions were taken from three different papers and they do not match word for word, they all essentially provide the same definition of confidentiality, integrity and availability.

Another aspect of security is privacy. It is often misconstrued that privacy and confidentiality mean the same thing and therefore if the one is dealt with, the other is dealt with as well (Hunter, 2002). Privacy has been defined as “the concept that an individual has the right to decide what information he/she will disclose” (Hunter, 2002, p. 222). On the other hand, confidentiality can be seen as ensuring that information, after it has been disclosed by the individual, is not made public without proper permission. While confidentiality has been defined within the CIA Triangle, privacy, while not supported as a constitutional right in some countries, has been established as an individual's right by laws and customs over the years (Hunter, 2002).

One reason for patients' information to be kept secure is possible identity theft. An example of this happened in August 2004, when an employee at the Seattle Cancer Care Alliance, Richard Gibson, stole a cancer patient's name, date of birth and social security number (Scott, 2004). He then used this information to obtain four credit cards in this patient's name and racked up a bill of more than $9,000 in debt.

Computer theft is another threat that must be taken into account. In November 2003, a laptop that contained databases with the names, birth dates, social security numbers and blood types of 145,000 blood donors was stolen from UCLA (UC Santa Cruz, 2007). The following year in May, another laptop was stolen from the UCLA Healthcare financial office. This put another 62,000 patients at risk (UC Santa Cruz, 2007).

Another risk is when Personal Identity Information (PII) or any other sensitive information is stored in locations that have broader access rights than is appropriate (UC Santa Cruz, 2007). In April 2007, during a reconfiguration of a web site for the Health Sciences Center library, files containing names and social security numbers were accidentally copied to a more accessible area of the Internet (UC Santa Cruz, 2007).

It should also be remembered that when disposing of confidential information, the manner of disposal must be permanent. In March 2007, the Georgia Division of Public Health discarded paper records containing Social Security numbers and medical histories without shredding them (UC Santa Cruz, 2007). Since these documents were not shredded, anyone picking them up out of the trash would have the information without having to by-pass security.

Compromised computers can also lead to a security breach of information. A computer disk, which was owned by a private vendor, was stolen in April 2007 (UC Santa Cruz, 2007). This disk contained the addresses, birth dates, full names and Social Security numbers of 2,900,000 individual patients (UC Santa Cruz, 2007).

The afore-mentioned examples show what can happen if the proper security measures are not taken. The subsequent problems might have been prevented if industry standards had been used to guide the creation of secure environments. The computer thefts could have been prevented if the laptops had been securely locked down to something permanent. Also, for portable devices, it would be a good idea to use encryption in order to protect any information on those devices (UC Santa Cruz, 2007).

An organization should also make sure that they are aware as to who has access to which folders ***before*** any information is placed there (UC Santa Cruz, 2007). This is to prevent unauthorized access even before the information is stored. Another best practice would be to ascertain that any sensitive information is not placed in publicly accessible areas (UC Santa Cruz, 2007).

In order to help secure information, industry standards may be used in order to direct attempts towards protecting sensitive information during its creation, storage and transmission.

1.4 Standards in the Healthcare Environment

While the use of computers in the health industry started in the 1960s (Berner, Detmer, & Simborg, 2005), the actual need for organized standardization activities, as well as the common use of standards, within the healthcare environment was only realized in the late 1980s (Kokolakis, Gritzalis, Katsikas and Ottes, 2002).

According to the chapter “Technical Standards Used in Health Care Informatics” in the book “Health Care Informatics: An Interdisciplinary Approach” published in 2002, the technical standards that are used within the Health Care Informatics Environment can be categorized into a number of different categories ranging from general standards all the way to telecommunications standards.

These categories are listed as follows (Smith, 2002):

- Identifier standards;
- General communications standards;
- Specific communications standards;
- Content and structure standards;
- Standards for software applications;
- Telecommunications standards.

An overview of each of these categories is subsequently presented.

1.4.1 Identifier Standards

Identifier standards used in healthcare are necessary in order to uniquely specify each patient, provider, site of care and product in an electronic format. The Health Insurance Portability and Accountability Act (HIPAA), passed in 1996, included provisions to help address the need for a standard national provider identifier, a national employer identifier, a national healthcare provider identifier and other standards that would lead to administrative simplification.

Within this category of standards, there are four subsections which are (Smith, 2002):

- Patient identifiers, which use Social Security numbers and Universal Healthcare identifiers to help identify the patient;
- Provider Identifiers, which consist of using Universal Provider Identifier numbers as well as National Provider Identifiers;
- Site-of-Care Identifiers to help identify healthcare facilities, practitioners and retail pharmacies. An example of a Site-of-Care Identifier is the Health Industry Number (HIN);
- and finally the Product and Supply Labeling Identifiers which use the Label Identifier Code, Health Industry Bar Code, Health Industry Number, Universal Product Number, Universal Product Code and National Drug Code to identify each product.

1.4.2 General Communication Standards

General communications standards are those communication standards that are used for most of the electronic message transactions in healthcare and have been generally accepted both by users and by vendors. Examples of these standards would be: Health Level Seven, the Common Object Request Broker Architecture and P1157: Medical Data Interchange Standard (Smith, 2002).

1.4.3 Specific Communication Standards

Specific communication standards are communication standards that are released for a particular health domain. These domains can include pharmacy, medical devices, imaging or insurance (Smith, 2002).

1.4.4 Content and Structure Standards

Content and structure standards are aimed at the development of standards for the design of the Electronic Health Record (EHR). The guides within this category offer direction, but do not establish a standard practice for users to follow (Smith, 2002).

1.4.5 Standards for Software Applications

In order to transmit information, a variety of software applications are required. Recently, there has been a lot of emphasis placed on Web technologies in healthcare since these standards are used to transfer information and data through the World Wide Web (Smith, 2002). These standards can be important for use in healthcare informatics together with applications that have been developed to use the Web.

1.4.6 Telecommunication Standards

The telecommunications standards are used to communicate information and electronic commerce (Smith, 2002).

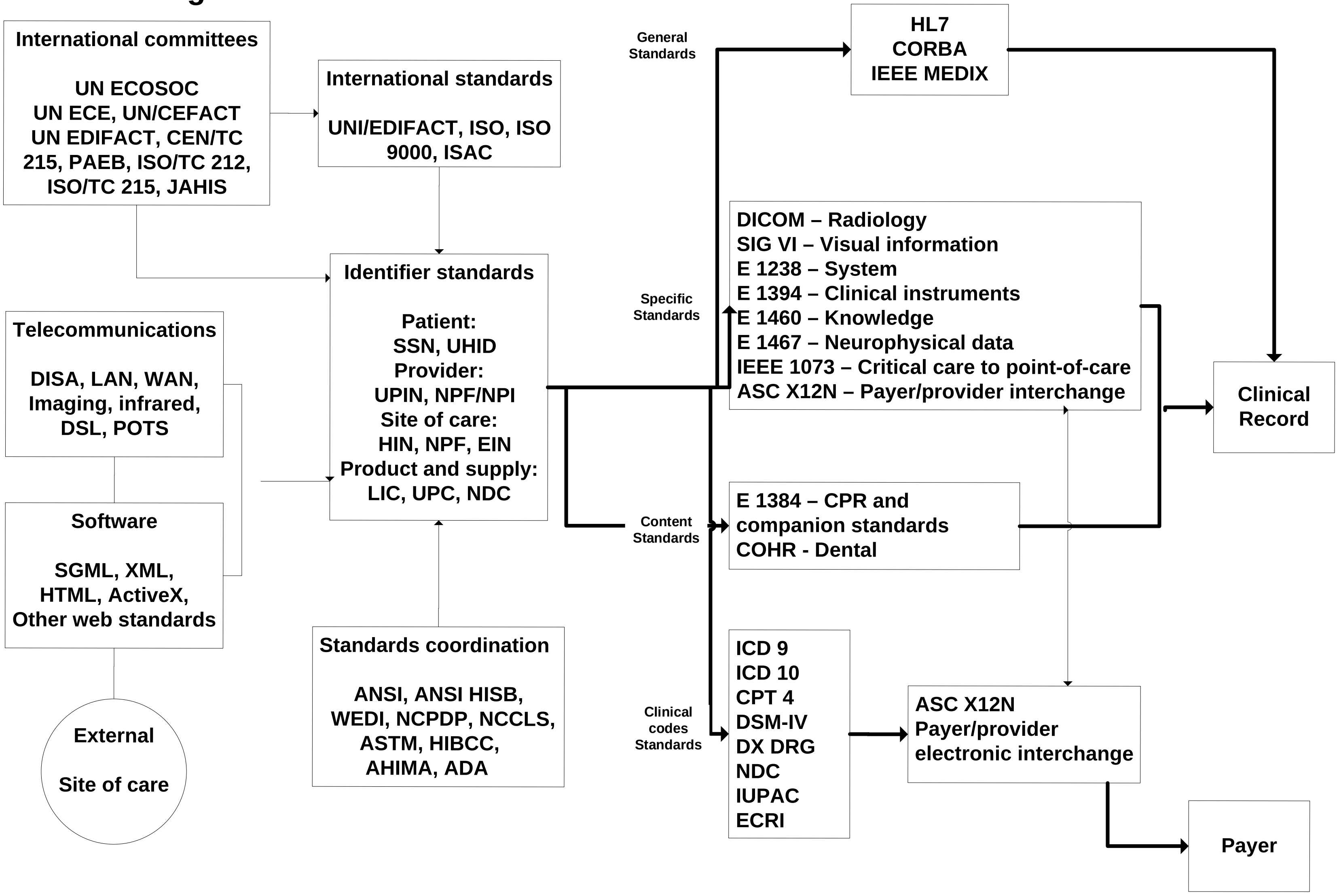
Figure 1.2 provides a graphical representation of the categories of technical standards used in healthcare as well as some of the standards that reside in each category (Smith,2002).

In a paper entitled “*Healthcare information standards: comparison of the approaches*”, healthcare informatics standards are categorized as follows (Spyrou, et al., 2002):

- Vocabulary standards intend to establish common definitions for medical terms;
- Structure and content standards give a clear description of the data elements that will be included in electronic health records;
- Messaging standards facilitate the electronic exchange of data between two or more disparate computer systems;
- Visual integration standards ensure that applications automatically synchronize, based on their common context, according to the user’s selection of application;
- Security standards ensure that an individual’s health information remains confidential and is protected from unauthorized access, alteration or destruction. These standards are especially important because electronic healthcare records make information accessible to multiple users in multiple locations and with different levels of accessibility to the healthcare data elements.

This research focuses primarily on this last category of healthcare standards, namely security standards.

Figure 1.2: Technical Standards Used in Health Care Informatics



1.5 Problem Statement

One of the most valuable functions of health information systems is to provide interoperability. It allows health establishments to share information even to the extent of global information exchange. However, the provision and existence of interoperability are entirely dependent on the adoption and use of standards. To this effect, the healthcare environment has many standards-developing organizations and bodies, each developing guidelines, standards and specifications to support interoperability in healthcare informatics. The large number of healthcare organizations and standards that exist, or are in development, make it difficult to monitor and track the overall landscape of healthcare standards (National Institute of Standards and Technology, 2006). This statement is as applicable to security standards for the healthcare environment. This research, therefore, addresses the problem of a proliferation in standards bodies and standards, in particular, security standards, which make it difficult to identify, understand, adopt and deploy these standards in a coherent manner.

In order to investigate the afore-mentioned problem statement, the following research questions are addressed:

- How is the healthcare environment constituted?
- Within this milieu, why is security particularly important?
- What is the status quo with regard to standards bodies and standards in the healthcare environment and, in particular, security standards?
- How can this environment, specifically health information systems, be secured through the use of security standards?

Through effectively addressing the afore-mentioned research questions, the objectives, discussed in the following section, are achieved in this dissertation.

1.6 Objectives

The principal objective of this study is to develop a standards-based security model for health information systems. The model is derived from an investigation of standards that have been developed to address security in healthcare.

This objective is achieved by addressing the following sub-objectives that are based on the research questions stated in Section 1.5:

- Investigate the healthcare environment and health information systems in order to gain insight into the healthcare landscape.
- Establish the level of importance of and the need for security in healthcare.
- Discuss standards bodies and standards in the healthcare environment and, in particular, security standards.
- Incorporate the information gleaned from the afore-mentioned investigations in a standards-based security model for health information systems.

In order to reach the objectives of this research, the following methodology will be followed.

1.7 Methodology

The research conducted for this project is primarily of a phenomenological nature. This is also known as interpretivist research - the researcher gathers information and filters it, while involving himself in the study. In this kind of research, subjectivity plays a role, with the researcher having to argue for towards the interpretation of the research area and the proposed solution.

Since the research is predominantly of a phenomenological nature, the execution of a proper literature study was employed as a suitable research method. An extensive literature study was conducted to gather information as pertaining to the following:

- The history of healthcare information systems;
- The importance of security in healthcare;
- Standards bodies and standards, in particular security standards in healthcare.

The information gathered was interpreted and through logical argumentation, a standards-based security model for health information systems was proposed.

1.8 Layout of Dissertation

The layout of the dissertation is divided into five chapters and is demonstrated in Figure 1.3.

Chapter 1 has covered the healthcare environment, health information systems and the role of the government. The importance of security in healthcare and the different types of standards in the healthcare environment were discussed. The chapter also covered the problem statement, research objectives and methodology used for this research. Chapter 2 provides a discourse on the history of computer health records as well as the terminology associated with the EHR. Chapter 3 deals with the various standards and what they necessitate.

Chapter 4 presents the proposed solution of the research, namely a standards-based model for security in healthcare. Chapter 5 concludes the dissertation by showing how the objectives of the research were met and touches on the benefits and limitations of the research process and research output.

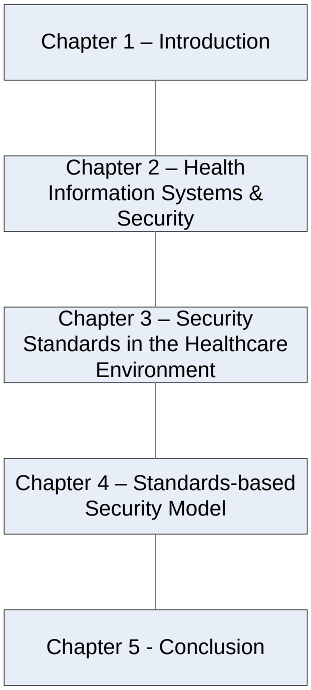

Chapter 1 – Introduction
Chapter 2 – Health Information Systems & Security
Chapter 3 – Security Standards in the Healthcare Environment
Chapter 4 – Standards-based Security Model
Chapter 5 - Conclusion

Figure 1.3: Proposed Layout of Dissertation

1.9 Summary

This chapter introduced two of the main focus points of this research, namely security and healthcare. This serves as background information to the more detailed literature study conducted in the following chapters, before the model solution is presented in Chapter 4.

Chapter 2: Health Information Systems and Security

2.1 Introduction

Chapter 1 introduced the healthcare environment and the importance of security in healthcare. There was also a brief introduction to standards in the healthcare industry. Now that there has been a clear outlining of what this research will attempt to achieve, there needs to be a discussion on Health Information Systems and what security is required to implement them. This will be discussed from the perspective of HIPAA and Information Security Management.

2.2 Health Information Systems

2.2.1 History/Background of HIS

The paper-based medical record arose in the 19th century as a highly personalized "lab notebook" that clinicians could use to record their observations so that they could be reminded of pertinent details when they next saw the same patient (Shortliffe, 1999). Doctors tended to work alone and wrote down their patients' medical records using this paper-based format. Patients were considered friends to these early doctors and often paid them directly (Tipton & Krause, 2004). However, there have been various challenges regarding the traditional paper-based clinical record which have been both noted and discussed for decades (Milholland, 1989). One of the problems with paper-based records is that there is usually only a single copy which is the original document (Hunter, 2002). This document could be used by many people over a varying length of time which could lead to the loss of this document. Another concern is that while one person is using the original document, is that if there is not another copy, then no one else would be able to use the document even if it was an emergency thus reducing availability. Thus as time progressed, people started to think that perhaps there was another way that could provide well-organized and well-timed access to patients' health records (Waegemann, 2003). This led to innovators beginning to recognize the power of computer-based systems (Milholland, 1989)

During the early 1960s, computers were first used within a hospital setting; however, then they were only used for administrative and financial functions. At this time, there was early work being conducted in the medical informatics area. This work focused on clinical computing to improve clinical decisions and reduce medical errors, as well as ensuring faster access to applicable medical information and decision-support functions (Berner, Detmer, & Simborg, 2005). These first systems that were designed to include features and functions in order to replace the paper system were used in the critical care units and were designed to collect, store, organize and retrieve data related to direct patient care and were given different names (Hunter, 2002). Examples of the early Electronic Medical Record (EMR) versions, or the Computer-based Patient Records (CPR), include the HELP system at LDS Hospital in Utah, the COSTAR system at Massachusetts General Hospital, the TMR system at Duke and the Regenstrief Medical Record System (Berner, Detmer, & Simborg, 2005).

Even with all of the scientific medicine growth (more pharmaceuticals, etc), the adoption of computer applications was between low and non-existent for many different reasons. One of these reasons was that clinicians were not willing to accept early systems because they felt that they were too expensive, slow and awkward. Administrators were against these EMRs because it was not clear what the financial benefits would be at the time. Another reason for lack of adoption in the United States was that the federal government created the Medicare and Medicaid legislation. Under this law, administrators and insurers both felt satisfied to let medical staff continue to practice separately, without sharing information (Berner, et al., 2005).

However, by the beginning of the 1980s, technology that could compliment EMRs had greatly evolved. The original mainframe computers were being replaced with distributed networks of microcomputers, Microsoft Windows had been introduced and networking proliferated. This eventually led to the creation of the HL7 standard to allow for data interchange of health-related information.

Unlike during the 1960s and 1970s, there were a number of governmental programmes that promoted policies that helped distribution of the EMR. A conference held at the National Institute of Health in America in the late 1980s led to a report being released in 1991 specifically dealing with the Electronic Health Record (EHR) (Berner, et al., 2005). This report, called “The Computer-based Patient Record: An essential technology for healthcare”, looked at three main features: uses and users, technology and policy and implementation. This report was the Institute of Medicine’s most widely distributed publication and led to the construction of the Computer-based Patient Record Institute. Since merely recasting the medical record was not enough, a complete rethink was needed. Thus the medical record became known as the Computer-based Patient Record (CPR) and 12 essential functions were associated with it.

The most spectacular change since then has been the explosion in the use of the World Wide Web. This presented a potential increase of e-health and CPRs. In the latter half of 2003, the National Library of Medicine licensed SNOMED-CT, an EMR standard, for use by healthcare organizations throughout the United States (Berner, et al., 2005). Even though there have been many changes with regards to these various health information systems, the goal of increasing the quality of patient care is still resonant within the EHRs of today (Hunter, 2002).

Kathleen Hunter continues, by referencing Stega, Pollizi & Milholland, that in order to achieve these goals: “the system seeks to meet the information needs of clinicians through improved timeliness, accuracy, reliability, integrity and availability of data; improved data organization; increased diagnostic value from collected data and reduction of repetitive work and of costs” (Stega, Pollizi & Milholland, 1980).

2.2.2 Terminology

Because of the extemporized use of the three afore-mentioned terms (CPR, EMR and Electronic Health Record (EHR)) in the medical healthcare profession, there is some misunderstanding of and confusion between the different medical healthcare systems. Although various definitions are available from the literature, the truth is that there is no single general description that successfully classifies these three terms. The first published international EHR technical specification “ISO/TS 18308: 2004 Health Informatics-Requirements for an Electronic Health Record Architecture” contains seven different definitions drawn from four countries, each reflecting slightly different shades of meaning between different countries and organizations (Health Level Seven, Inc., 2004). This plethora of definitions typically has more similarities than differences and often merely constitutes a different perspective on the underlying data.

The difference between these and other systems is discussed below.

2.2.2.1 The Computer-Based Patient Record (CPR)

A CPR is described as a lifetime patient record that includes all information from all specialties and requires full interoperability. However, this specific definition is unlikely to be achieved due to implementation issues (Waegemann, 2003).

The U.S. Department of Defense, Veterans Affairs and the Indian Health Service originally set out to create an electronic patient record by using a backbone layer that would serve as an information mediator among various legacy systems (Carter, Brown, Nelson, Lincoln, & Tuttle.). This would be called the first definition of a CPR. The CPR has also been viewed as not a product or an object. The CPR is rather described as a set of processes that are put into place and supported by technology (Shortliffe, 1999).

2.2.2.2 The Electronic Medical/Patient Record (EMR/EPR)

An EMR/EPR is similar to a CPR, but does not necessarily contain a lifetime record and rather focuses on relevant information. It also has full interoperability within an enterprise (hospital, clinic, practice) (Waegemann, 2003).

The EMR is sometimes described as an “alphabet soup” due to all of the various names that it has been called, some of these being Clinical Data Repository and Electronic Patient Record. The problem does not end at what to call it, but also its definition. According to the Japan Association of Medical Informatics (JAMI), a standard EMR does not cover all application areas, but must support an order transmission system and an order result reference system for all types of application areas (Japan Association of Medical Informatics, 2003). For the purpose of distinguishing the EMR from the CPR and EHR, Ondo, Wagner and Gale define it as “a complete on-line record that is accessible to all that need it when it is needed” (Ondo, Wagner, & Gale, 2002).

2.2.2.3 The Continuity of Care Record (CCR)

The CCR is a standardized summary of health information that is transportable when a patient is seen at another provider to ensure “continuity of care” and reduction of medical errors. The CCR has been designed by a consortium of leading information technology and medical societies to enable the flow of information with the patient during transitions of care. It is an XML document readable by any computer with a Web browser and does not require special software (such as an electronic health record) or special transmission lines. It is a bridge to connect hospitals, nursing homes, home health agencies and physicians' offices while other national standards are developed and widely integrated into electronic health-record systems. A number of electronic medical-record vendors are already incorporating the CCR into the ambulatory EMR systems (Health Services Advisory Group, n.d.).

2.2.2.4 The Personal Health Record (PHR)

According to the Personal Health Working Group (2003), a PHR can be described as an electronic health-record system that: allows each person to control his/her own information; contains information for a person's entire lifetime; is accessible from any place at any time; is private and secure; is transparent (people can see who entered the information) and permits easy exchange of information across the healthcare system. These above attributes must be reflected in order to achieve a successful PHR (Personal Health Working Group, 2003).

2.2.2.5 The Electronic Health Record (EHR)

An EHR is a form of electronic storage that provides instant availability of information to authorized practitioners, which includes enhanced access to medical information and greater efficiency (Waegemann, 2003). Although ISO was not able to define the EHR back in 2000, it was able to define what functions the EHR should perform (International Organization for Standardization [k], 2000). The main purpose of the EHR is to supply a standard record of care supporting present and future care by any clinician. This will help by allowing any clinician to know the patients' conditions even if they are new patients. The EHR has further been defined as "any information relating to past, present or future physical/mental health or condition of an individual, which resides in electronic system(s) used to capture, transmit, receive, store, retrieve, link and manipulate multimedia data for the primary purpose of providing healthcare and health-related services"(Murphy, Waters & Amatayakul, 1999, p. 5). The EHR also has a number of secondary uses: medico-legal, quality management, education, research, public and population health, policy development, health-service management and billing/finance/reimbursement (International Organization for Standardization [k], 2000).

Another possible definition of an EHR was put forward by the Electronic Health Record Taskforce in 2001. According to it, based on the essentials that people were looking for, it is: "an electronic longitudinal collection of personal health information, usually based on the individual, entered or accepted by healthcare providers, which can be distributed over a number of sites or aggregated at a particular source. The information is organized primarily to support continuing, efficient and quality healthcare. The record is under the control of the consumer and is to be stored and transmitted securely" (Smallwood, 2001).

Now that the EHR has been defined, what is expected of these systems? The IOM released a report identifying essential features and the necessary functions of the EHR (Hunter, 2002). This list has changed very little over the years, although some authors may have placed more detail into this list or expressed the list in a different way. M.J. Barret released a list in the year 2000 in his paper "The evolving computerized medical record". The list that he constructed contained the following elements he felt would make an "ideal" EHR:

- Review all client records;
- Measure expected improvements in a client's functional ability;
- Measure cost-effectiveness;
- Document the evidence of quality care for third parties;
- Track client status post discharge;

- Identify “best practices” from data in the records;
- Identify appropriate care for a specific client;
- Identify the immediate and long-term impact of treatments;
- Assess various indicators of quality, safety and effectiveness;
- Benchmark client types;
- Benchmark individual client progress and health outcomes.

One of the greatest incentives to adopting EHRs will be through reaching a critical mass of information sharing. Like the first few people with telephones or electronic mail, investors in healthcare information technology are by and large dealing with internal information systems unable to interact with outside systems (Ash & Bates, 2005). While there has not been a wide-scale adoption of the EHR, there are still a number of potential benefits. There are, however, a number of costs of the EHR. These costs refer more to the acquiring and implementing a system. Costs may include (Hunter, 2002):

- The extensive personal and organizational resources used during the vendor-selection process;
- The ongoing, significant and necessary costs of hardware and software maintenance of the systems;
- Costs for hiring a consultant to manage the implementation of the EHR system;
- Training of users on how to operate the system;
- The training also makes staff unavailable for their everyday work, which could lead to extra staff to cover the essential areas of an organization;
- Other, lesser costs could pertain to infrastructure, technology overheads and the impact of collateral projects.

Since there are a small number of implementations of the EHR, most of the benefits of implementing the EHR are potential benefits, which include (Hunter, 2002):

- Improving the quality of healthcare provided to individuals, communities and the nation;
- Documentation benefits;
- Time-saving;
- Possible reduction of staff required to maintain data records;
- More complete, better organized, less redundant and more legible documentation;
- Simultaneous access to the same information;
- Data stored as discrete data elements, which may be used for clinical, operational and strategic studies.

2.2.2.5.1 Security Concerns

With consideration for the context of EHRs and various facts presented about the adoption of this technology, the focus now shifts to the fact that security is considered (at least by some) as a major barrier to the implementation of EHRs.

As recent as 2005, a man by the name of Gordon Atherley argued that there would be problems with the EHR as it is a new technology – he asserted that EHRs consume too many resources that could be used to improve healthcare service delivery or development and if public policies fail, then people within the organization will lose confidence, especially in healthcare information technology. Atherley therefore conducted a study to try to prove his arguments were correct. His study showed that the main concern about EHR adoption was security, in particular people felt that privacy and confidentiality were undermined too much and felt that this was a severe public risk. Another chief security concern was the possibility of breakdowns in security occurring during implementation.

Atherley's study concluded that the public was still enormously concerned about both security and availability issues concerning the EHR (Atherley, 2005). While his study did not intend to discover security issues, it did end up exposing people's concerns about security within the EHR. Physicians do not concern themselves with the security aspects of a program as they feel that the Information Technology department should be monitoring the security features (Ash & Bates, 2005).

Another security issue is that since the EHR is designed to provide wide-range, even remote, connectivity this leaves the EHR open to security holes and flaws. It has also been suggested that a medical information officer be appointed to understand the implementation strategies (Ash & Bates, 2005).

In another study that was initiated to determine problems during the EHR setup, some security issues were also uncovered. When the results were released, the experiment showed that there were two major security concerns: users and administrators were commonly concerned about data loss and their other concern was about privacy, as there was no reliable way to predict who would need access to the EHR and who wouldn't (Tonnesen, LeMaistre, & Tucker).

2.2.2.5.2 EHR – Final Thoughts

The world has changed since the healthcare profession began. Presently, there is the personal computer and the Internet that have changed the world. People are able to communicate and send data from one side of the world to the other and not only via e-mail. There are web cameras that allow people to video conference and applications that allow one to verbally communicate with others. Because of these types of communication, certain expectations have been created in healthcare (Hunter, 2002). From 40 years ago until today, the electronic healthcare system has seen some tremendous advancements. A significant result of these advances is that healthcare professionals have become increasingly dependent upon the availability of systems and reliant upon the correctness of the data that they hold - this, in combination with the overall sensitivity of much of the data, dictates a requirement to preserve information security (Furnell, et al., 1998).

Nowadays, healthcare facilities are migrating towards facilities that provide control, confidentiality, integrity and accountability (TippingPoint, n.d). Healthcare organizations also allow easier, but secure, access to information. There has also been a trend towards allowing patients to access their own information online. Large healthcare networks are also being used to connect more and more medical devices (TippingPoint, n.d). Without defining a security architecture, this would be truly impossible.

2.3 Information Security in Healthcare

A while ago, medical facilities were very open environments where it was not uncommon for interns or medical students to browse through medical records with little to no consent (TippingPoint, n.d.). Hospitals had large sprawling networks that interconnected to other hospitals and clinics and, in some cases; connections were also established to medical colleges and research organizations.

These healthcare organizations are now changing course mainly due to the onslaught of regulations and privacy liability. The obligation to provide proper protection for healthcare information is motivated by increasing legislative requirements, one of which is the well-known Health Insurance Portability and Accountability Act (HIPAA) of 1996. This act is the primary driver for security in healthcare environments (TippingPoint, n.d).

2.3.1 HIPAA

The Healthcare Information Portability and Accountability Act (HIPAA), Public Law 104-191 was signed into law by the President Bill Clinton in the US on August 21, 1996. It contains five titles, namely (Swindom, 2004):

Title I: Healthcare Access, Portability and Renewability
Title II: Preventing Healthcare Fraud and Abuse; Administration Simplification
Title III: Tax-Related Health Provisions
Title IV: Application and Enforcement of Group Health Plan Requirements
Title V: Revenue Offsets

The second of these titles, namely “Preventing Healthcare Fraud and Abuse; Administration Simplification” is applicable in the context of this research. In order to protect the privacy and security of health information as well as encourage efficiency, the Administrative Simplification Compliance Act of HIPAA was passed (Department of Health and Human Services [a], 2006). The Department of Health and Human Services (HHS) has published a set of rules implementing a number of provisions. These provisions include a (Department of Health and Human Services [a], 2006):

- Privacy Rule;
- Electronic Transactions and Code Sets Rule;
- National Identifier requirements for employers, providers and health plans; and
- Security Rule.

Generally, the specifications of HIPAA apply to the following (Department of Health and Human Services [a], 2006):

- Covered Healthcare Providers;
- Health Plans;
- Healthcare Clearinghouses; and
- Medicare Prescription Drug Card Sponsors.

Covered Healthcare Providers are providers of medical or other healthcare services/supplies who transmit health information in electronic form. This transmission of information is usually a transaction for which HHS has adopted a standard (Department of Health and Human Services [a], 2006). Health Plans are individual/group plans that provide/pay for the cost of healthcare (Department of Health and Human Services [a], 2006).

Any public/private entity that practices another entity's healthcare transactions from standard to non-standard format or vice-versa is known as a Healthcare Clearinghouse (Department of Health and Human Services [a], 2006). The last type of covered entity, the Medicare Prescription Drug Card Sponsor, is a non-governmental entity that offers an endorsed discount drug programme (Department of Health and Human Services [a], 2006).

In particular, the Security Rule created by HIPAA will be further investigated as an example of the standards emanating from a legal perspective. This does not negate the importance of the other provisions of the act (particularly in Title II) with regard to security. The other provisions are not discussed as they do not constitute the focus area of this research.

This Security Rule has a number of requirements, one of those being the reviewing and modifying of security policies and procedures on a regular basis (Department of Health and Human Services [f], 2006). The rule "Security Standards for the Protection of Electronic Protected Health Information", otherwise known as the Security Rule, was adopted in order to help implement the requirements of HIPAA.

The HIPAA Security Standards that are used for providing security and help keep information private can be divided into four categories. These four categories include (Department of Health and Human Services [a], 2006):

- Administrative Safeguards;
- Physical Safeguards;
- Technical Safeguards; and
- Organizational Requirements, Policies & Procedures and Documentation Requirements;

Each of these categories will now be briefly discussed.

2.3.1.1 Administrative Safeguards

One of the first steps that an organization can take in order to protect electronic health information is to implement reasonable and appropriate administrative safeguards (Department of Health and Human Services [b], 2006). These safeguards need to establish foundations for a covered entity's security programme. But what exactly are administrative safeguards?

HIPAA's Security Rule defines these administrative safeguards as, "*administrative actions and policies and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.*" (Department of Health and Human Services [b], 2006, p. 2) These safeguards encompass over half of HIPAA's security requirements. To ensure compliance with the Administrative Safeguards standards, an evaluation of currently implemented security controls and a thorough risk analysis must be performed (Department of

Health and Human Services [b], 2006). These safeguards are listed under the Security Rule at § 164.308 (Department of Health and Human Services [b], 2006).

2.3.1.2 Physical Safeguards

Another step in the protection of electronic health information is the use of appropriate physical safeguards for information systems and related equipment and their facilities (Department of Health and Human Services [c], 2006). These physical safeguards are defined by the Security Rule as, "*physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion"* (Department of Health and Human Services [c], 2006, p. 2). When deciding on and implementing physical safeguards, a covered entity must take all physical access to electronic protected health information into account.

These safeguards are listed under the Security Rule at § 164.310 (Department of Health and Human Services [c], 2006).

2.3.1.3 Technical Safeguards

Due to the ever changing technology progressions, technical safeguards are becoming more important. While technology progresses, so does the emergence of new security challenges. In order to reduce risks, both internal and external, covered entities must use technical safeguards (Department of Health and Human Services [d], 2006). The definition of technical safeguards according to the Security Rule is, "*the technology and the policy and procedures for its use that protect electronic protected health information and control access to it*." (Department of Health and Human Services [d], 2006, p. 2)

These safeguards are listed under the Security Rule at § 164.312 (Department of Health and Human Services [d], 2006). It must also be made clear that the Security Rule is based on flexibility, scalability and technology neutrality (Department of Health and Human Services [d], 2006). Therefore, there are no specific types of technology that are suggested for implementation. This allows covered entities to select their own security measures, as long as they are appropriate.

2.3.1.4 Organizational, Policies and Procedures and Documentation Requirements

While the safeguards discussed in Sections 3.1.1 – 3.1.3 comprise the majority of standards and implementation, there are further standards that are listed under the Security Rule at § 164.314, Organization Requirements, and § 164.316, Policies and Procedures and Documentation Requirements (Department of Health and Human Services [e], 2006).

2.3.1.5 Summary of HIPAA Security Rule Standards

The table below summarizes the various sections and subsections of each of the Security Rule safeguards (Department of Health and Human Services [e], 2006, p. 10-11).

Table 2.1: HIPAA Security Rules

Administrative Safeguards			
Standards	**Sections**	**Implementation Specifications** **(R) = Required, (A) = Addressable**	
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)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Healthcare Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(R)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		

Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)
Physical Safeguards			
Standards	**Sections**	**Implementation Specifications (R) = Required, (A) = Addressable**	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)
Technical Safeguards			
Standards	**Sections**	**Implementation Specifications (R) = Required, (A) = Addressable**	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to	(A)

		Authenticate Electronic Protected Health Information	
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)
Organizational Requirements			
Standards	**Sections**	**Implementation Specifications** **(R) = Required, (A) = Addressable**	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plan	§ 164.314(b)(1)	Implementation Specifications	(R)
Policies and Procedures and Documentation Requirements			
Standards	**Sections**	**Implementation Specifications** **(R) = Required, (A) = Addressable**	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

This discussion of the HIPAA and its associated provisions has shown that there are important requirements for security originating from legal sources. While this study will not further investigate the content of laws, but rather standards that deal with security (originating from standards bodies), it recognizes the importance of including provision for legal requirements in a standards-based model for security in healthcare.

2.3.2 Information Security Management

The HIPAA and other laws are recognized as primary drivers for the implementation of proper security measures, because of the legal liability associated with them. However, information security and information security management principles did not necessarily originate due to legal pressures. The legal framework was rather created to force companies to implement proper security principles, for which various standards and guidelines were already in existence. For example, the BS 7799, from which the well-known ISO 17799 (now ISO 27002) standard originated, was published in 1995, before the enactment of the HIPAA. It is, therefore, appropriate to investigate some basic principles in the area of information security and information security management, in order to establish its relevance in healthcare.

Before discussing what an Information Security Management System is, it must be clarified what Information Security is. According to the ISO/IEC 17799: 2005, “Information Security is the protection from a wide range of threats in order to ensure business continuity, minimize business risks and maximize return on investments and business opportunities“. In order to achieve proper Information Security, a suitable set of controls need to be implemented. These controls can take many forms such as in the form of policies, processes, procedures, organizational structures and hardware/software functions. This is known as Information Security Management (ISM). Interestingly, at first glance, the overlap between the HIPAA Security Rule and these ISM principles can be seen.

In order to properly implement Information Security Management, there are certain activities that need to be initiated by healthcare providers as part of managing Information Security (Cooper & Collmann, 2000). These activities, which will be briefly discussed, have been grouped together into a toolkit created by the Work Group on Confidentiality, Privacy and Security that was chartered by the Computer-based Patient Record Institute (CPRI). The toolkit is touted as ensuring the creation and maintenance of a security policy that is compliant with the HIPAA Security and Privacy Standards. The four activities that need to be initiated are (Cooper & Collmann, 2000):

1. Monitoring and adjusting to changing laws, regulations and standards
2. Developing, implementing and continuously updating data-security policies, procedures and practices
3. Enhancing patient understanding of the organization’s information security efforts
4. Institutionalizing responsibility for information security

Each of these activities is subsequently discussed as taken from the overview provided by Cooper and Collmann (, 2000).

2.3.2.1 Monitoring Laws, Regulations and Standards

The CPRI Toolkit provides a large amount of attention to HIPAA-provoked federal activity in health-information security and also provides extensive materials concerning state and professional activities in health-information assurance. Using the resources that are provided by the CPRI Toolkit, healthcare organizations should be able to keep track of the various federal, state and professional requirements in health-information security and privacy with which they must be compliant. This activity of the toolkit is one that never ends as laws, regulations and standards may change.

The recognition of the importance of the legal dimension in healthcare is evident in this toolkit.

2.3.2.2 Updating Health Information Policies, Procedures and Practices

The CPRI Work Group on Confidentiality, Privacy and Security has published a number of booklets on specific topics in health information security. These booklets have been reprinted as one of the chapters of the CPRI Toolkit. These booklets come with samples and case studies showing critical steps that healthcare organizations should take to help implement a health information security policy. The samples include samples of actual security policies that are implemented by eight different healthcare organizations. The chapter also covers topics such as risk assessment, assigning roles and responsibilities, information security training, how to enforce security policies, issues in electronic transmission and a discussion on information technology such as firewalls and encryption.

2.3.2.3 Enhancing Patient Understanding of an Organization's Health Information Security Program

The Department of Health and Human Services (DHHS) suggests that organizations allow patients the right to review and propose corrections to their medical records as well as permitting patients to review a list of disclosures. The toolkit, mentioned above, contains a chapter on procedures and forms on how to responsibly provide these types of services.

It is clear that this third activity is geared towards satisfying the demand for greater accountability in the use of health information.

2.3.2.4 Institutionalizing Sound Security Practices

In order for an organization to properly institutionalize sound security practices, supporting structures need to be placed at all levels of the organization. Support structures that are consistently discussed at security seminars are that the CEO of a company should publicly support an organization's information security program and that confidentiality is everybody's business (Cooper & Collmann, 2000).

Having investigated information security in healthcare and with consideration for the importance of both laws and standards in this area, it is appropriate to briefly discuss the difference between laws and standards.

2.3.3 Laws vs Standards

It is clear that in the healthcare environment, due consideration must be given to both laws and standards in the creation of a secure environment for healthcare applications and data. Internationally, governments are mandating what would otherwise be general best practices to force healthcare organizations to protect their customer information and prevent corporate misdeeds - this has ushered in a new era for running healthcare businesses (Tuyikeze, 2006).

Allaert and Barber provide an interesting discussion on the difference between laws and standards in a paper published in the International Journal of Medical Informatics (2000). They make the point that laws and standards differ from each other during the elaboration process and specifically that some standards may provide a perfect answer to a legal obligation. This can be seen in the HIPAA Act where the implementation thereof is driven through standards defined, for example, as part of the Security Rule (and others). The paper further explains that while respect for the law is mandatory, standards are firmly optional. The following table presents the main differences between laws and standards, as summarized from their paper.

Table 2.2: Differences between Laws and Standards (summarized from Allaert & Barber, 2000)

Differences		
	Laws	**Standards**
Elaboration Process		
How the process is conducted	Democratic	Aristocratic
Organization whose members vote on the implementation	Members of Parliament	Members of the actual Standards Organization
How members are chosen	Elected into office	Appointed
Who decides on the members	The majority of citizens within a country	Professional/Commercial Organizations
		National Standards Organizations
Respective Forces		
Implications of Non-Compliance	Legal	Financial
Driving Force	Mandatory	Market Rules
		Market Needs
		Product Liability
		Service Liability
Conflict versus Cooperation		
When does the one need the other?	When uncontrolled development of technical solutions can lead to incompatibility and interference with the objectives of the law	When a standard needs to be enforced to allow cooperation

From this section, it can be concluded that the objective of this research, which is to propose a standards-based model for security in health information systems, should include a legal dimension. This is further discussed in Chapter 4.

2.4 Conclusion

This chapter has discussed the history of the Health Information System and helped clarify the terminology associated with the storage of electronic health records. Security in the healthcare industry was then discussed from the point-of-view of the legal obligation (where HIPAA was used as an example) and information security management (where the CPRI Toolkit was discussed). Finally, the differences between laws and standards were pointed out as a precursor to the extended discussion on security standards and standards bodies in healthcare in Chapter 3.

Chapter 3. Security Standards in the Healthcare Environment

3.1 Introduction

Standards for Information and Communication Technology (ICT) have been, and continue to be, developed by official standards bodies and have an international, regional or national remit. This chapter will briefly discuss the reasons for standards, a few of the leading standards bodies that are responsible for the development of standards as well as security standards relevant to the healthcare industry. It should be stated that in most cases, it was not possible to gain access to the actual standards that are discussed. The information used to discuss the standards was taken from their standards bodies websites which typically comprised information in summarized format.

3.2 Security Standards

3.2.1 Overview

While there is a main standardization organization (the ISO), there are also other notable standard bodies that are confined to specific areas of the world. Two prominent ones are the American Society for Testing Materials (ASTM) and the Committee for Standardization (CEN) in Europe. While these three organizations are responsible for the majority of standards, including security standards, for the healthcare industry, there is another party that has produced a standard that is used considerably in the Healthcare industry. This standard would be the communication standard and its various versions released by Health Level 7 (HL7).

3.2.2 The Need for Standards

Standards are necessary not only within the healthcare environment, but in all industries. For example, if there was no standard base for light bulbs, then you would have to buy new lights and lamps every time that you changed a light bulb (Smith, 2002). However, within the healthcare informatics environment, many of the applications used have not been designed to exchange information easily (Smith, 2002). This is one of the reasons why there has been a lack of Electronic Health Record implementation as well as integration. Furthermore, Kathleen Smith states that technical standards are needed in healthcare informatics in order to provide sharing of data and information to assist in the performance of healthcare systems.

Within the context of standards bodies, there are two categories of said standard bodies, namely standards-coordinating groups and standards development groups (Smith, 2002). The purpose of standards-coordination groups is to coordinate the formation of technical healthcare informatics standards. Existing standards-coordinating groups include the:

- American National Standards Institute (ANSI);
- Workgroup for Electronic Data Interchange (WEDI);
- National Council for Clinical Laboratory Standards (NCCLS)

The second category of standards bodies are the groups that are formed for the purpose of developing the actual technical standards for the applications that are used in healthcare informatics. A few examples of this category include the:

- National Council for Prescription Drug Programs (NCPDP);
- American Society for Testing and Materials (ASTM) Committee E-31 on Health Informatics;
- Health Industry Business Communications Council (HIBCC)

Each of these groups consists of individuals, vendors and any other interested parties. This chapter will look at the standards that have been created by the second category of standards bodies and specifically those that deal with security and privacy in the healthcare environment.

3.2.3 ASTM Standards

ASTM International **(**ASTM**)** is an international standards developing organization that was formed in 1898 and was originally known as the American Society for Testing and Materials. ASTM International is responsible for developing and publishing voluntary technical standards for a wide range of materials, products, systems, and services. Although ASTM is not a national standards organization, it does support thousands of volunteer technical committees.

While ASTM is responsible for the creation of standards within multiple industries, all of their standards can be grouped into six categories (Wikipedia [b], 2007):

- Standard Specifications that defines the requirements to be satisfied by subject of the standard;
- Standard Test Methods that defines the way a test is performed. The result of the test may be used to assess compliance with a Specification;
- Standard Practices that defines a sequence of operations that, unlike a test, does not produce a result;
- Standard Guides that provides an organized collection of information or series of options that does not recommend a specific course of action;
- Standard Classifications that provides an arrangement or division of materials, products, systems, or services into groups based on similar characteristics such as origin, composition, properties, or use;
- Terminology Standard that provides agreed definitions of terms used in the other standards.

While ASTM is one of the largest standards development groups in the world, ASTM's Committee E-31 develops standards specifically for health information and health information systems (Smith, 2002). The current ranges of standards that have been addressed by ASTM Committee E-31 include EHR architecture, content, portability, format, privacy, security and communications. However, this research will focus on those standards used to provide security and privacy.

There are no special requirements needed for anyone to join ASTM International (ASTM International, 2003). Memberships in most of ASTMs committees are voluntary and are typically initiated by the member's own request.

During 2007 ASTM recorded that it had 30,000 members, of which 1100 of them were organizational members, from more than 120 countries (ASTM International [a], 1996-2008). According to the US Internal Revenue Service, ASTM International is recognized as a nonprofit organization (Wikipedia [b], 2007).

ASTM International offers four different "types" of membership which are (ASTM International [b], 1996-2008):

- Informational Members;
- Participating Members;
- Organizational Members; and
- Student Members.

The Informational members have an interest in the ASTM International standards and any related technical information. However, they choose not to participate on any of their technical committees (ASTM International [b], 1996-2008). They do however want to receive key information regarding standardization issues and to be kept informed of the standards field (ASTM International [b], 1996-2008).

The Participating members are the opposite of the Informational members. They choose to join the ASTM International technical committees and help to actively develop the new standards and revise the existing ones (ASTM International [b], 1996-2008). These members are personally involved in the development of intellectual capital. Participating members can be further classified into four "levels" (ASTM International [b], 1996-2008):

- Users, which include industry and end users;
- Producers, which should constitute less than 50% of every committee in order to meet antitrust laws requirements;
- Consumers;
- And "General Interest", which include academics and consultants.

Unlike the previous two types of members, Organizational members are organizations that choose to support ASTM International by assigning a representative that can take part in the voluntary consensus process as either an Informational or a Participating member (ASTM International [b], 1996-2008). The support of these Organizational members servers the greater public good, while at the same time helping their employee, industry and international trade growth (ASTM International [b], 1996-2008).

Lastly, Student members are those members who are full-time undergraduate or graduate students who receive monthly electronic versions of the ASTM Magazine and the online edition of Access ASTM International quarterly.

Company members are listed alphabetically on the ASTM web site. Member countries are unfortunately not depicted on a map, as was available for CEN and HL7. These maps are shown in Sections 3.2.4 and 3.2.5.

The ASTM standards concerning security and privacy are subsequently addressed.

3.2.3.1 E2085-00a: The Standard Guide on Security Framework for Healthcare Information

This standard describes a framework for the protection of healthcare information. It addresses both storage and transmission of information ("Standards List", n.d.). The framework was designed to accommodate a very large distributed user base, spread over many organizations and advises the use of certain technologies. It makes use of well-known security algorithms, such as SHA-1, triple-DES and others. The development of this standard was considered essential as due to the increased use of computer-based information systems, the ability to share and exchange healthcare information securely is of the utmost importance (ASTM International [a], 2006).

3.2.3.2 E2084: The Standard Specification for Authentication of Healthcare Information using Digital Signatures

This standard covers the use of digital signatures to provide authentication of healthcare information ("Standards List", n.d.). It describes how the components of a digital signature system meet the requirements specified in Guide E 1762, which describes the scope of and requirements for authentication of healthcare information. This includes specifications of allowable signature and hash algorithms, management of public and private keys and specific formats for keys, certificates and signed healthcare documents (ASTM International [b], 2006).

3.2.3.3 E2212-02[a]: The Standard Practice for Healthcare Certificate Policy

This standard addresses the policy for digital signatures that support the authentication, authorization, confidentiality, integrity and non-repudiation requirements of persons and organizations that electronically create or transact health information. There are three types of certificates: one for computerized entities (servers, applications, etc), one for individual persons and the last one for clinical individuals ("Standards List", n.d). "The policy" also covers the definition of healthcare certificates and other healthcare parties involved with digital signatures as well as the appropriate use of the certificates. Other definitions provided are for the general conditions for the issuance of healthcare certificates, certificate formats and profiles and what the requirements for the protection of key material are (ASTM International [c], 2006).

3.2.3.4 E1986-98: The Standard Guide for Information Access Privileges to Health Information

This guide covers the process of granting and maintaining access privileges to health information. It directly addresses the maintenance of confidentiality of personal, provider and organizational data in the healthcare domain ("Standards List", n.d). This guide addresses explicit requirements for granting access privileges to patient-specific health information and applies to all gathering of, use, supervision, preservation, admission, and access of all individual, groups, and organizational data related to health care (ASTM International [e], 2006).

3.2.3.5 E1987-98: The Standard Guide for Individual Rights regarding Health Information

This guide outlines the rights of individuals, both patients and providers, regarding health information and recommends procedures for the exercise of those rights ("Standards List", n.d). This standard is proposed to help strengthen the Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records (E1869). E1869 covers the main principles for confidentiality, privacy, access and security of person identifiable health information. The focus of this standard is computer-based. However E1869 is intended as a base for development of more specific standards and as such does not deal with specific technical requirements (ASTM International [f], 2006). E1987-98 is meant to work in conjunction with E1986-98 (“Standards List”, n.d).

3.2.3.6 E1762-95: Standard Guide for Properties of Electronic Health Records and Record Systems

The standard defines a document structure for use by electronic signature mechanisms as well as defining the characteristics of the electronic signature process itself (“Standards List”, n.d). The standard further characterizes electronic signatures by (Kokolakis, Gritzalis, Katsikas and Ottes, 2002):

- Defining minimum requirements for electronic signature mechanisms.
- Defining signature attributes for use with electronic signature mechanisms.
- Describing acceptable electronic signatures mechanisms and technologies.
- Defining minimum requirements for user identification, access control and other security requirements for electronic signatures.
- Outlining technical details for all electronic signature mechanisms in sufficient detail to allow interoperability between systems supporting the same signature mechanism.

These technical details help interoperability between systems that support the same electronic signature mechanisms. In addition, this standard also helps define requirements for user identification and access control (ASTM International [d], 2006).

3.2.3.7 E2117-00: Standard Guide for Identification and Establishment of a Quality Assurance Program for Medical Transcription

E2117-00 helps establish a quality assurance program to ensure the accuracy of any healthcare documentation. While this standard does institute essential and desirable elements, it is not professed to be an in-depth inventory (ASTM International ^{g}, 2006)

3.2.3.8 E1869-97: Standard Guide for Confidentiality Privacy Access and Data Security Principles for Healthcare Information Including Computer-Based Patient Records

This standard, being focused on computer-based systems, covers the principles for confidentiality, privacy, access and security of person-identifiable health information. However, the principles also apply to health information and patient records that are not in electronic format. E1869-97 provides a basis for the construction of laws, regulations, systems and policies for health information systems and computer-based patient record systems. This guide does not address specific technical requirements as it is intended as a base for development of more specific standards (Kokolakis, Gritzalis, Katsikas and Ottes, 2002)

3.2.3.9 E1902-97: Standard Guide for Management of the Confidentiality and Security of Dictation, Transcription and Transcribed Health Records

This standard covers a broad description of certain steps to be taken by those involved in the process of dictation and transcription of patient care documentation to protect the records. This includes during development, maintenance, transmission, storage and retrieval. This standard supports patients' rights and identifies procedures for preventing breaches of these patient rights. These rights include confidentiality, privacy and secure documentation (Kokolakis, Gritzalis, Katsikas and Ottes, 2002)

3.2.3.10 E1985-98: Standard Guide for User Authentication and Authorization

This standard covers mechanisms that may be used to authenticate Healthcare information users to computer systems, as well as to authorize particular actions by users. These may include access to Healthcare information documents and specific operations on those documents (Kokolakis, Gritzalis, Katsikas and Ottes, 2002).

E1985-98 addresses both centralized and distributed environments, by defining the requirements about the kinds of information which shall be transmitted between systems. The standard also addresses the technical specifications for how to perform user authentication and authorization (Kokolakis, Gritzalis, Katsikas and Ottes, 2002)

This concludes the discussion on the security and privacy-related standards released by ASTM. The focus now shifts to the standards developed by the European Committee for Standardization.

3.2.4 CEN Standards

The European Committee for Standardization, otherwise known as CEN, is a non-profit organization. CENs mission is to provide an infrastructure for the development, maintenance and distribution of coherent sets of standards and specifications (Wikipedia [c], 2007).

CEN was founded in 1961 and has its headquarters in Brussels. It consists of 30 national standards bodies as members who work together to develop voluntary

European standards (EN) in various sectors. These 30 members are from the European Economic Community (ECC) and the European Free Trade Association (EFTA) as well as other countries that are likely to join the European Union (EU) or EFTA in the near future (Wikipedia [c], 2007). CEN contributes to the EUs objective, to promote free trade, the safety of workers and consumers, interoperability of networks, environmental protection, exploitation of research and development programs and public procurement, with voluntary technical standards (European Committee for Standardization, 2007).

While CEN promotes the EUs objectives, it also has its own objectives. These two objectives are (Welcomeurope, 2007):

- To promote voluntary technical harmonization in Europe in conjunction with worldwide bodies and its partners in Europe; and
- To promote the conformity assessment of products and their certification.

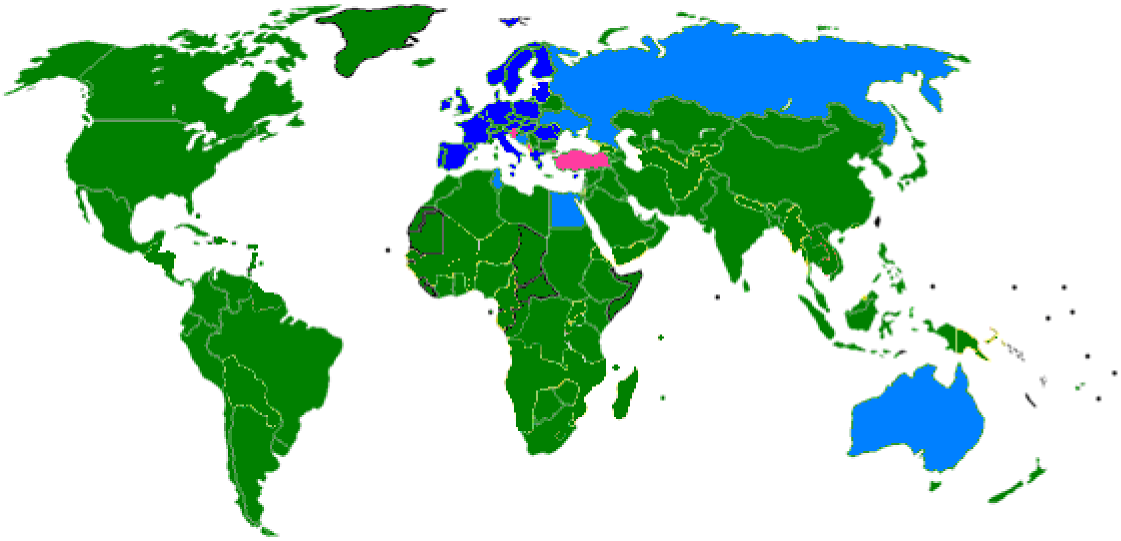
In order for CEN to achieve these objectives, a number of activities need to be performed. These activities are (Welcomeurope, 2007):

- Providing European standards and technical specifications in all areas of economic activity with the exception of electro-technology and telecommunication;
- Providing the infrastructure and process (procedures, information channels and structures) for the development of standards and specifications;
- Defining normative documents such as EN and ENV and other documents (such as CWA) and those for information and transfer of knowledge;
- Giving information and holding training sessions about European standardization and European standards and related fields; and
- Distinguishing conformity assessment and Keymark and other certification marks.

CEN is organized as a ‘horizontal’ organization consisting of a large number of sectors. These sectors are represented in nearly every area that their partners (CENELEC and ETSI) do not represent.

CENs members can be broken up into three different types: Current Members, Affiliates and Partner Standardization Bodies.

Figure 3.1: CEN Members



A map of standards bodies who are CEN members

Key:

■ Current Members

■ Affiliates

■ Partner Standardization Bodies

■ Non-Members

3.2.4.1 ENV12388: The Algorithm for Digital Signature Services in Health Care

This is a European standard that defines the algorithm used for digital signatures in medical information exchange. It is used in the Secure Medical Record Information Communication (SEMRIC) Project. It is required to achieve legal acceptability of the information exchange (American National Standards Institute [a], 2006). Digital signature techniques are also essential parts of several security services of great importance for the Healthcare sector (Kokolakis, Gritzalis, Katsikas and Ottes, 2002). The functionality of the use of this algorithm requires additional specifications of protocol elements related to the application requirements (American National Standards Institute [a], 2006). The algorithm that is defined in this standard is the RSA algorithm (Kokolakis, Gritzalis, Katsikas and Ottes, 2002).

3.2.4.2 ENV13608: The Security for Healthcare Communication Standard

This standard specifies a methodology for defining, expressing and selecting a communication protection profile specification. ENV13608 also defines a standard way of securing healthcare objects (so that they can be transported over open, unsecured networks, or stored in open unsecured repositories) and specifies services and methods for securing interactive communications used within health care (including reservation of data integrity, confidentiality with respect to the data being exchanged and accountability in terms of authentication of one or both conversing parties) (American National Standards Institute [b], 2006).

3.2.4.3 prENV12251: Secure User Identification for Healthcare; Identification and Authentication by Passwords-Management and Security

The objective of this European Pre-standard is to improve the authentication of individuals wishing to utilize a Healthcare IT system, by strengthening the automatic software procedures associated with the management of user identifiers and passwords, without resorting to additional hardware facilities. The authors of the pre-standard admit that other technologies, such as chip cards and biometrics, have been introduced and will eventually phase out the use of passwords. However, they argue that in the mean time it is necessary to facilitate the secure use of passwords in Healthcare IT systems. Finally, this standard consists of several requirements regarding the construction and management of user identifiers and passwords (Kokolakis, Gritzalis, Katsikas and Ottes, 2002)

3.2.4.4 ENV12924: Security Categorization and Protection for Healthcare Information Systems

This standard aims to specify a method of categorizing Health Information Systems in the context of security and to specify a corresponding set of protective requirements. The systems are categorized according to the Availability, Confidentiality and Integrity attributes of the information. The category is determined according to the value given to each of those attributes. Six of those combinations are chosen to create six categories (Kokolakis, Gritzalis, Katsikas and Ottes, 2002). The discussion of this standard is further expanded in Chapter 4, Section 4.2.2.

3.2.5 HL7

Health Level 7, Inc. (HL7) is a non-profit standards developing organization which, when compared to the two other standards bodies, is moderately new as it was founded in 1987. HL7 is involved in the development of international healthcare standards. The acronym “HL7” is also used as a reference to some of their specific standards (eg. HL7 v2.x). HL7 helps provide standards for the exchange, management and integration of data that supports clinical patient care and the management, delivery and evaluation of healthcare services. HL7 is involved in the standardization of many interfaces between healthcare systems all over the world. The goal of HL7 is to provide the largest possible measure of standardization while providing openness for local variations (NHS, 2001).

HL7 collaborates with other standards development organizations to encourage supportive and compatible standards. It promotes standards to help increase the effectiveness and efficiency of healthcare delivery. Another reason that HL7 collaborates is to ensure that their standards are meeting real-world requirements as well as enabling them to initiate the development of appropriate standards.

The membership of the HL7 community takes the form of a global organization and country-specific affiliate organizations with its main headquarters being established in Ann Harbor, Michigan, U.S. HL7’s global membership can be broken down into the following percentages: 45% are located within Europe; 35% in North America; 15% in Asia-Oceania and the last 5% covers elsewhere (Health Level 7, 2007). While HL7’s membership takes the form of a global organization, its organizational structure differs. A Board of Directors manages HL7 and consists of eleven positions, eight of which are elected and the other three are appointed. The rest of the members form a collective “Working Group” which is responsible for defining standard protocol. This “Working Group” is composed of (Wikipedia [a], 2007):

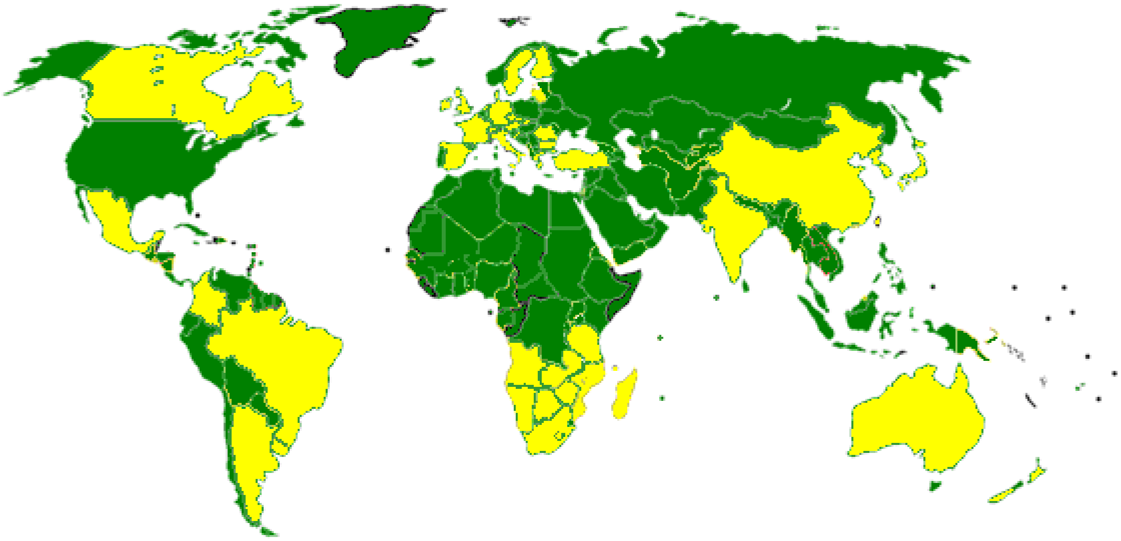
- Standing Administrative committees who focus on organizational or promotional activities, such as Education, Implementation, Marketing, Outreach Committee for Clinical Research, Publishing and Performance Improvement and Tooling;

- Special interest groups serve as a test bed for exploring new areas that may need coverage in HL7's published standards, such as Clinical Genomics, Clinical Guidelines, Community Based Health Services, etc;
- Technical committees are directly responsible for the content of the Standards, framing the actual language of the specifications.

HL7 is involved at the application layer of the communication model between open systems and specifies communication contents and exchange formats. The HL7 communication standard was specifically developed for use in the healthcare environment and enables communication between nearly all institutions in most fields of healthcare. In the past, there have been two versions of this communication standard and a third one has recently been developed (NHS, 2001), namely HL7 Version 3.

Figure 3.2 displays the member countries of HL7.

Figure 3.2: HL7 Members



A map of standards bodies who are HL7 members

Key:

🟨 Members

🟩 Non-Members

3.2.5.1 HL7 Version 3.0

Version 3.0 creates messages by utilizing a formalized methodology. This methodology involves the development of a variety of models, including the Reference Information Model (RIM). The methodology also calls for the creation of a model which captures information flows and defines application roles needed to support messages. This is known as the Interaction Model (NHS, 2001)

Previously HL7 messages supported a single format using ASCII encoding. However, HL7 v3 can use an expanded suite of data interchange formats. Version 3 will support XML as well as the component technologies of ActiveX and CORBA (NHS, 2001). The HL7 Version 3 Messaging is based on a formal methodology, the HL7 Development Framework (HDF), and object orientated principles. To further improve the messaging used for Version 3, the HL7 Vocabulary Technical Committee has developed a way for HL7 specifications to draw upon codes and vocabularies from a variety of sources. This ensures that that those systems that implement HL7 specifications have an unmistakable understanding of the code sources code value domains that they are using. HL7 Messaging is largely transported by Microsoft's Minimum Lower Layer Protocol (MLLP).

The HL7 Development Framework is continuously evolving. This framework seeks to develop conditions to assist interoperability between healthcare systems. It should be made clear that the HDF is not only used for messaging, but is also used to document the processes, tools, actors, rules and artifacts relevant to development of all other HL7 standard specifications. HL7 hopes to encompass all standard specifications within the HDF.

HL7 Version 3 also uses a protocol called the Clinical Context Object Workgroup (CCOW). This protocol was designed to allow dissimilar systems to synchronize both in real-time and at the user-interface level. It is able to this as it is vendor independent and allows the applications to display information in a unified way. The CCOW protocol makes possible a process called “Context Management.” This is the process of using particular “subjects” of interest to ‘virtually’ link different applications so that it appears to the user that they operate in an integrated, consistent way. The “subjects” of interest may include things such as: users, patients, clinical encounters, charged items, etc. The CCOW standard also attempts to facilitate a type of near “plug-and-play” interoperability.

3.2.6 ISO Standards

The International Organization for Standardization (ISO) forms a specialized system for worldwide standardization and consists of a worldwide federation of national bodies (Smith, 2002). ISO was founded on 23 February 1947 and is headquartered in Geneva, Switzerland (ISO [a], 2007). The national bodies that are members of ISO participate in the development of International Standards through technical committees that are established by the respective organization to deal with particular fields of technical activity (ISO 17799, 2005). The main objective of ISO is to: “promote the development of world-wide standardization and related activities” (Smith, 2002). It should be pointed out that the term ISO is not an acronym. Rather ISO was taken from the Greek word “isos” which means equal. ISO was chosen as the definition of the Greek word “isos” fits in with ISO’s aim: “to equalize and standardize across cultures” (ISO, 2008).

ISO defines itself as a non-governmental organization. However, ISO does have the ability that the standards that they create often become law, making them more powerful than most governmental organizations. Essentially ISO performs as an association with strong governmental links (ISO [a], 2007).

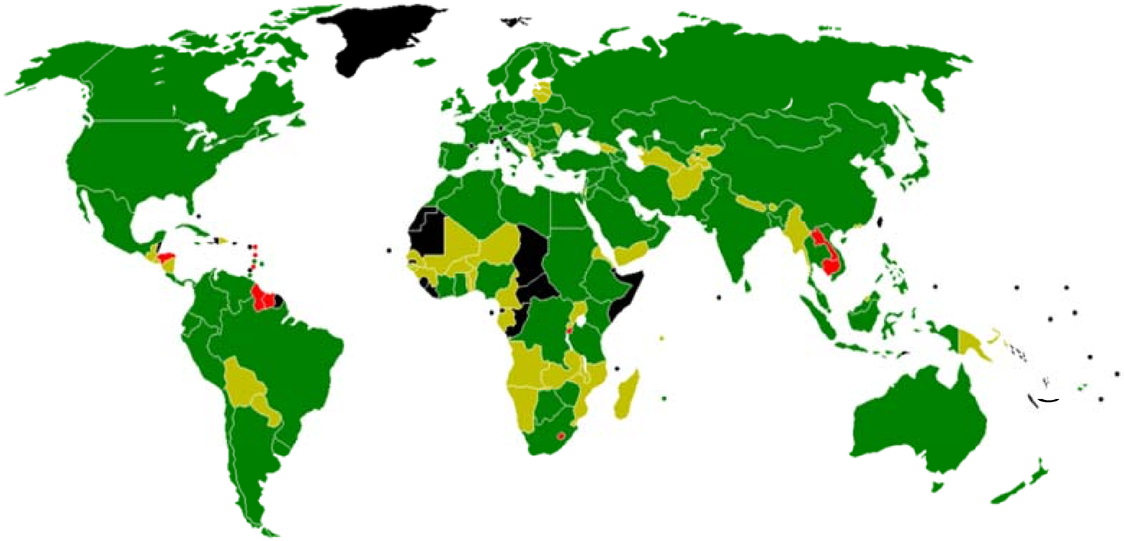
Out of the 195 countries across the globe, ISO has 157 national members (ISO [b], 2007). Members of ISO can either be participating members or observing members and can be broken up into three categories:

- Member bodies;
- Correspondent members;
- Subscriber members;

The Member bodies are those national bodies that are considered the most representative standards body within a country. These members are the only members that have voting rights in the ISO organization. The Correspondent members are those countries that may be informed about the work that ISO has been doing, however they do not participate in circulating the standards. This is because these members do not have their own standards organizations. Finally, Subscriber members are small economy countries. However, they are able to track the standards development by paying reduced membership fees.

Figure 3.3 displays the countries that are members of ISO as well as what type of members they are.

Figure 3.3: ISO Members



A map of standards bodies who are ISO members

Key:

🟩 Members

🟨 Correspondent members

🟥 Subscriber members

⬛ Other places with an ISO 3166-1 code who aren't members of ISO

ISO includes 223 technical committees, two of which are the ISO/TC 212 and the ISO/TC 215. The ISO/TC 212 committee deals with “Standardization and guidance in the field of laboratory medicine and in vitro diagnostic test systems” (ISO/TC 212, 2002, para. 1). A few examples of their work area would be quality management, pre- and post-analytical procedures, analytical performance, laboratory safety, reference systems and quality assurance. On the other hand, ISO/TC 215 was established in 1998 in order to address “Standardization in the field of information for health, and Health Information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems”. Another objective of this committee is to ensure compatibility of data for comparative statistical purposes and to reduce duplication of effort and redundancies (ISO/TC 215 Working Group 3, n.d.).

Other ISO technical committees have also been responsible for releasing standards dealing with security of electronic information both on their own, as well as in cooperation with other standards bodies. The standards developed which are relevant to the healthcare environment, are: the ISO 22857, the ISO/TR 21089, the ISO/TR 22221, the ISO/TS 17090, the ISO/TS 21091 and the ISO/TS 22600.

3.2.6.1 ISO 22857: Guidelines on Data Protection to Facilitate Trans-Border Flows of Personal Health Information

ISO 22857 was published in 2004 to assist in providing guidelines on data protection requirements. This standard helps facilitate the transfer of personal health information across national borders and covers both the data protection principles and the security policy to ensure compliance. This standard aims to facilitate international health-related applications involving the transfer of personal health data. It looks to provide data subjects with assurance that health data relating to them will be adequately protected when sent to another country (International Organization for Standardization [a], 2007).

While national privacy and data protection requirements can not only vary substantially, but can also change relatively quickly, this standard tends to generally encompass some of the more stringent of both international as well as national requirements. However, this standard still comprises a minimum (International Organization for Standardization [a], 2007).

3.2.6.2 ISO/TR 21089: Trusted End-to-End Information Flows

This standard attempts to provide trusted end-to-end information flow healthcare records by offering guidelines. ISO/TR 21089 also guides to the key trace points and audit events in the electronic entity/act record lifestyle. This standard also offers the recommendation of best practices for healthcare providers as well as health record stewards, software developers and vendors, end users and other stakeholders (International Organization for Standardization [b], 2007).

3.2.6.3 ISO/TR 22221: Good Principles and Practices for a Clinical Data Warehouse

ISO/TR 22221 is a standard that was recently published in 2006 and its main focus being that of clinical databases which maintain or access clinical data for secondary purposes. Its goal is to define principles and practices in the creation, use, maintenance and protection of clinical databases. This standard complements contemporary security standards in development and addresses secondary uses of the EHR such as quality assurance. The standard describes principles and practices for security considerations for a clinical database. These security issues are further extended with regard to the EHR in population-based application (International Organization for Standardization [c], 2007).

3.2.6.4 ISO/TS 17090: Public Key Infrastructure

This standard is broken up into three sections; each describing a different aspect of a public key infrastructure.

ISO/TS 17090-1 defines the basic concepts of a healthcare public key infrastructure (PKI). It also helps to provide a scheme of interoperability requirements to establish a PKI enabled secure communication of health information. This standard introduces public key cryptography and the basic components of a PKI. It further discusses digital certificates, such as public key identity and associated attribute certificates. These certificates can be used by certification authority hierarchies and bridging structures (International Organization for Standardization [d], 2007).

ISO/TS 17090-2 covers the specification of certificate profiles that are required for interchanging healthcare information. This can be applied to healthcare information interchange within a single organization, between different organizations and across jurisdictional boundaries. It also focuses on specific healthcare issues relating to certificate profiles (International Organization for Standardization [e], 2007).

ISO/TS 17090-3 is not a technical standard, but rather focuses on guidelines for certificate management such as the structure and minimum requirements for certificate profiles and associated certification practice statements (International Organization for Standardization [f], 2007).

3.2.6.5 ISO/TS 21091: Directory Services for Security, Communications and Identification of Professionals and Patients

ISO/TS 21091 was published in 2005 to provide the minimum specifications for directory services for healthcare. This standard is a technical standard that helps provide common directory information and services to allow the secure exchange of healthcare information over the public networks. This standard anticipates the support of inter-enterprise, inter-jurisdiction and international communication between various “communities”. It must also be mentioned that the healthcare directory that this standard attempts to help create, will only support standard LDAP Client searches (International Organization for Standardization [g], 2007).

3.2.6.6 ISO/TS 22600: Privilege Management and Access Control

ISO/TS 22600-1 as well as ISO/TS 22600-2 were both released in 2006 and are meant to help support the needs of healthcare information sharing across unaffiliated providers of healthcare organizations as well as health insurance companies together with their patients, staff members and trading partners. They both also support collaboration between several authorization managers (International Organization for Standardization [h], 2007).

While ISO/TS 22600-1 provides more of an overview for this standard, 22600-2 delves deeper into the formal models used. This part of the standard introduces the various models such as the (International Organization for Standardization [i], 2007):

- Domain Model;
- Document Model;
- Policy Model;
- Role Model;
- Authorization Model;
- Delegation Model;
- Control Model;
- Access Control Model

The Access Control Model can be used to help provide security.

3.3 Conclusion

Interest in standards has increased significantly in this decade as more and more people became aware of the necessity for standards for realization of an adequate infrastructure for healthcare reform and with the heightened interest in a national information highway (Hammond, 1995). This has led to a proliferation in standards, including standards addressing security and privacy in healthcare.

In this chapter, several security standards relating to healthcare information from four prominent standards bodies (ASTM, CEN, HL7 and ISO), were discussed, with the objective of establishing the status quo of security standards in healthcare. It should be mentioned, however, that the list of standards that were discussed is not necessarily exhaustive. There may be additional standards which were not accessed during the literature study (in some cases due to limited access allowed by the standards bodies).

In the next chapter, the information gathered so far is incorporated in a standards-based security model for health information systems.

Chapter 4: A Standards-Based Security Model for Health Information Systems

4.1 Introduction

In the previous chapter, a number of high-ranking standards bodies were discussed. Those standards bodies provide, amongst others, the healthcare industry with standards to assist organizations to become more efficient and reliable. Amongst these standards are standards dealing with the security of information that is stored in electronic healthcare systems. This chapter introduces a standards-based security model for health information systems to ensure that such standards are applied in a manner that contributes to securing the healthcare environment as a whole.

4.2 The Standards-Based Security Model

4.2.1 Introduction

The diagram (Figure 4.3), which can be found as a fold-out at the end of the chapter, shows a diagrammatic representation of the model. The model can be broken up into various "layers" of participation which include:

1. The Health Information System Standards, which provide a security categorization model for the various sub-systems (SS-1, SS-2, … SS-N) of the HIS;
2. The Technical and Administrative Standards, depicted as a circle encompassing the HIS, which protect the Health Information System and the data it stores for the sub-systems;

3. The Information Security Management System Standards, depicted as a circle around both the HIS and the technical and administrative standards layers, which serve as an ISMS for the entire Healthcare Environment; and
4. The Inter- and Intra-Health Information System Communication Standards, which facilitate flow of data between HISs.

Each of these layers will be discussed in subsequent sections of this chapter.

4.2.2 The Health Information System Standards Layer

In Figure 4.3, the Health Information System is depicted as the central point of the security model. As defined in Chapter 2, the HISs are what the healthcare environment will typically use to perform their jobs and store any and all patient information. As such, these HISs cannot be a single system that doctors and staff use. Rather, the HIS will be composed of multiple sub-systems that each performs their own function separately from the other sub-systems. For example, there may be a sub-system that deals exclusively with patient registration and identification. This sub-system should function completely separately from a sub-system that is used to extract specific patient information.

Each of the sub-systems contained in the HIS can be categorized according to a security categorization model and analyzed to include the different environmental and connectivity factors that are found in the ENV12924 standard, which was briefly introduced in Chapter 3, viz (Louwerse, 2002):

1. Security category;
2. Physical environment;
3. Physical connectivity; and
4. Logical connectivity.

The subsequent sections explain how these categories are applied to categorize the HIS environment from a security perspective, based on the recommendations of the ENV12924 standard and summarized from Louwerse (2002).

4.2.2.1 Security Category

Within the security category, there are six defined security categories. These categories correlate back to the C.I.A. Triangle and the degree of importance for each "side" of the triangle. The categories are displayed within the following table.

Table 4.1: Security Categories (Louwerse, 2002)

Category	Availability	Confidentiality	Integrity
I	Non-Critical	Sensitive	Non-Critical
II	Non-Critical	Sensitive	Critical
III	Critical	Sensitive	Critical
IV	Non-Critical	Very Sensitive	Non-Critical
V	Non-Critical	Very Sensitive	Critical
VI	Critical	Very Sensitive	Critical
None	..	Non- sensitive	..

The sub-systems are categorized according to the following:

- Sub-systems that handle sensitive data that does not require integrity and availability are categorized under category one.
- Sub-systems that handle sensitive data as well as requiring integrity, but not focusing on availability are categorized under category two.
- Sub-systems that handle sensitive data and require both availability and integrity are categorized under category three.

- Sub-systems that do not require integrity and availability but hold very sensitive data are categorized under category four.
- Sub-systems that are not focused on availability but hold very sensitive data as well as requiring integrity are categorized under category five.
- Sub-systems that require both availability and integrity and hold very sensitive data are categorized under category six.
- Any other sub-systems are not categorized.

4.2.2.2 Physical Environment

While the previous section covers the security-specific aspects needed to categorize the HIS sub-systems, attention must also be paid to the physical security aspect, aka as the physical environment, in which the servers and databases are stored.

The physical environments assumption results are summarized in Table 4.2:

Table 4.2: Physical Environment (Louwerse, 2002)

PEA	Physical Environment Assumptions
1	No easy access, not remote from security supervision
2	No easy access, remote from security supervision
3	Staff present while public present, not remote from security supervision when public not present
4	Staff present while public present, remote from security supervision when public not present
5	Not always staff present while public are present, not remote form security supervision when public not present
6	Not always staff present while public are present, remote form security supervision when public not present

4.2.2.3 Physical Connectivity

The physical connectivity categorization covers the physical cables that are used to connect the servers and PCs storing the information for the Health Information System.

4.2.2.4 Logical Connectivity

Logical connectivity refers to how the equipment is “logically” connected to the healthcare network. The network would appear to be made up of various network domains with each domain having a “security policy” that governs the equipment within those domains.

The logical connectivity assumption results are depicted in Table 4.3:

Table 4.3: Logical Connectivity (Louwerse, 2002)

LCA	Logical Connectivity Assumptions
1	All parts of the system belong to one security domain
2	More than one security domain, but some HCE
3	Some components controlled by external domains

Having concluded the application of a security categorization exercise, the model presented in this chapter proposes that the next layer, technical and administrative standards, be used to fulfill the requirements posed by the security categorization exercise.

4.2.3 The Technical and Administrative Standards Layer

It is clear that within an organization, there are two elements that contribute to effectively and efficiently implementing information security. The first element would be the implementation of technology to improve security. Essentially this element is the “how” of protecting the information. An example would be the use of encryption mechanisms or password access to information. These are collectively referred to as technical standards in the model. The second element would focus more on the administrative side of an organization and essentially covers “what” must be done to protect the information. This element would deal with the policies and procedures that employees should follow in order to guarantee security. This can, for example, deal with legislative issues ensuring compliance and conducting risk assessments. These are collectively referred to as administrative standards in the model.

Therefore, the model proposes that security standards that do not fall in the HIS, ISMS or communication standards layers, reside in the technical and administrative standards layer. An example of a technical security standard is the ASTM standard E2084: The Standard Specification for Authentication of Healthcare Information using Digital Signatures. This standard deals with the use of digital signatures to help provide authentication of the healthcare information being stored and clearly specifies “how” authentication should be done. An example of a standard that falls into the “what” (administrative) standards is the ASTM standard E1986-98: The Standard Guide for Information Access Privileges to Health Information. The access privileges a user has within a healthcare system are covered by this standard. This type of decision has to be made by management rather than a technical mechanism.

In the model, the administrative half of this layer is depicted by a dotted outside line. The dotted line indicates that there is an overlap between the administrative half of this layer and the Information Security Management System standards layer. Due to the Information Security Management System layer dealing with managerial aspects in order to manage information security it is fairly obvious that the layer may take on an administrative role to achieve its objectives. Thus, the administrative standards layer cannot be completely separated from the ISMS Standards layer.

4.2.4 The Information Security Management System Standards Layer

There is no single silver bullet for information security – this means that information security can only be successfully and effectively implemented in a company, if all the constituting dimensions are implemented in a holistic and comprehensive way (von Solms & von Solms, 2007). It is widely touted that information security cannot be implemented in an ad hoc fashion using technical solutions only; therefore, the model proposes the ISMS layer, which ensures that security is addressed in a holistic and comprehensive way.

Three standards will be discussed as applicable in this layer, namely the ISO 17799 (envisaged ISO 27002), the ISO 27001 and the "Draft Standard for High Level Security Policies for Healthcare Establishments".

The ISO 17799 standard was adopted from the previously created standard BS 7799: Part 1 (von Solms & von Solms, 2007). BS 7799 was accepted by the British Standards Institute (BSI) in 1995 (von Solms & von Solms, 2007). Towards the end of the 1990s, a second part of BS 7799 was released in order to specify the process to be followed in order to become BS 7799 compliant (von Solms & von Solms, 2007). ISO 17799/BS 7799: Part 2 has been renamed ISO 27001 and in 2008, ISO plans to rename ISO 17799 to ISO 27002. ISO 17799 is discussed in section 4.2.4.1 and the ISO 27001 is discussed in section 4.2.4.2.

ISO 17799 (formerly BS 7799: Part 1) is a 'guideline' document and gives advice as to what companies should have in place in order to follow 'best practices' for their Information Security Management (S.H von Solms & R. von Solms, 2007). Conversely, the ISO 27001 is rather different. ISO 27001 (formerly BS 7799: Part 2) is a very specific and strict standard that spells out what a company must comply with, in detail, in order to be officially certified against ISO 17799 (von Solms & von Solms, 2007).

So while ISO 17799, in essence, states that “this aspect is good to have in place and if the company wants to implement it, they can”, ISO 27001 states that “this aspect is compulsory and must be implemented in order for the company to be certified”. Currently, there are a large number of international as well as national companies that use and abide by the ISO 17799 Standard (von Solms & von Solms, 2007). ISO 27001, on the other hand, is not as widely adopted thus having fewer companies actually taking the next step and preventing themselves from becoming formally certified (von Solms & von Solms, 2007).

4.2.4.1 ISO 17799

The ISO 17799 standard includes 11 security control clauses that can be used to ensure Information Security.

These control clauses are (ISO 17799, 2005):

a) Security policy;
b) Organizing information security;
c) Asset management;
d) Human resources security;
e) Physical and environmental security;
f) Communications and operations management;
g) Access control;
h) Information systems acquisition, development and maintenance;
i) Information security incident management;
j) Business continuity management;
k) Compliance.

There will be a brief discussion on the objectives of each clause. The discussion is based on information from the ISO/IEC 17799:2005 edition.

4.2.4.1.1 Information Security Policy

The objective of the information security policy is to provide management with direction and support for information security in accordance with business requirements and relevant laws and regulations.

4.2.4.1.2 Organizing Information Security

This clause has two objectives. The first objective is to manage information security within the organization, while the other objective is to maintain the security of the organization's information and information processing facilities that are accessed, process, communicated to, or managed by external parties.

4.2.4.1.3 Asset Management

Asset management deals with the responsibility for assets, whose objective is to achieve and maintain appropriate protection of organizational assets, and informational classification, whose objective is to ensure that information receives an appropriate level of protection.

4.2.4.1.4 Human Resource Security

Human resource security will ensure that, prior to employment, employees, contractors and third-party users understand their responsibilities and are suitable for the roles they are considered for and to reduce the risk of theft, fraud or misuse of facilities.

During employment, this clause is meant to ensure that employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities and are equipped to support organizational security policy in the course of their normal work and to reduce the risk of human error.

When employees, contractors and third-party users exit an organization or change employment, this clause will ensure that it is done so in an orderly manner.

4.2.4.1.5 Physical and Environmental Security

The securing areas section of this clause covers the prevention of unauthorized physical access, damage and interference to the organization's premises and information. The security of equipment section is used to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

4.2.4.1.6 Communications and Operations Management

This clause of has the following objectives:

- To ensure the correct and secure operation of information processing facilities;
- To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements;
- To minimize the risk of system failures;
- To protect the integrity of software and information;
- To maintain the integrity and availability of information and information processing facilities;
- To ensure the protection of information in networks and the protection of the supporting infrastructure;
- To prevent unauthorized disclosure, modification, removal or destruction of assets and interruption to business activities;

- To maintain the security of information and software exchanged within an organization and with any external entity;
- To ensure the security of electronic commerce services and their secure use;
- To detect unauthorized information processing activities.

4.2.4.1.7 Access Control

The access control clause deals with the following objectives:

- To control access to information;
- To ensure authorized user access and to prevent unauthorized access to information systems;
- To prevent unauthorized user access and compromise or theft of information and information processing facilities;
- To prevent unauthorized access to networked services;
- To prevent unauthorized access to operating systems;
- To prevent unauthorized access to information held in application systems;
- To ensure information security when using mobile computing and teleworking facilities.

4.2.4.1.8 Information Systems Acquisition, Development and Maintenance

This clause achieves the following objectives:

- To ensure that security is an integral part of information systems;
- To prevent errors, loss, unauthorized modifications or misuse of information in appliances;
- To protect the confidentiality, authenticity or integrity of information by cryptographic means;

- To ensure the security of system files;
- To maintain the security of application system software and information;
- To reduce risks resulting from exploitation of published technical vulnerabilities.

4.2.4.1.9 Information Security Incident Management

This clause has two different objectives to achieve. The first is to ensure that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

The second objective is to ensure a consistent and effective approach is applied to the management of information security incidents.

4.2.4.1.10 Business Continuity Management

The objective of this clause is 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.

4.2.4.1.11 Compliance

Compliance covers legal compliance, whose objective is to avoid breaches of any law, statutory, regulatory, or contractual obligations and of any security requirements; security policy compliance, whose objective is to ensure compliance of systems with organizational security policies and standards, as well as making considerations for information systems audits, whose objective is to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

The importance of the legal dimension was previously discussed in Chapter 2, when the Health Insurance Portability and Accountability Act was discussed. The model proposed in this dissertation acknowledges the importance of the legal dimension and sees it as part of the ISMS layer of the model. Thus, compliance with relevant laws (from a security perspective) will thus form part of the information security management efforts, which also encourages a holistic approach.

4.2.4.2 ISO 27001

The ISO 27001 is intended to be used in conjunction with ISO/IEC 27002 (ISO 17799), the Code of Practice for Information Security Management. Organizations that implement an ISMS in accordance with the best practice advice in ISO/IEC 27002 are likely, simultaneously, to meet the requirements of ISO/IEC 27001, but certification is entirely optional (Wikipedia [d], 2007).

The PDCA (Plan-Do-Check-Act) model is central to the ISO 27001. It is not unique to ISO 27001, or to information security, but rather a simple approach to developing and improving an organization's management system ("ISO27001 CENTRAL", 2004). It is commonly adopted for implementation of an ISMS using the ISO 27001. The meaning of each letter in the acronym PDCA is (Wikipedia [e], 2007):

PLAN

Establish the objectives and processes necessary to deliver results in accordance with the specifications.

DO

Implement the processes.

CHECK

Monitor and evaluate the processes and results against objectives and specifications and report the outcome.

ACT

Apply actions to the outcome for necessary improvement. This means reviewing all steps (Plan, Do, Check, Act) and modifying the process to improve it before its next implementation.

It is clear, therefore, that the implementation of an ISMS, using a PDCA cycle, is a continuous process. The standard also demands specific strict documentation requirements for the ISMS, management responsibility towards the ISMS, management review of the ISMS and continual improvement of the ISMS (von Solms & von Solms, 2007).

4.2.4.3 Draft Standard for High-Level Security Policies for Healthcare Establishments

This draft standard has been prepared by the MEDSEC consortium to be submitted to CEN/TC251 for consideration and is discussed in a paper written by Kokolakis, Gritzalis & Katsikas in 2002. As such, most of the information conferred in this section will be from this paper.

This planned standard is designed to apply to those information systems, whether they are automated or not, which process personal health information. The draft standard will also apply to all forms of health information (both soft and hard copies) as well as all systems that process health information, regardless of the nature and purpose of that processing. The security policy framework is conceptually viewed at four levels of abstraction. These four levels are: Generic Principles, Principles, Guidelines and Measures (Kokolakis, Gritzalis, & Katsikas, 2002).

Generic principles are used to govern security and privacy of personal health information and of any HISs that process this type of information. It is a good idea to base security policies developed for HISs on a set of generic principles. Principles result when generic principles are considered under a specific administrative environment. Guidelines are specific operational steps that should be followed by an HCE staff member. These result when principles are considered within a specific technological environment. Measures result when guidelines are considered within a specific installation environment (Kokolakis, Gritzalis, & Katsikas, 2002).

Each of these “levels” has a type of dependency. Generic principles are society and culture-dependant, principles are administration-dependant, guidelines are technology-dependant and measures are installation-dependant (Kokolakis, Gritzalis, & Katsikas, 2002).

The draft standard consists of nine principles and guidelines, these being (Kokolakis, Gritzalis, & Katsikas, 2002):

- IS security policy;
- Contractual regulations;
- Management of IS security;
- Education awareness;
- Limited information circulation;
- Data subject’s rights;
- Quality of health information;
- Medical and epidemiological research;
- Security regulations.

Each of these principles/guidelines will now be briefly discussed.

4.2.4.3.1 IS Security Policy

According to the draft standards P100: “Every healthcare establishment should adopt an Information Systems Security Policy, regarding the protection of personal health information and the systems that process it.” (Kokolakis, Gritzalis, & Katsikas, 2002, p. 28).

4.2.4.3.2 Contractual Regulations

P200 of the draft standard states that: “The duties and responsibilities of all individuals employed or working on behalf of every HCE, which are relevant to information security and privacy aspects, should be described in the written contract between the HCE and every member of the staff or each contractor.” (Kokolakis, Gritzalis, & Katsikas, 2002, p. 29).

4.2.4.3.3 Management of IS

This third principle contains P300, which states that: “An effective and efficient organizational structure should be implemented for the monitoring and enforcement of the Information Systems Security Policy.” (Kokolakis, Gritzalis, & Katsikas, 2002, p. 31).

4.2.4.3.4 Education Awareness

Education awareness is covered by P400. According to this principle, “The importance of ensuring the security and privacy of individual rights and freedoms in the health field should be raised between both the healthcare establishment staff and the public.” (Kokolakis, Gritzalis, & Katsikas, 2002, p. 33).

4.2.4.3.5 Limited Information Circulation

According to this principle's guideline (P500), "Personal health information is considered to be sensitive and should be protected with care." The guideline continues by declaring that: "Circulation of personal health information should be made according to the provisions set out in the Information Systems Security Policy and according to specific guidelines." (Kokolakis, Gritzalis, & Katsikas, 2002, p. 34).

4.2.4.3.6 Data Subject's Rights

The data subject's rights are formulated as: "Information systems in the healthcare field exist and operate with a view toward serving patients according to the human rights and freedoms and according to the legal provisions pertaining to civil rights." All of this is classified under principle P600 (Kokolakis, Gritzalis, & Katsikas, 2002, p. 36).

4.2.4.3.7 Quality of Health Information

According to P700, in order for quality of health information assurance, "Personal health information should be processed in a way that ensures a high quality (integrity and accuracy) level." (Kokolakis, Gritzalis, & Katsikas, 2002, p. 40).

4.2.4.3.8 Medical and Epidemiological Research

Principle P800 of the medical and epidemiological research guideline states that, "Requests for personal health information – and for a purpose previously unspecified – could be addressed, provided that the informed and freely given consent of the person concerned has been obtained and that he/she has been informed about his/her rights of refusal, access and correlation." (Kokolakis, Gritzalis, & Katsikas, 2002, p. 40).

4.2.4.3.9 Security Regulations

The security regulation guidelines are enclosed within P900. This guideline is meant to prevent a number of effects and is defined as “Appropriate measures should be taken for the security of health information and for the protection of the privacy of the data subjects, aiming at preventing (Kokolakis, Gritzalis, & Katsikas, 2002, p. 41):

1. Denial of the services of the system;
2. Accidental or deliberate destruction of data;
3. Unauthorized access to, or disclosure of data;
4. Accidental or deliberate alteration of data; and
5. Unauthorized creation of data.

P900 further states that, “These measures comprise technical, organizational, personnel management (procedural) and physical security measures.” (Kokolakis, Gritzalis, & Katsikas, 2002, p. 41).

4.2.4.4 Similarities and Differences between the ISO 17799 and the Draft Standard

Having discussed Information Security Management Systems from both the ISO: 17799 and the Draft Standards point-of-view, there are certain similarities between the two. Similarly, it could be said that while there are indeed similarities, there also appear to be a number of differences. The similarities and differences that will be discussed next are based on a comparison of the clauses of the ISO: 17799 that were discussed earlier and the principles/guidelines of the Draft Standard that were discussed in the previous sub-section.

Both the ISO: 17799 and the Draft Standard include a clause or principle to deal with the creation of an organization-wide Information Security Policy. Although they have different names, another principle that they both have in common is the legal aspect of providing information security. The ISO 17799 uses the eleventh clause, Compliance, to prevent breaches of laws and regulations. The Draft Standard covers this within P200 of the contractual regulations principle.

The Draft Standards next principle, “Management of Information Systems Security”, deals with managing the Information Systems Security Policy. ISO 17799 has two clauses that help deal with the management of Information Security: “Organizing Information Security” and “Information Security Incident Management”. P400, the “Education Awareness” principle, correlates back to the ISO: 17799 clause, “Human Resources Security”. While this clause does have a few differences with P400 (i.e., also covers awareness before an employee starts) both cover employee awareness during their employment period within an organization.

P500, the “Limited information circulation” principle associates with the ISO 17799’s clause: “Communications and Operations Management”. The “Access Control” clause of ISO 17799 covers the task of ensuring authorized access from authorized users and prevents unauthorized access as well. This clause together with the clauses: “Physical and Environmental Security” and Information Systems Acquisition, Development and Maintenance” map back to P900, “Security Regulations”, of the Draft Standard.

A summary of these similarities is tabled in Table 4.4 below.

Table 4.4: Similarities between ISO 17799 and Draft Standard

Similarities	
ISO: 17799	**Draft Standard for High Level Security Policies for Healthcare Establishments**
Clause 1: Security Policy	P100: IS Security Policy
Clause 11: Compliance	P200: Contractual regulations
Clause 2: Organizing Information Security	P300: Management of IS Security
Clause 9: Information Security Incident Management	
Clause 4: Human Resources Security	P400: Education awareness
Clause 3: Asset Management	P700: Quality of health information
Clause 6: Communications and Operations Management	P500: Limited information circulation
Clause 5: Physical and Environmental Security	P900: Security regulations
Clause 7: Access Control	
Clause 8: Information Systems Acquisition, Development and Maintenance	

While there are similarities between these two standards, each of them still has content that the other does not. The Draft Standard does not contain a principle or a guideline that seeks to resolve issues that arise due to interruptions during business activities or major failures. However, the ISO: 17799 does contain the "Business Continuity Management" clause. While ISO: 17799 does have this extra condition, the Draft Standard has its own extra condition included within P600: "Data subject's rights". Whereas it may appear to discuss a user's roles within an organization, this principle, in fact, pertains to a user’s human and civil rights rather than information rights. Another extra principle that the Draft Standard has is the P800: “Medical and epidemiological research” principle. This principle also deals with a patient’s rights although not as much as the previous principle.

A summary of these differences is displayed in Table 4.5.

Table 4.5: Differences between ISO 17799 and Draft Standard

Differences	
ISO: 17799	**Draft Standard for High Level Security Policies for Healthcare Establishments**
Clause 10: Business Continuity Management	P600: Data subject’s rights
	P800: Medical and epidemiological research

According to Barry Barber of Health Data Protection Ltd, this Draft Standard is focused particularly towards the healthcare sector, while the ISO 17799 provides a more general viewpoint on Information Security. Because of this, the healthcare sector has two possible paths to take as it moves into the future.

It can either only use standards that are aimed at the healthcare sector in particular, or it can adopt a more general standard like the ISO 17799 and add items that aim specifically at the healthcare sector (Barber, 2002). If it decides to adopt healthcare-specific standards, then these standards will have to be continuously under review as well as be separately maintained by the healthcare sector (Barber, 2002). However, if it decides to use a more general approach there would be a lesser quantity of standards material, which would lead the healthcare sector towards a wider world of Information Security implementation (Barber, 2002).

4.2.5 Inter- and Intra-HIS Communication Standards Layer

While each system within the model is depicted separately from the other HISs, there must be a way to communicate between these systems in order to ensure that patients' medical information can be accessed wherever the patient may go, regardless of geographic location. This means that, according to the model, there must be four types of communication between the Health Information Systems:

1) Communication between HISs within the same state\province;
2) Communication between HISs across state\provincial borders;
3) Communication between HISs across countries borders;
4) Communication between HISs between continents.

While these four types of communication should theoretically be possible, there are problems on a practical, implementation level. According to Ruotsalainen (2004), current local/enterprise-wide information systems are not intended to provide cross-organizational secure access of patient data and are only able to provide local or regional communication (2004). Rogers and Reardon indicate that there are numerous obstructions for cross-organizational communication and list the barriers as a lack of (1999):

- a harmonized legal and ethical framework;
- a harmonized policy on trust, privacy and confidentiality;
- security services for trans-border communication;
- common security standards.

All of these obstructions are present between both regions and countries (Ruotsalainen, 2004).

4.2.5.1 Communication Standards

In order to allow information exchanges to be performed between the various HISs, a communication platform is needed (Ruotsalainen, 2004).

Most health platforms can be used for the integration of distributed health information systems, which are typically found regionally or among countries (Ruotsalainen, 2004). The current trend in Europe is to simply use Internet-like technologies to try to “glue” various regional platforms. This is where standardization can help with communication. If a common communication standard is used as a platform, cross-border communication could potentially be made easier and more secure.

Therefore, three different communication standards will be discussed in this section, namely the Health Level 7 Version 3.0, the ISO/DIS 22857 and a brief discussion on DICOM, in order to illustrate what is used in the healthcare environment at present. HL7 3.0 was chosen as Health Level 7 is considered a leading standards body in the communication area of healthcare and deals with the “how” information is communicated. ISO/DIS 22857 is also discussed, as ISO is the official international standards’ body in a wide variety of industries and deals with the “what is needed” for communication. DICOM is considered as an example of a communication standard in a specific health domain (imaging). It is used mostly for the transport of medical images (X-rays, etc).

Most of the information regarding HL7 Version 3.0 is taken from a document released by the NHS in 2001. The ISO/DIS 22857 communication standard information is covered by a document released in 2003 by the International Organization of Standardization.

4.2.5.1.1 HL7 Version 3.0

In Chapter 3, the HL7 Version 3.0 was discussed as one of the communication standards that can be used for communication between different HISs. Typically, the early versions of the standard have used very pragmatic, but not always rigorous, solutions to meet the requirements of already installed hospital and departmental systems, some of which use mature technologies.

With regards to the systems architecture, no assumptions are made by HL7. Due to HL7's system architecture:

- Communicating systems can be distributed or centrally organized;
- The entire extent of HL7 does not need to be implemented; most users begin with the transmission of administration/demographic data;
- Exchange of data between systems can be implemented using various operating systems or programming languages;
- As a rule, communication over a network is intended, but not required

The HL7 message communication also standardizes message structures, representation of messages for transmission and message triggering application events. To aid companies in adapting their data structures to HL7's, there are more and more commercial tools to accomplish this (NHS, 2001).

HL7 is an important step towards interoperability in communication. While HL7 does not provide "plug and play", it still saves time and costs for both users and manufacturers of application systems (NHS, 2001).

The fundamentals of the HL7 Communication standard are, according to Figure 4.1, that in order for two or more applications to communicate via HL7, the applications would require an HL7 interface. The procedure for HL7 communication, as outlined by the diagram, is as follows (Blobel, Spiegel, Pharow, Engel & Krohn, 2002):

- After an event has occurred, such as patient information is requested by an application, the information is “wrapped” by the HL7 Interface in order to standardize the message format into HL7.
- From there, the wrapped HL7 message will be sent to the secure HL7 communication server.
- From there, the wrapped message will then be forwarded to the application where the information is needed.

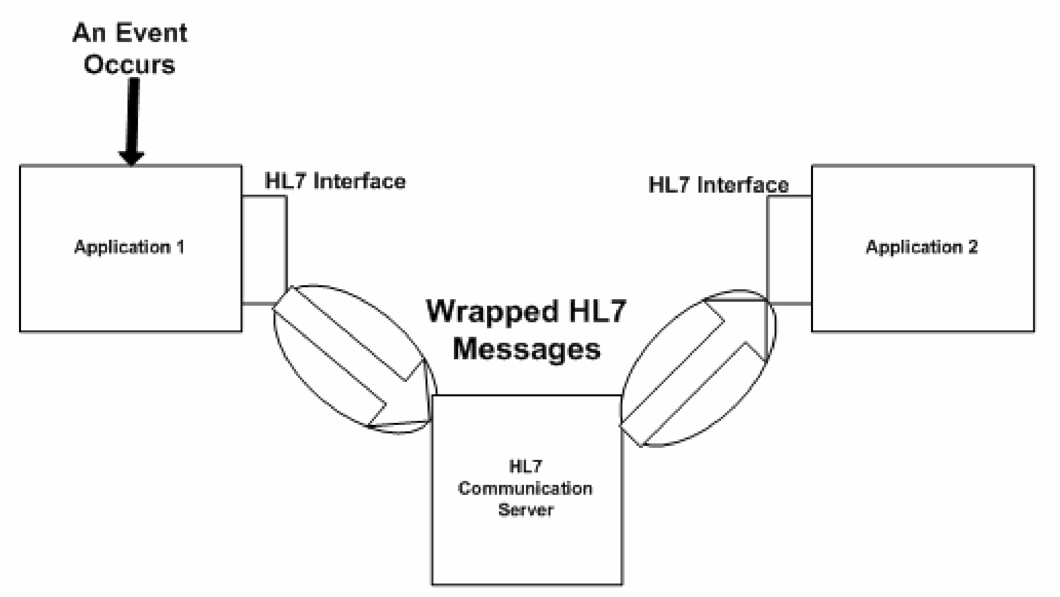


Figure 4.1: HL7 Communication Security

The cornerstone of the HL7 Version 3 development process is the Reference Information Model (RIM). RIM is a large pictorial representation of the clinical domains and identifies the life-cycle of events that a message will carry. The core classes of RIM are displayed in Figure 4.2 (NHS, 2001).

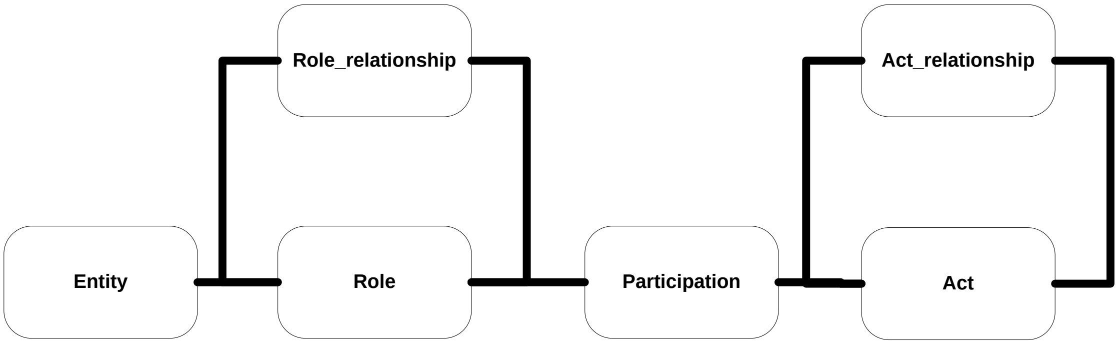


Figure 4.2: The Core Classes of the RIM

RIM uses the Unified Service Action Model (USAM) to help simplify the clinical functions of HL7 Version 3. RIM is essential to increasing precision and reducing implementation costs (NHS, 2001).

4.2.5.1.2 ISO/DIS 22857

ISO/DIS 22857 is an international standard that provides guidance on data protection requirements to facilitate the transfer of personal health data across national borders (International Organization of Standardization [j], 2003). The information used in this section was taken from a document dedicated to the ISO/DIS 22857 standard. This standard can, however, also be informative in respect to the protection of health information within national boundaries. Unlike HL7, where the applications need an HL7 Interface to standardize the message types, this standard does not require synchronization of existing standards, legislation or regulations. It must also be noted that this standard is only similar to a regular standard with regard to international exchange of personal health data (International Organization of Standardization [j], 2003).

This standard does not attempt to provide legal advice with regards to information security, but rather encompasses guidelines. The standard is not solely a data-protection standard either. It also covers the security policy that an organization should adopt to ensure compliance (International Organization of Standardization [j], 2003).

ISO/DIS 22857 has seven clauses that it uses to define guidelines to help facilitate international health-related applications involving the transfer of personal health data. These clauses are (International Organization of Standardization [j], 2003):

1) General principles and roles;
2) Legitimizing data transfer;
3) Criteria for ensuring adequate data protection with respect to the transfer of personal health data;
4) Security policy;
5) High-level security policy;
6) Rationale and observations on measures to support Principle Ten concerning security of processing;
7) Personal health data in non-electronic form.

General principles and roles reflect general principles found in international documents on communication and also deal with the main roles of data importers/exporters and data controllers/processors. The legitimizing data transfer clause introduces two main requirements for a transfer of personal health data to be legitimate according to this standard and covers consent and adequacy of data protection (International Organization of Standardization [j], 2003).

While the second clause deals with the two main requirements for a transfer of personal health data, it is only dealt with in general. The third clause, however, deals with those same two main requirements in a much more detailed view and lays down all of the criteria for adequacy and also takes the concept of consent much further. The security policy clause explains what is meant by ‘high level’ data protection according to this standard (International Organization of Standardization [j], 2003).

The high-level security policy clause lays down, in detail, the requirements for such a high-level policy in order to help guarantee that the criteria for adequacy of data protection is certain. The sixth clause on the list provides detailed requirements which relate to administrative and technical means for ensuring data security that need to be outlined in the data importer's policy. The last clause covers all health data that is not stored in electronic format (International Organization of Standardization [j], 2003).

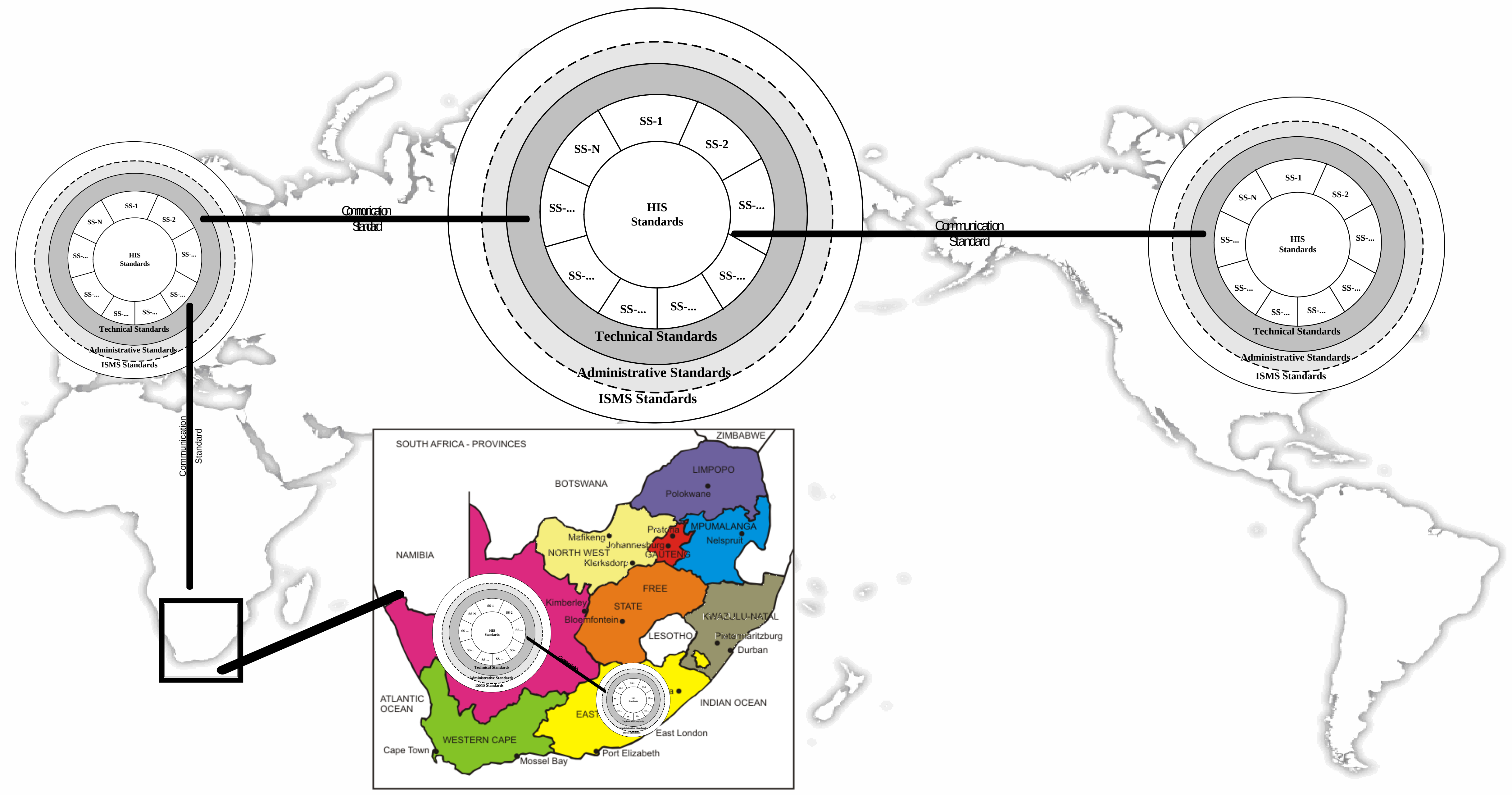
4.2.5.1.3 DICOM

Digital Imaging and Communications in Medicine (DICOM) defines the coding of medical images, the protocols of interchange between both sides and a security policy to hide information from third-party people. One of the newer versions, DICOM 3.0, has added waveform support to allow Electroencephalogram (EEG) and Electrocardiogram (ECG) interchanges ("Standards List", n.d). A number of major enhancements are that DICOM is applicable to a networked environment and to an off-line media environment; it specifies how devices that conform to this standard react to commands and data being exchanged as well as the levels of conformance, and can specify an established technique for uniquely identifying any information object (National Electrical Manufacturers Association 2003).

DICOM is supported by most radiology Picture Archiving and Communication Systems (PACS) vendors (Smith, 2002). DICOM may be implemented by allowing the transfer of messages and images that have been made by multiple vendors and located at either one or many sites to communicate across an open-system network (Smith, 2002). In short, medical images can be captured and communicated more quickly, physicians can make diagnoses sooner and, therefore, treatment decisions can be made quicker (Smith, 2002).

4.3 Conclusion

This chapter outlined and discussed a security model based on standards that are used in the healthcare environment. This model focused around the health information system and various layers that covered aspects, from technical standards to communication between these systems. The next chapter will be used to bring all of the research together and draw up the conclusion.



Note that the inclusion of the world map in this diagrammatic depiction of the model, is simply for illustrative purposes and does not relate to the country of origin of particular standards that would apply when flow of data takes place between systems.

Chapter 5: Conclusion

5.1 Milieu

This research dissertation investigated the possibility of a standards-based model for the healthcare environment with specific emphasis being placed on security. To carry out this research, the topics of the healthcare environment as well as a general viewpoint of health information systems were researched. Furthermore, the research delved deeper into the health information system by outlining some of the commonly used terminology. Security was explored by inspecting well-known standards bodies that produce healthcare standards, in particular, the aspect of security standards.

The foundation of this final chapter assesses whether or not the research objectives of this dissertation have been satisfactorily met. This will be followed by the limitations of this research as well as any possible future research.

5.2 Revisiting the Problem Statement and Objectives

5.2.1 The Problem Statement

In Section 1.5 in Chapter 1, a number of questions were raised with regard to the problem of the proliferation in security standards. This problem, which makes it difficult to identify, understand, adopt and deploy these security standards in a coherent manner, has led to the creation of a number of objectives that are discussed in the next section.

5.2.2 The Objectives of This Research

The principal objective of this research was to investigate standards that address security in healthcare and develop a standards-based security model for health information systems.

In order to achieve this objective, it was necessary to concentrate on a number of sub-objectives.

Research Objective: *An investigation into the healthcare environment and health information systems in order to gain insight into the healthcare landscape.*

This objective was carried out in Chapter 1’s Section 1.2.1 and Section 1.2.2, where a brief introduction of the healthcare environment and health information systems was situated. A more in-depth view of health information systems was also investigated in Chapter 2’s Section 2.2, where the history of health information systems as well as some HIS terminology was discussed.

This sub-objective laid the foundation of the area of research as it depicted the environment and how governments could get involved within the healthcare industry. It further displayed that there is no singular definition of a health information system and that there are numerous types of electronic systems (aka CCR, PHR, EHR, etc.), each with its own purpose, such as allowing patients to take a more active role in the upkeep of their electronic records, to all patient information, from birth up until the present, being stored in these electronic records.

Research Objective: *Establishing the level of importance of and the need for security in healthcare.*

In Section 1.3 in Chapter 1, the importance of security in the healthcare environment was underscored by a number of examples of security breaches that have actually occurred. Section 2.3 of Chapter 2 also looked at information security in healthcare, in particular, from a HIPAA point-of-view. This section also took a look at Information Security Management, which showed the importance of implementing proper security principles in a holistic manner.

The examples provided showed that security within the healthcare environment is not perfect and that by applying best practices through using recognized standards, the possibility of health information being breached can be reduced. Investigating security from a more legal aspect (HIPAA) illustrated that there is a significant difference between laws and standards. While the legal aspect is excluded from this study due to scope limitations, its importance is, nevertheless, recognized.

The discussion on Information Security Management helped outline feasible steps that organizations could take to help improve the security of health information. While these steps are not mandatory by law, organizations implementing these steps have a possibility of being more secure than an organization that does not. It further contributes to organizations applying a comprehensive and focused approach to security.

Research Objective: *The discussion of standards bodies and standards in the healthcare environment and, in particular, security standards.*

The various standards bodies that provide security standards for the healthcare environment were discussed in Chapter 3. Together with these standards bodies, a number of security standards that have been produced by these bodies were briefly described with regard to their role in security.

This sub-objective needed to take into account the number of standards bodies that existed throughout the world. The reasons the standards bodies that were chosen to discuss are because:

- They cover a wide area of the globe, CEN in Europe, ASTM in America, HL7, ranging across a number of countries, and ISO, essentially used worldwide;
- The standards created by these standards bodies are commonly used; and
- These standards bodies have cooperated with each other in the past.

As for the security standards chosen, the security standards that were discussed covered a wide range of security aspects from encryption to digital signatures. The research attempted to discuss a comprehensive list of these standards for each standard body through interpreting information available from literature. It should be reiterated, however, that limited access to the web site of standards bodies hampered efforts to determine precisely which standards are under development, active or have been replaced as at the date of the discussion.

Research Objective: *The incorporation of the information gleaned from the afore-mentioned investigations in a standards-based security model for health information systems.*

This objective was achieved in Chapter 4 with the discussion of the proposed standards-based security model for health information systems. The model included a layer for the actual health information system, together with its sub-systems, a layer where both the technical and administrative standards would be found, a layer dealing with the standards that would be used by an Information

Security Management System, and a layer that covers those standards used for the communication between systems.

The completion of the previous sub-objectives made the construction of the standards-based model easier. Discovering a security categorization model for health information systems helped with the foundation of the model, the Health Information System Standards Layer. Investigating the security standards in Chapter 3 showed that there are two possible types of security standards: the more technical ones and those that are more administrative. This helped to visualize the Technical and Administrative Standards Layer. The discussion on Information Security Management displayed the need for a management-type system in order to supervise a coordinated and holistic approach to information security. The final layer of the model, the Intra- and Inter-HIS Communication Standards Layer, was needed in order to provide communication between the various systems situated in different geographic locations, as well as between the different sub-systems in its own system.

Although the research done for this dissertation was completed, there were certain restrictions during the research period.

5.3 Restrictions on the Research Process

Throughout the duration of this research, certain boundaries arose. These limitations fell into four areas. The first limitation was the number of standards bodies that create the standards that are used within the healthcare environment. Because there are too many standards bodies, it was decided to rather focus on those standards bodies that are both well known and are the forerunners of producing standards.

In line with this limitation, the sheer number of security standards that have been created placed another restriction on this research. Even when narrowing down the security standards specifically for the healthcare environment, the volume of standards meant that it was nearly impossible to discuss each and every one of them for the purpose of this dissertation.

The next limitation was placed on the area of security. It was decided that the main focus of this research was to be security standards that originated through standards bodies and not through legislation. This ruled out a number of standards, such as those created for HIPAA.

The final limitation was access to information about the security standards that were eligible for discussion. Due to the fact that not all standards bodies' websites provided full access to their standards, the amount of information that could be used was limited to brief summaries and possible synopses.

5.4 Benefits and Limitations of the Research

Even with these limitations in place, the model that was created as a result of the research does have benefit. One benefit is that the model presented in Chapter 4 provides a simple view that makes the health information system easier to understand in the context of its total security milieu.

Secondly, the model shows how the various standards work together, each adding a layer of security with a focus different to the other layers. It, therefore, promotes a holistic approach to security, which discourages a singular, technology-driven approach to security.

Taking the restrictions that were placed on the research process into account, a limitation on the actual research output resulted. The model has been informed through the consideration of a limited number of standards bodies and standards. It could be argued that the model may be expanded after an investigation of more standards. This does, however, create possible future research opportunities.

5.5 Directions for Future Research

Perhaps in the future, with information becoming more and more accessible, further research can be conducted with the full resources of security standards from standards bodies. Since the problem statement explicitly mentions the proliferation in standards, the necessity of creating a comprehensive catalogue or database of security standards in healthcare cannot be negated. The researcher further recommends that such a database should attempt to show the relationship between such standards, so that areas of overlap, for example, become clear.

Another possibility for future research is researching the legislation that can be used in the improvement of security within the healthcare environment. It is the opinion of the researcher that while the model currently proposes the legal dimension at the layer of the ISMS, it could be expanded to include a governance layer, which would further emphasize and realize the legal requirements in the model.

5.6 Epilogue

With both medical and financial patient information being stored, either electronically or on paper needing to be kept available and secure, inevitably there will always be a need for research on the topic of Information Security in the healthcare environment. Due to constant technological advances, this research topic in all areas of the healthcare environment is becoming more and more of a requirement everyday.

References

Allaert, F. A., & Barber, B. (2000). Law and Standards [Electronic Version]. *International Journal of Medical Informatics, 60*, 99-103.

American National Standards Institute [a]*.* (2006). Retrieved February 20, 2006, from http://webstore.ansi.org/ansidocstore/product.asp?sku=DIN+V+ENV+12388%3A1996

American National Standards Institute [b]*.* (2006). Retrieved February 20, 2006, from http://http://webstore.ansi.org/ansidocstore/product.asp?sku=DIN+V+ENV+13608-2%3A2000

Arzt, N. H. (2007, July 10). *Evolution of Public Health Information Systems: Enterprise-wide Approaches.* Retrieved August 26, 2007, from http://health.utah.gov/chd/UT_White_Paper.pdf

Ash, J. S., & Bates, D. W. (2005, January/February). Factors and Forces Affecting EHR System Adoption: Report of a 2004 ACMI Discussion. Retrieved March 31, 2006, from http://www.jamia.org/cgi/reprint/12/1/8.pdf

ASTM International [a]*.* (2006). Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2085.htm?E+mystore

ASTM International [b]. (2006). Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2084.htm?E+mystore

ASTM International [c]. (2006). Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2212.htm?E+mystore

ASTM International [d]. (2006). Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1762.htm?E+mystore

ASTM International [e]. (2006). Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1986.htm?E+mystore

ASTM International [f]. (2006). Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E1987.htm?E+mystore

ASTM International [g]. (2006). *E2117-00: Standard Guide for Identification and Establishment of a Quality Assurance Program for Medical Transcription.* Retrieved February 12, 2006, from http://www.astm.org/cgi-bin/SoftCart.exe/DATABASE.CART/REDLINE_PAGES/E2117-00.htm?E+mystore

ASTM International. (1996-2008). *Membership / Member Types.* Retrieved March 5, 2007, from http://www.astm.org/cgi-bin/SoftCart.exe/MEMBERSHIP/MemTypes.htm?L+mystore+flof6608+1199817989

ASTM International. (1996-2008). *Membership / Organizational Membership Directory.* Retrieved March 15, 2007, from http://www.astm.org/cgi-bin/SoftCart.exe/MEMBERSHIP/memborg/index.html?L+mystore+fbdc4689+1174449380

ASTM International. (2003, August). *Plain Talk for a New Generation : A Simple Decision.* Retrieved February 3, 2007, from http://www.astm.org/cgi-bin/SoftCart.exe/SNEWS/AUGUST_2003/plaintalk_aug03.html?L+mystore+qynk6378

Atherley, G. (2005). Evidence of Public Value and Public Risk of Electronic Health Records: An Issue for Social Justice? *ElectronicHealthcare, 4*(1), 96-103. Retrieved March 15, 2006, from http://emruser.typepad.com/canadianemr/Articles/EHR_Atherley.pdf

Barber, B. (2002). Conclusion. In Allaert, F-A., Blobel, B., Louwerse, K. & Barber, B. (Eds.), *Security Standards for Healthcare Information Systems: A perspective from the EU ISIS MEDSEC Project* (pp. 229-233). Amsterdam: IOS Press.

Barret, M. J. (2000). The evolving computerized medical record. *Healthcare Informatics, 17*(5), 85-92.

Bazzoli, F. (1996, April). State Networks Move Ahead, Learning from Pioneers' Travails. *Health Data Management*, pp. 60-65.

Berner, E. S., Detmer, D. E., & Simborg, D. (2005, January/February). Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States. Journal of the American Medical Informatics Association, 12(1), 3-7. Retrieved April 3, 2006, from http://www.jamia.org/cgi/reprint/12/3.pdf

Blobel, B., Spiegel, V., Pharow, P., Engel, K., & Krohn, R. (2002). Standard Guide for Implementing HL7 Communication Security. In Allaert, F-A., Blobel, B., Louwerse, K. & Barber, B. (Eds.), *Security Standards for Healthcare Information Systems: A perspective from the EU ISIS MEDSEC Project* (p.). Amsterdam: IOS Press.

Carter, J. S., Brown, S. H., Nelson, S. J., Lincoln, M. J., & Tuttle, M. S. (n.d.). The Creation and Use of a Reference Terminology for Inter-Agency Computer-based

Patient Records: The GCPR RTM Demonstration Project. Retrieved February 15, 2006, from http://adams.mgh.harvard.edu/pdf_repository/D010001512.pdf

Cooper, T., & Collmann, J. (2000). *How to Use the CPRI Toolkit: Managing Information Security in Health Care.* Retrieved October 21, 2007, from http://www.himss.org/content/files/proceedings/2000/sessions/ses041.pdf

Cooper, T., & Collmann, J. (2005). Managing Information Security and Privacy in Healthcare Data Mining State of the Art. In *Medical Informatics Knowledge Management and Data Mining in Biomedicine* (pp. 96-137). : Springer US.

Daniels, A. S. (n.d.). *Crossing the Quality Chasm; A New Health System for the 21st Century.* Retrieved November 2, 2007, from http://www.nri-inc.org/projects/SDICC/DIGMeeting/Daniels.pdf

Department of Health and Human Services [a]. (2007, March). Security 101 for Covered Entities [Electronic Version]. *Centers for Medicare & Medicaid Services, 2*(1), 1-11.

Department of Health and Human Services [b]. (2007, March). Security Standards: Administrative Safeguards [Electronic Version]. *Centers for Medicare & Medicaid Services, 2*(2), 1-11.

Department of Health and Human Services [c]. (2007, March). Security Standards:

Physical Safeguards [Electronic Version]. *Centers for Medicare & Medicaid Services, 2*(3), 1-11.

Department of Health and Human Services [d]. (2007, March). Security Standards: Technical Safeguards [Electronic Version]. *Centers for Medicare & Medicaid Services, 2*(4), 1-11.

Department of Health and Human Services [e]. (2007, March). Security Standards: Organizational, Policies and Procedures and Documentation Requirements [Electronic Version]. *Centers for Medicare & Medicaid Services, 2*(5), 1-11.

Department of Health and Human Services [f]. (2006, December 28). HIPAA Security Guidance [Electronic Version]. *Centers for Medicare & Medicaid Services*, pp. 1-7.

ECHI Project. (2001). *Design for a set of European community health indicators,*

European Committee for Standardization. (2007). *About Us.* Retrieved December 23, 2007, from http://www.cen.eu/cenorm/aboutus/index.asp

Farlex. (2008). *healthcare.* Retrieved December 26, 2007, from http://www.thefreedictionary.com/healthcare

Furnell, S. M., Davey, J., Gaunt, P. N., Louwerse, C. P., Mavroudakis, K., & Treacher,

A. H. (1998). The ISHTAR guidelines for healthcare security. *Health Informatics, 4*, 179-183. Retrieved August 31, 2007, from http://jhi.sagepub.com

Hammond, W. E. (1995). The status of healthcare standards in the United States [Electronic Version]. *International Journal of Bio-Medical Computing, 39*, 87-92.

Health Level 7. (2007, November 8). *HL7 Membership Numbers.* Retrieved January 3, 2008, from http://lists.hl7.org/read/attachment/117742/1/membership_worldwide.xls

Health Level Seven, Inc. (2004). HL7 EHR System Functional Model: A Major Development Towards Consensus on Electronic Health Record System Functionality. Retrieved April 12, 2006, from http://www.hl7.org/ehr/downloads/dstu/EHR-SWhitePaper.zip

Health Management Systems, Inc. (2007). *Momentum Grows for Expanding Coverage to the Uninsured.* Retrieved September 7, 2007, from http://www.hmsy.com/nl/Prism%20Winter%202007%20Final%20Letter.pdf

Health Services Advisory Group. (n.d.). *Continuity of Care Record (CCR) Project.* Retrieved October 25, 2007, from http://acute.hsag.com/CCR_Project.pdf

Hunter, K. M. (2002). Electronic Health Records. In *Health Care Informatics: An Interdisciplinary Approach* (pp. 209-230). Missouri: Mosby.

International Organization for Standardization [a]. (2007). *ISO 22857:2004.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36522

International Organization for Standardization [b]. (2007). *ISO/TR 21089:2004.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35645

International Organization for Standardization [c]. (2007). *ISO/TR 22221:2006.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40783

International Organization for Standardization [d]. (2007). *ISO/TS 17090-1:2002.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35489

International Organization for Standardization [e]. (2007). *ISO/TS 17090-2:2002.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35490

International Organization for Standardization [f]. (2007). *ISO/TS 17090-3:2002.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35491

International Organization for Standardization [g]. (2007). *ISO/TS 21091:2005.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35647

International Organization for Standardization [h]. (2007). *ISO/TS 22600-1:2006.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36337

International Organization for Standardization [i]. (2007). *ISO/TS 22600-2:2006.* Retrieved September 11, 2007, from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40930

International Organization for Standardization [j]. (2003). *Health informatics - Guidelines on data protection to facilitate trans-border flows of personal health information.* Retrieved April 1, 2005, from http://www.cihi.ca/cihiweb/en/downloads/event_partner_may03_iso22857_e.pdf

International Organization for Standardization [k]. (2000). *Requirements for an Electronic Health Record Reference Architecture.* Retrieved October 26, 2006, from http://www.cihi.ca/cihiweb/en/downloads/infostand_ihisd_isowg1_TSV0.5_e.pdf

International Organization for Standardization. (2002, August 8). *ISO/Tc 212, Clinical laboratory testing and in vitrodiagnostic test systems.* Retrieved December 5, 2007, from http://isotc.iso.org/livelink/livelink/1972264/ISO_TC_212_Work_Programme.doc?func=doc.Fetch&nodeid=1972264

ISO 17799 (2005). *ISO 17799: 2000 Code of Practice for Information Security Management*. : .

ISO [a]. (2007). *Discover ISO: Meet ISO.* Retrieved December 10, 2007, from http://www.iso.org/iso/about/discover-iso_meet-iso.htm

ISO [b]. (2007). *General Information on ISO.* Retrieved December 10, 2007, from http://www.iso.org/iso/support/faqs/faqs_general_information_on_iso.htm

ISO. (2008). *Discover ISO: ISO's name.* Retrieved January 2, 2008, from http://www.iso.org/iso/about/discover-iso_meet-iso/discover-iso_isos-name.htm

ISO/TC 212. (2002, August 8). *ISO/TC 212, Clinical laboratory testing and in vitro diagnostic test systems.* Retrieved October 13, 2007, from http://isotc.iso.org/livelink/livelink/1972264/ISO_TC_212_Work_Programme.doc

ISO/TC 215 Working Group 3. (n.d.). *ISO/TC 215 Working Group 3 Health Informatics - Semantic Content.* Retrieved November 3, 2006, from http://www.tc215wg3.nhs.uk/pages/default.asp

ISO27001 CENTRAL. (2004). Retrieved August 5, 2007, from http://www.17799central.com/pdca.htm

Japan Association of Medical Informatics. (2003, February). JAMI Viewpoint Concerning the Definition of the Electronic Medical Record. Retrieved February 12, 2006, from http://www.jami.jp/denshikarute_en.pdf

Kokolakis, S., Gritzales, D., Katsikas, S., & Ottes, F. (2002). Overview on Security Standards for Healthcare Information Systems. In Allaert, F-A., Blobel, B., Louwerse, K. & Barber, B. (Eds.), *Security Standards for Healthcare Information Systems: A perspective from the EU ISIS MEDSEC Project* (pp. 13-21). Amsterdam:

IOS Press.

Kokolakis, S., Gritzalis, D., & Katsikas, S. (2002). Draft Standard for High Level Security Policies for Healthcare Establishments. In Allaert, F-A, Blobel, B., Louwerse, K. & Barber, B. (Eds.), *Security Standards for Healthcare Information Systems: A perspective from the EU ISIS MEDSEC Project* (pp. 23-47). Amsterdam: IOS Press.

Louwerse, K. (2002). Demonstration Results for the Standard ENV12924. In Allaert, F-A., Blobel, B., Louwerse, K. & Barber, B. (Eds.), *Security Standards for Healthcare Information Systems* (pp. 111-139). Amsterdam: IOS Press.

Mendelson, D. N., & Salinsky, E. M. (1997, May/June). Health Information Systems And The Role Of State Government A taxonomy and evaluation of state government efforts on the health information frontier. *Health Affairs* Retrieved September 5, 2007, from http://content.healthaffairs.org/cgi/reprint/16/3/106.pdf

Milholland, D. K. (1989). *A measure of patient data management system effectiveness: Develolpment and testing*. Unpublished doctoral dissertation, University of Maryland, Baltimore.

Murphy, G. F., Waters, K. A., & Amatayakul, M. (1999). EHR vision, definition and characteristics. In G.F. Murphy, M.A. Hanken, & K.A. Waters (Eds.), Electronic health records: Changing the vision (pp. 3-26). Philadelphia: W.B. Saunders.

Mykkanen, J., Porrasmaa, J., Korpela, M., Hakkinen, H., Toivanen, M., Tuomainen, M., et al. (2004). Integration Models in Health Information Systems: Experiences from the PlugIT Project. *Medinfo*. Retrieved January 3, 2008, from http://cmbi.bjmu.edu.cn/news/report/2004/medinfo2004/pdffiles/papers/4451Mykkanen.pdf

National Electrical Manufacturers Association. (2003). *Digital Imaging and Communications in Medicine (DICOM) Part 1: Introduction and Overview.* Retrieved February 15, 2006, from http://medical.nema.org/dicom/2003/03_01PU.PDF

National Institute of Standards and Technology. (2006, December 22). *Health Care Standards Landscape.* Retrieved July 15, 2007, from http://www.itl.nist.gov/div897/docs/hc_roadmap.html

NHS. (2001). HL7. In *NHS IT Standards Handbook* (225). Retrieved August 26, 2007, from http://www.hl7italia.it/bac_Utenticoordinatori_717/225chap.pdf

Ondo, K. J., Wagner, J., & Gale, K. L. (2002). The Electronic Medical Record (EMR), Hype OR Reality?. Retrieved March 10, 2006, from http://www.himss.org/content/files/proceedings/2002/sessions/ses063.pdf

Peacott, J. (2003). *Health Care Without Government.* Retrieved November 12, 2007, from http://www.libertarian.co.uk/lapubs/econn/econn098.pdf

Personal Health Working Group. (2003, July 1). Retrieved September 3, 2006, from http://www.connectingforhealth.org/resources/final_phwg_report1.pdf

*R*ogers, R., & Reardon, J. (1999). Barriers to a Global Information Society for Health Recommendations for International Action [Electronic Version]. *Studies in Health Technology and Informatics*

Ruotsalainen, P. (2004, March 31). A cross-platform model for secure Electronic Health Record communication [Electronic Version]. *International Journal of Medical Informatics, 73*(3), 291-295.

Schoenberg, R. (2005). Security of Healthcare Information Systems. In *Consumer Health Informatics Informing Consumers and Improving Health Care* (pp. 162-187). : Springer New York.

Scott, M. (2004, November 22). HIPAA Gavel Drops? A Message to Healthcare. *Radiology Today, 5*(24), 38. Retrieved June 13, 2007, from http://www.pogowasright.org/documentation/2004/SeattleCancer_01.html

Shortliffe, E. H. (1999).The Evolution of Electronic Medical Records. Retrieved March 15, 2006, from http://smi-web.stanford.edu/pubs/SMI_Reports/SMI-1999-0782.pdf

Smallwood, R. (2001). Developing a National Electronic Health Record. Retrieved March 10, 2006, from http://www.himss.org/content/files/proceedings/2001/sessions/ses132.pdf

Smith, K. (2002). Technical Standards Used in Health Care Informatics. In *Health Care Informatics: An Interdisciplinary Approach* (p. 209-230). Missouri: Mosby.

Spyrou, S. S., Bamidis, P., Chouvarda, I., Gogou, G., Tryfon, S. M., & Maglaveras, N. (2002). Healthcare information standards: comparison of the approaches. *Health Informatics Journal, 8*, 14-19. Retrieved August 31, 2007, from http://jhi.sagepub.com

Standards List. (n.d.). Retrieved January 11, 2007, from http://www.who.int/ehscg/resources/en/ehscg_standards_list.pdf

Stega, M., Pollizzi, J., & Milholland, A. (1980). *A successful clinical computer system*. Paper presented at the Fourth Annual Symposium on Computer Applications in Medical Care, Los Angeles, CA.

Swindom, G. (2004). HIPAA Final Security Rule Information Security Reference Guide. Sygate Technologies, Inc.

Thompson, D. (Ed.). (1993). *The Oxford Dictionary of Current English* (2). Denmark: Oxford University Press.

TippingPoint. (2005). *Securing Critical Data and IT Infrastructure in Healthcare Environments.* Retrieved October 21, 2007, from http://www.3com.com/solutions/en_US/healthcare/solutions/SecuringHealthcareEnvironments-3Com.pdf

Tipton, H. F., & Krause, M. (2004). Information Security Management Handbook (Fifth). : CRC Press LLC..

Tonnesen, A. S., LeMaistre, A., & Tucker, D. (n.d.). *Electronic Medical Record Implementation Barriers Encountered During Implementation.* Retrieved March 20, 2006, from http://www.amia.org/pubs/symposia/D005401.PDF

Tuyikeze, T. (2006). A Model for Information Security Management and Regulatory Compliance in the South African Health Sector (Masters dissertation, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa).

UC Santa Cruz. (2007, November 19). *Security Breach Examples and Practices to Avoid Them.* Retrieved December 20, 2007, from http://its.ucsu.edu/security_awareness/breaches.php

Von Solms, S. H., & von Solms, R. (2007). *Information Security Governance (Draft)*.

Waegemann, C. P. (2003, May). In HER vs. CPR vs. EMR. Retrieved February 12, 2006, from http://www.providersedge.com/ehdocs/ehr_articles/EHR_vs_CPR_vs_EMR.pdf

Wagener, Y., & Alkerwi, A. (n.d.). Health information Systems in Europe – Structures and Processes – Final Report. In . Retrieved October 22, 2007, from http://ec.europa.eu/health/ph_projects/2001/monitoring/fp_monitoring_2001_a7_frep_13_en.pdf

Welcomeurope. (2000-2008). *CEN (European Committee for Standardization).* Retrieved October 23, 2007, from http://www.welcomeurope.com/default.asp?id=1520&idreseau=110

WHO & AFRO. (n.d.). *Health Information Systems.* Retrieved September 31, 2007, from http://www.afro.who.int/his/index.html

Wikipedia [a]. (2007, November 30). *Health Level 7.* Retrieved December 5, 2007, from http://en.wikipedia.org/wiki/Health_Level_7

Wikipedia [b]. (2007). *ASTM International.* Retrieved December 5, 2007, from http://en.wikipedia.org/wiki/ASTM_International

Wikipedia [c]. (2007, December 11). *European Committee for Standardization.* Retrieved December 15, 2007, from http://en.wikipedia.org/wiki/European_Committee_for_Standardization

Wikipedia [d]. (2007). *ISO/IEC 27001.* Retrieved July 31, 2007, from http://en.wikipedia.org/wiki/ISO_27001

Wikipedia [e]. (2007). *PDCA.* Retrieved August 5, 2007, from http://en.wikipedia.org/wiki/PDCA

Appendices

The following paper was presented whilst conducting research towards this dissertation:

Appendix A:

Paper 1

Thomson, S., & Pottas, D. (2006). *“Improving the Security of Health Care Information Through Electronic Means”*. ISSA 2006, Johannesburg, South Africa

IMPROVING THE SECURITY OF HEALTH CARE INFORMATION THROUGH ELECTRONIC MEANS

Steven Thomson[a], Dalenca Pottas[b]

a Department of Information Technology, Nelson Mandela Metropolitan University

b Department of Applied Informatics, Nelson Mandela Metropolitan University

a Steven.Thomson@nmmu.ac.za, +27 41 504-3646, PO Box 77000, Port Elizabeth, 6031

b Dalenca.Pottas@nmmu.ac.za, +27 41 504-9100, PO Box 77000, Port Elizabeth, 6031

ABSTRACT

Around 40 years ago the health care sector began to look towards computers to help with the everyday functions that clinicians performed. While a good idea at the time, it took 20 years before the concept of a health care or health information system was truly accepted as the information and communication technology had matured enough to implement the systems. Health care systems have evolved from stand-alone systems to systems with limited interoperability. However, due to lack of standards, wide-scale interoperability has not been achieved as yet.

Research is currently ongoing to examine the advantages and disadvantages of health information systems. There are various points of view amongst researchers as to whether the disadvantages outweigh the advantages with regards to security in particular. This paper sets out to investigate both sides of this argument, through literature studies. The paper concludes that the security and privacy of health information can indeed be improved through the use of electronic health records (EHRs), but only through proper consideration for the factors that support an EHR environment, e.g. technological, organizational and governance / legislative factors.

KEY WORDS

Electronic health records, standardization, HL7, security, privacy

IMPROVING THE SECURITY OF HEALTH CARE INFORMATION THROUGH ELECTRONIC MEANS

INTRODUCTION

Availability is generally accepted as a critical characteristic of information. This is especially applicable in reference to the availability of electronic patient information. If doctors or medical personnel are unable to access the necessary information, then patients could be given incorrect diagnoses and erroneous treatment.

Over the years, various approaches have evolved towards computerizing and improving the availability of electronic patient information, viz Computer-based Patient Records (CPRs), Electronic Medical Records (EMRs)/Electronic Patient Records (EPRs) or Electronic Health Records (EHRs). The objective in general, is to provide access to patient information by clinical staff at any given location; facilitate accurate and complete claims processing by medical aid companies and documentation of prescriptions, amongst other functions.

Interestingly, the acronyms CPR, EMR and EHR are often confused. It is frequently overlooked that these three terms actually constitute three different types of health information systems. The Computer-based Patient Record, or CPR, was the original concept of the electronic healthcare system, but these became outdated because of incompatibility between different vendors' software. The Electronic Medical Record, or EMR, is the current standard and provides greater interactivity and real-time accessibility. Finally, the Electronic Health Record, or EHR, is the next step in the evolution of electronic patient records. The major difference between the EMRs and the EHRs is that instead of the hospital owning and running the systems, the EHRs will be owned by the patients themselves. They will, in turn, allow certain providers to be able to access their medical records.

Notably, there are indications from literature, that security-related issues are considered as barriers to the use of EHRs. This appears to hamper the general acceptance of and progress towards the implementation of EHRs. The objective of this paper is to illustrate that EHRs should be used in modern healthcare because they improve the availability of patient information, understandably a critical consideration in the operation of the healthcare sector. In addition, it will be argued that the confidentiality, integrity, availability and privacy of electronic patient information are strengthened through the use of EHRs. However, this can only be achieved through proper consideration for the factors that support an EHR environment, e.g. technological, organizational and governance / legislative factors. This paper will analyze the factors that hamper the confidence in and the implementation of EHRs and will show how proper consideration of those factors will ensure that the EHR can operate effectively and securely, with due consideration to the privacy of patient information.

Background

Historic Overview

The paper-based medical record arose in the 19th century as a highly personalized "lab notebook" that clinicians could use to record their observations so that they could be reminded of pertinent details when they next saw the same patient (Shortliffe, 1999). Doctors tended to work alone and wrote down their patients' medical records using this paper-based format. Patients were considered friends to these early doctors and often paid them directly (Tipton & Krause, 2004). As time progressed, people started to think that maybe there was another way that could provide well-organized and well-timed access to patients' health records (Waegemann, 2003).

During the early 1960s, computers were first used within a hospital setting, however at this time they were only used for administrative and financial functions. At this time there was early work being conducted in the medical informatics area. This work focused on clinical computing to improve clinical decisions and reduce medical errors as well as ensuring faster access to applicable medical information and decision support functions. Examples of the early EMR versions, or the CPRs, include the HELP system at LDS Hospital in Utah, the COSTAR system at Massachusetts General Hospital, the TMR system at Duke and the Regenstrief Medical Record System (Berner, Detmer, & Simborg, 2005).

Even with all of the scientific medicine growth (more pharmaceuticals, etc), the adoption of computer applications was between low and non-existent for many different reasons. One of these reasons was that clinicians were not willing to accept early systems because they felt that they were too expensive, slow and awkward. Administrators were against these EMRs because it was not clear what the financial benefits would be at the time. Another reason for lack of adoption in the United States, was that the federal government created the Medicare and Medicaid legislation. Under this law, administrators and insurers both felt satisfied to let medical staff continue to practice separately (Berner, et al., 2005).

However, by the beginning of the 1980s, technology that could compliment EMRs had greatly evolved. The original mainframe computers were being replaced with distributed networks of microcomputers, Microsoft Windows had been introduced and networking proliferated. This eventually led to the creation of the HL7 standard to allow for data interchange of health-related information.

Unlike during the 1960s and 1970s, there were a number of governmental programs that promoted policies that helped distribution of the EMR. A conference held at the National Institute of Health in America in the late 1980s led to a report being released in 1991 specifically dealing with the Electronic Health Record. This report, called "The Computer-based Patient Record: An essential technology for health care", looked at three main features: uses and users, technology and policy and implementation. This report led to the construction of the Computer-based Patient Record Institute and was the Institute of Medicine's most widely distributed publication. Since merely recasting the medical record wasn't enough, a complete rethink was needed. Thus the medical record became known as the Computer-based Patient Record (CPR) and twelve essential functions were associated with it.

The most spectacular change since then was the explosion in the use of the World Wide Web. This presented a potential increase of e-health and CPRs. In the latter half of 2003 the National Library of Medicine licensed SNOMED-CT, an EMR standard, for use by health care organizations throughout the United States (Berner, et al., 2005).

The richness and variety of medical concepts are major barriers to formulating a widely accepted and standardized clinical vocabulary that is suitable for encoding patient-specific information in the electronic medical record (Shortliffe, 1999). However, it is generally accepted that standards are needed to allow the EHR to be used on a wide scale. The issue of standardization is expanded on Section 4.

Terminology

Because of the extemporized use of the three afore-mentioned terms (CPR, EMR and EHR) in the medical healthcare profession, there is somewhat misunderstanding and confusion between the different medical healthcare systems. Although various definitions are available from the literature, the truth is that there is no single general description that successfully classifies these three terms. The first published international EHR technical specification "ISO/TS 18308: 2004 Health Informatics-Requirements for an Electronic Health Record Architecture" contains seven different definitions drawn from four countries, each reflecting slightly different shades of meaning between different countries and organizations (Health Level Seven, Inc., 2004). The truth is that this plethora of definitions typically has more similarities than differences and often merely constitutes a different perspective on the underlying data.
The difference between these systems is subsequently discussed.

The Computer-based Patient Record (CPR)

A CPR is described as a lifetime patient record that includes all information from all specialties and requires full interoperability. However this specific definition is unlikely to be achieved due to implementation issues (Waegemann, 2003).

The U.S. Department of Defense, Veterans Affairs and the Indian Health Service originally set out to create an electronic patient record by using a backbone layer that would serve as an information mediator among various legacy systems (Carter, Brown, Nelson, Lincoln, & Tuttle.). This would be called the first definition of a CPR. The CPR has also been viewed as not a product or an object. The CPR is rather described as a set of processes that are put into place and supported by technology (Shortliffe, 1999).

The Electronic Medical / Patient Record (EMR / EPR)

An EMR/EPR is similar to a CPR, but does not necessarily contain a lifetime record and rather focuses on relevant information. It also has full interoperability within an enterprise (hospital, clinic, practice) (Waegemann, 2003).

The EMR is sometimes described as an "alphabet soup" due to all of the various names that it has been called, some of these being Clinical Data Repository and Electronic Patient Record. The problem does not end at what to call it, but also its definition. According to the Japan Association of Medical Informatics (JAMI) a standard EMR does not cover all application areas, but must support an order transmission system and an order result reference system for all types of application areas (Japan Association of Medical Informatics, 2003). For the purpose of distinguishing the EMR from the CPR and EHR, Ondo, Wagner and Gale define it as "a complete on-line record that is accessible to all that need it when it is needed" (Ondo, Wagner, & Gale, 2002).

The Electronic Health Record (EHR)

An EHR is a form of electronic storage that provides instant availability of information to authorized practitioners, which includes enhanced access to medical information and greater efficiency (Waegemann, 2003). As per the scope of this research paper, the concept of EHRs will be further investigated in Section 3.

From 40 years ago until today, the electronic healthcare system has seen some tremendous advancement. But are these advancements really enough? Are health care workers content with the current systems? Currently the levels of use of EHRs is still low, although there is a heightened awareness of and interest in the technology. After expanding on the concept of EHRs in Section 3, the issue of standardization is addressed in Section 4. Section 5 investigates the factors that hamper the adoption of EHRs.

Electronic health records (EHRS)

Overview of EHRs

Although ISO was not able to define the EHR back in 2000, they were able to define what functions the EHR should perform. The main purpose of the EHR is to supply a standard record of care supporting present and future care by any clinician. This will be of tremendous assistance by allowing any clinician to know a patient's prior conditions even if they are new patients.

The EHR also has a number of secondary uses: medico-legal, quality management, education, research, public and population health, policy development, health service management and billing/finance/reimbursement (ISO, 2000, online, pg. 10-11). Another possible definition was put forward by the Electronic Health Record Taskforce in 2001. According to them, based on the essentials that people were looking for: "An electronic health record is an electronic longitudinal collection of personal health information, usually based on the individual, entered or accepted by health care providers, which can be distributed over a number of sites or aggregated at a particular source. The information is organized primarily to support continuing, efficient and quality health care. The record is under the control of the consumer and is to be stored and transmitted securely" (Smallwood, 2001, p. 3).

One of the greatest incentives to adopting EHRs will be through reaching a critical mass of information sharing - like the first few people with telephones or electronic mail, investors in health care information technology are by and large dealing with internal information systems unable to interact with outside systems (Ash & Bates, 2005). While the adoption of this technology has been slow, it does have a number of advantages, including enhanced access to medical information and greater efficiency (Calgary Health

Region, 2003, online, pg. 1). The typical functions of an EHR are now expanded on in the form of highlighting the advantages of EHRs in general.

Advantages of EHRs

EHRs have a number of functions that will help benefit not only healthcare workers, but the patients as well.

Decision-Making

The EHR will assist health care providers to make decisions using the most up-to-date and precise information. Decision-making will be expedited. For example, diagnoses can be based on tests already conducted, the results of which will be retained by the EHR. The necessity of running duplicate tests will be eliminated and decisions can be made immediately. The EHR will also aid clinicians' decision-making by providing access to patient health record information where and when they need it and by including evidence-based decision support.

EHRs contain a number of other features that help to improve decision-making. These features include an evidence-based reminder system and provision for compliance and prescription cost containment (EPC Task Force, 2005). These reminder systems have shown to significantly advance preventative practices in a number of areas. These areas include vaccinations, breast cancer screening, colorectal screening and cardiovascular risk reduction. There are even studies that show a positive effect on improving drug dosing, drug selection and screening for drug interactions (The National Academy of Sciences, 2001). This all contributes to improved health care delivery.

Improved Accessibility

By providing wide scale connectivity, authorized staff will be able to securely and quickly access patient information to help make decisions on patient care, wherever they need care. The EHR vastly improves the efficiency and effectiveness of the information retrieval function (EPC Task Force, 2005).

Accessibility is taken a step further by providing the patients access to their medical records. They are allowed to enter certain information into their records to help medical staff verify medical record accuracy (EPC Task Force, 2005). This recognizes input from the patient from the perspective that they can note symptoms on a regular basis to facilitate the creation of a record of how and what they feel. These notes from the patient (over time) may assist to increase the accuracy of diagnoses.

Time Efficiency

The EHR computerizes and reorganizes the clinician's workflow to improve efficiency. The EHR also supports the collection of data for uses other than direct clinical care, such as billing and quality management (HIMSS EHR Committee, 2003). Gone are the days of lost patient folders and unnecessary tests, all of which optimizes time efficiency and overall quality of health care delivery.

Patient Safety

Patient safety is improved through keeping record of prescribed drugs, allergic reactions and any existing medical conditions to name a few (Calgary Health Region, 2003, online, pg. 1). The evidence-based reminder system helps remind medical staff about all types of disease prevention and early detection screening tests (EPC Task Force, 2005). This enhances patient safety since health care workers are constantly reminded about these tests and prevention steps to always be aware of their patients' health.

Enhanced Health Information Management

The EHR will enhance health information management by eliminating the need to transport records for completion and providing major reduction in storage space requirements. The evidence-based reminder system that helps with decision making is also used in health maintenance (EPC Task Force, 2005). Another way the Health Information Management is improved is the fact that the EHRs are dependant on medical knowledge. Thus the EHRs continually update the evidence-based rules that also support patient safety (EPC Task Force, 2005).

Enhanced Revenue Management

Revenue Management is the science and art of enhancing firm revenues while essentially selling the same amount of product (Bell, 2005, p. 5). The EHR will also help enhance revenue management by eliminating denials due to lost charges and improves the ability to justify charges (Quadramed, 2004).

Results Management

This advantage correlates to some of the afore-mentioned advantages. The computerized records provide easy accessibility to medical data at the time and place it is needed. Reduced lag times greatly improve time efficiency and patient safety. Patient safety is improved due to quicker recognition and treatment of medical problems. Furthermore any previous test results are displayed thus reducing redundant tests being run which helps to further reduce time wastage.

Finally electronic results can allow for better interpretations and since various providers will be linked together, critical linkages and care coordination are enhanced (The National Academy of Sciences, 2001).

The realization of all the advantages discussed in Section 3.2, are highly dependent on standardization efforts for EHR systems across the world.

STANDARDIZATION

The EHR is not a physical system as much as it is a concept. This concept is realized through a collection of various standards. There are three main standards bodies currently active in international standards directly related to the EHR, viz ISO (International Standards Organization), CEN (Committee European Normalization - the European Standards Organization), and HL7 (Health Level 7) that is U.S.-based but now has over 20 international affiliates (Health Level Seven, Inc., 2004).

EHR standards, as classified by an ISO EHR *ad hoc* Task Group (Health Level Seven, Inc., 2004), will be discussed in the following subsections.

Core Interoperability Standards

There are four pre-requisites that are necessary to attain interoperability of medical information within the EHR. Firstly, a standardized EHR reference model and a standardized service interface model are needed to provide functional interoperability. The reference model must provide an information architecture between the sender and the receiver of any information being sent. The service interface model will provide interoperability between the EHR system and any other necessary components (eg access control and security services) within an inclusive clinical information system.

The other two pre-requisites are also connected. A standardized set of domain specific concept models provides archetypes and templates for various domain-specific concepts, whilst standardized terminologies support these archetypes (Health Level Seven, Inc., 2004).

Interoperability is arguably the single most important benefit of EHR standards since this is the area most lacking in health information management today (Health Level Seven, Inc., 2004).

Content Standards

Content standards are a significant group of standards that can be broken down into “content standards for the EHR” and “content standards for EHR systems” (Health Level Seven, Inc., 2004).

The content standards for the EHR includes standards for data elements including minimum data sets and disease registers, as well as standards for data element content of parts of an EHR. These content standards may also contain standards for transmission of standardized data sets. This differs from the content standards for the EHR system as these (EHR system) content standards refer to functional content of EHR systems (Health Level Seven, Inc., 2004).

Standards for EHR-related services

There are certain EHR-related services that would be better handled by Technical (TG) and Working (WG) Groups within those specific service areas. However, there are areas such as access control and consent management standards that will be handled best by a joint effort between an EHR TG/WG and a specialist TG/WG. There are other services though that are best left to the EHR TG/WGs. The main area that falls into this category is patient/clinician identification demographics (Health Level Seven, Inc., 2004).

Standards for specific EHR technologies, sectors and stakeholders

These standards often occur because of a lack of generic standards and would only be necessary to allow interoperability between specialized and generic EHR standards.

There have been legitimate instances of the need for special interest versions of generic EHRs. In these instances, the underlying functional model and function set ensures compatibility as they are the same. These standards are further being extended to allow realm-specific specializations. This will allow a care profile in one country to be different from a care profile in another country (Health Level Seven, Inc., 2004).

EHR Meta Standards

The EHR Meta Standards deal with the high-level standards. The main standards include the ISO Emergency Framework, the Health Indicators Conceptual Framework, the Health Informatics Profiling Framework and an EHR Enterprise Architecture standard (Health Level Seven, Inc., 2004).

The issue of standards is receiving increasing attention and good progress is being made (Ash & Bates, 2005). There is general consensus in the health care environment that the success of the health care system (public and private) is dependent on the ability to consolidate information from a variety of sources - it is recognized that this ability is dependent on the standardization of health information (Committee on Standardization of Data and Billing Practices, 2003).

FACTORS AFFECTING EHR IMPLEMENTATON

Background and Statistics

The various factors and forces that influence the acceptance of EHRs differ within two settings: firstly there is the inpatient setting and then there is the outpatient setting. According to the American College of Medical Informatics (ACMI), this distinction relates to a difference in the strength of the factors rather than the number of types (Ash & Bates, 2005).

The ACMI believe that the main area where the EHR lacks is in the actual acceptance of the EHR. In fact, after a survey was conducted in 2002 by the ACMI, 83.7% of respondents in the USA did not have anything resembling a Computerized Physician Order Entry (CPOE) system, 9.6% responded that they had CPOE fully available and 6.5% responded that CPOE was partially available. This survey also determined that most of the hospitals within the inpatient setting with CPOE were either Veteran Affairs or military hospitals. Furthermore if these hospitals are expelled from the survey, around 6% of other hospitals fully implement CPOE. Even though a comprehensive survey is not available for the outpatient setting, the level of EHR acceptance is estimated at between 5% and 39%. Further data from the HIMSS mention that there is a 10% adoption gap in the pediatric practice while there is more than a 40% adoption gap in the internal medicine practice (Ash & Bates, 2005).

Security Concerns

With consideration for the context of EHRs and various facts presented about the adoption of this technology, the focus now shifts to the fact that security is considered (at least by some) as a major barrier to the implementation of EHRs.

As recent as 2005, a man by the name of Gordon Atherley argued that there would be problems with the EHR as it is a new technology – he asserted that EHRs consume too many resources that could be used to improve healthcare service delivery or development and if public policies fail, then people within the organization will lose confidence, especially in healthcare information technology. Atherley therefore conducted a study to try to prove his arguments were correct. His study showed that the main concern about EHR adoption was security, in particular people felt that privacy and confidentiality were undermined too much and felt that this was a severe public risk. Another chief security concern was the possibility of breakdowns in security occurring during implementation.

Atherley's study concluded that the public was still enormously concerned about both security and availability issues concerning the EHR (Atherley, 2005). While his study did not intend to discover security issues, it did end up exposing people's concerns about security within the EHR. Physicians do not concern themselves with the security aspects of a program as they feel that the Information Technology department should be monitoring the security features (Ash & Bates, 2005).

Another security issue is that since the EHR is designed to provide wide-range, even remote, connectivity this leaves the EHR open to security holes and flaws. It has also been suggested that a medical information officer be appointed to understand the implementation strategies (Ash & Bates, 2005).

In another study that was initiated to determine problems during the EHR setup, some security issues were also uncovered. When the results were released, the experiment showed that there were two major security concerns: users and administrators were commonly concerned about data loss and their other concern was about privacy, as there was no reliable way to predict who would need access to the EHR and who wouldn't (Tonnesen, LeMaistre, & Tucker).

Considering the concerns relating to security and privacy as mentioned above, the rest of Section 5.2 categorizes the concerns in terms of technological, organizational and governance / legislative factors, with a view to showing that these factors must be controlled to ensure effective and secure operation of EHRs.

Technology Issues

As stated previously, one of Atherley's arguments was that the EHR was too new of a technology to be implemented. This is a valid point because if the medical staff does not know how to use the technology correctly, then problems can occur. Therefore the staff needs to be trained thoroughly on how to use the EHR. However training creates its own problems. While medical staff is more technologically savvy now-a-days, they will still need to be taught how to use the system. We are generally doing a poor job of training future clinicians in the role that computing and communications technology can and should play in our health-care system, and are thereby leaving them poorly equipped for the challenges and opportunities they will face in the rapidly changing practice environments that surround them (Shortliffe, 1995).

As long as training is occurring, health care workers will be taken out of the office and will not be able to perform their daily routine. This is not a unique scenario and applies to any environment where training is required. Due to time constraints, some institutions may rush the training courses, perhaps not teaching security precautions well enough. This could lead to security-related problems, such as staff leaving the system open to unauthorized people.

From a technological point of view, openness versus proprietary solutions is still debated. Some people feel strongly that all vendors should make data sharing as free as possible, while others feel that such ease of sharing could be a problem. For one thing, if data is too freely available then privacy and confidentiality concerns are raised (Ash & Bates, 2005). These issues (privacy and confidentiality) are further put at risk by the fact that individual unique identifiers are envisaged for each possible patient. These unique identifiers would not only be hard to implement, but would also bring about immense privacy concerns.

Clinics also want remote connectivity to be included in the EHR system to allow their staff to access the patient medical records from their very homes (Ash & Bates, 2005). This would create an even bigger security risk then the unique identifiers if not properly monitored. Accessing important and confidential patient information via the Internet for example would open the hospitals network to anyone with a hacking tool or hacking experience.

With regards to the technological problems, it must be ensured that any technology training that the staff may be given is run properly and at a pace that will allow all staff members to obtain a proper grasp on the EHR technology. It must also be ensured that technology (eg encryption) be used appropriately to protect information sent between medical facilities and accessed by medical staff as part of their daily work.

Organizational Issues

From a change management perspective, EHRs (as with any other information system) cannot be implemented without obtaining the support of medical staff and other users of the system. Resistance to change could be very problematic in terms of the success of an EHR project.

Clinicians and other users might feel that the EHR may interfere with their workflow and will not support the EHR implementation. Consequentially, if clinicians believe that management wants to try and force them into using the EHR, they may dig in their heels. This may lead to ignorance towards the use of the EHR systems by the clinicians, which may open up security holes.

Conversely, the drive towards the use of the EHR may come from other sources. If the momentum comes from the clinical staff, other clinicians may be more willing to adopt sooner, and promptness may be at a higher level. One estimate of readiness is the extent to which certain categories of people hold positions within the organization. In particular, administrators at the highest level should offer both moral and financial support as well as demonstrating that they actually believe in the patient care benefits of the systems (Ash & Bates, 2005).

The bottom line is that regardless of who initiates an EHR project, proper change management principles must be applied.

Another question is about ownership of the EHR. In many cases EHRs are being created at the institutional level. These systems are largely funded by the institutions themselves. Secondly, a growing number of health services are being provided outside the publicly funded or government-financed system. These services are provided either by private service providers or via private insurance. There may even be a move toward individuals either administering their own EHR or hiring the services of a third party company to manage their EHR. These different possible owners do not provide full interoperability thus leading to the issue of linking these separate systems being very problematic for security reasons (Office of Health and the Information Highway Health Canada, 2001).

While the organizational concerns can prevent the adoption of the EHRs, these issues can not be blamed on the actual concept of the EHR as it should be the responsibility of the organization to deal with these problems. The organization's managers and its individuals need to come up with an agreeable solution that will suit both sides. In this way they could encourage both sides to accept the changes that an EHR would bring about.

Governance/Legislation Issues

While EHRs have improved technologically over the years, policies aimed to help speed up EHR implementation have not been able to keep up with these changes. The two most important policy issues that need to be agreed upon are privacy and liability.

Privacy entails a person's right to decide when, how and to what level they share their personal information. Some of these privacy concerns include what information should be included, who should have access, which information and under what circumstances should that data be shared with other health providers, how will a patient access their own records and when will the patient need to give consent. The requirement for international interoperability provides even more barriers to privacy. Adopting solutions from other countries is difficult since countries have different ways of handling privacy (Office of Health and the Information Highway Health Canada, 2001). HIPAA's own privacy standards present another alarming difficulty to the use of the EHRs. Even though the HIPAA stipulates privacy requirements in the "Privacy Rule", this rule does not predict the type of unhindered sharing of information amongst entirely distinct health care providers (Culbertson, 2005).

CONCLUSION

This paper investigated various points of view amongst researchers as to whether the disadvantages of health information systems outweigh the advantages with regards to security in particular. Both sides of this argument were examined through literature studies.

While it could be argued that both points of view have merit, we come to the conclusion that using concerns about the security and privacy of health information as a reason not to implement EHRs / healthcare information systems, does not carry weight.

A 1997 study by the US-based National Research Council pointed out that the major vulnerabilities of storing electronic health information are related to inappropriate use of patient-specific information by health workers who have access to those data as part of their regular work (Shortliffe, 1999). Seen in this light, the study postulates that such risks are as great or greater when data are stored in paper charts.

In a study conducted at a public hospital in the Eastern Cape, a very high percentage (95%) of staff agreed that patient folders are not readily available (Nkundla, Pottas & Eloff, 2004). This emphasizes that the availability of paper-based data continues to be a problem. A report from (Tonnesen, et al.) states that the data loss electronically has been nil, while the inability to find paper-based data continues to be a major problem.

These examples call attention to the fact that EHRs can improve the security and privacy of health information. The transformation of healthcare information systems to support greater accessibility and standardization (even across continents) is eminent. In order to ensure that adoption of the concept of EHRs improves, it is recommended that more attention is paid to implementing proper technological, organizational, governance / legislative and other relevant frameworks, to support the environment. This should dispel the misconception that security and privacy-related issues are considered as barriers to the adoption and use of EHRs.

REFERENCES

Ash, J. S., & Bates, D. W. (2005, Jan/Feb). *Factors and Forces Affecting EHR System Adoption: Report of a 2004 ACMI Discussion.* Retrieved March 31, 2006, from http://www.jamia.org/cgi/reprint/12/1/8.pdf

Atherley, G. (2005). Evidence of Public Value and Public Risk of Electronic Health Records: An Issue for Social Justice? *ElectronicHealthcare, 4*(1), 96-103. Retrieved March 15, 2006, from http://emruser.typepad.com/canadianemr/ Articles/EHR_Atherley.pdf

Bell, P. C. (2005). *Revenue Management.* Retrieved April 17, 2006, from http://www.ivey.uwo.ca/faculty/ Peter_Bell/RM%20Ahmedabad%202005.pdf

Berner, E. S., Detmer, D. E., & Simborg, D. (2005, January/February). Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States. *Journal of the American Medical Informatics Association, 12*(1), 3-7. Retrieved April 3, 2006, from http://www.jamia.org/cgi/reprint/12/3.pdf

Carter, J. S., Brown, S. H., Nelson, S. J., Lincoln, M. J., & Tuttle, M. S. (n.d.). *The Creation and Use of a Reference Terminology for Inter-Agency Computer-based Patient Records: The GCPR RTM Demonstration Project.* Retrieved February 15, 2006, from http://adams.mgh.harvard.edu/pdf_repository/D010001512.pdf

Committee on Standardization of Data and Billing Practices. (2003, February). *Recommendations of the Committee on Standardization of Data and Billing Practices.* Retrieved April 19, 2006, from http://www.medicalschemes.com/publications/ZipPublications/Presentation%20Papers/StandardisationManual.pdf

Culbertson, W. (2005, November 17). *Legal and Privacy Impacts of Electronic Health Records (EHR) and the National Health Information Network (NHIN).* Retrieved April 12, 2006, from http://www.sharpworkgroup.com/presentations/WEDI111705.pdf

EPC Task Force. (2005, June 6). *Interim report of the EPC Task Force educational activities of Electronic Medical Records.* Retrieved April 5, 2006, from http://edaff.siumed.edu/Committees/EPC_EMR/Interim%20Report%20of%20the%20EPC%20EMR%20Task%20Force%2006062005.pdf#search='EHR%20Advantages'

Health Level Seven, Inc. (2004). HL7 EHR System Functional Model: A Major Development Towards Consensus on Electronic Health Record System Functionality. Retrieved April 12, 2006, from http://www.ehr-s.org/walt/SanAntonio/EHR-S%20DSTU%20Ballot%20Package/Reference%20Documents/HL7_EHR-S_DSTU_White_Paper.pdf

HIMSS HER Committee. (2003, September 24). HIMSS Electronic Health Record Definitional Model Version 1.1. Retrieved March 15, 2006, from http://www.himss.org/content/files/ehrattributes070703.pdf

Japan Association of Medical Informatics. (2003, February). JAMI Viewpoint Concerning the Definition of the Electronic Medical Record. Retrieved February 12, 2006, from http://www.jami.jp/denshikarute_en.pdf

Nkundla, S., Pottas, D., & Eloff, M.M. (2004). The Protection of Public Health Data - A Case Study. Proceedings of the ISSA (Information Security South Africa) Conference held in Midrand, Johannesburg, 2004. Proceedings on CD.

Office of Health and the Information Highway Health Canada. (2001, January). Toward Electronic Health Records. Retrieved April 14, 2006, from http://dsp-psd.communication.gc.ca/Collection/H21-166-2001E.pdf

Ondo, K. J., Wagner, J., & Gale, K. L. (2002). The Electronic Medical Record (EMR), Hype OR Reality? Retrieved March 10, 2006, from http://www.himss.org/content/files/proceedings/2002/sessions/ses063.pdf

Quadramed. (2004). Enabling Your Electronic Health Record. Retrieved March 22, 2006, from http://www.quadramed.com/web/docs2/Brochure.pdf

Shortliffe, E. H. (1995). Medical informatics meets medical education. JAMA 1995, 273:1061-1065.

Shortliffe, E. H. (1999). The Evolution of Electronic Medical Records. Retrieved March 15, 2006, from http://smi-web.stanford.edu/pubs/SMI_Reports/SMI-1999-0782.pdf

Smallwood, R. (2001). Developing a National Electronic Health Record. Retrieved March 10, 2006, from http://www.himss.org/content/files/proceedings/2001/sessions/ses132.pdf

The National Academy of Sciences. (2001). Key Capabilities of an Electronic Health Record System. Retrieved April 5, 2006, from http://www.nap.edu/openbook/NI000427/html

Tipton, H. F., & Krause, M. (Eds.). (2004). Information Security Management Handbook (Fifth). : CRC Press LLC.

Tonnesen, A. S., LeMaistre, A., & Tucker, D. (n.d.). Electronic Medical Record Implementation Barriers Encountered During Implementation. Retrieved March 20, 2006, from http://www.amia.org/pubs/symposia/D005401.PDF

Waegemann, C. P. (2003, May). EHR vs. CPR vs. EMR. Retrieved February 12, 2006, from http://www.providersedge.com/ehdocs/ehr_articles/EHR_vs_CPR_vs_EMR.pdf