2010

Secure exchange of information in electronic health records

Alejandro Flores
University of Wollongong

Secure Exchange of Information in Electronic Health Records

A thesis submitted in partial fulfilment of the requirements for the awards of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

By

Alejandro Flores

School of Information Systems & Technology

2010

Dedicated to
Paulina

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Alejandro Flores
December, 2010

Abstract

Information technology is expected to become an essential tool in providing reliable information for supporting the delivery of health care services. Nevertheless, incorporating such technologies to support the provision of healthcare raises concerns over the protection of patient's information. The technological, social and legal implications regarding the access and release of medical data have to be considered carefully during the implementation of interconnected health information systems. Secure and effective data exchange along with the protection of patient's confidentiality are two issues that electronic health records need to address to make them reliable and secure in a shared care environment. In this thesis, the author explores these issues by analysing several topics regarding electronic health records, communication, exchange of information and security. The result of this analysis provides an understanding of the framework required to support the exchange of EHRs in a shared care environment. The core of this contribution consists in the description of an approach which uses attribute-based encryption to protect the confidentiality of

patients' information during the exchange of electronic health records among healthcare providers. Attribute-based encryption allows the reinforcing of access policies and reduces the risk of unauthorized access to sensitive information. A prototype version of a communication interface based on the proposed solution has been implemented and tested to evaluate its viability. The prototype has shown that attribute-based encryption provides an answer to restrictions presented by traditional approaches and facilitate the reinforcing of existing security policies over the transmitted data.

Acknowledgements

My sincere gratitude goes to everyone that has supported me through this long process.

To both my supervisors, Dr. Khin Than Win and Prof. Willy Susilo. I would like to thank you for their guidance, patience and support through these years. They never stop believing and supporting me in those difficult moments. I am honoured to have been their student.

To the National Commission for Scientific research and technology (CONICYT), Government of Chile, I would like to give my thanks for providing me with a scholarship to support my permanence in the doctoral program at the University of Wollongong. To the University of Talca, Chile, I give my gratitude for your support.

To my family and friends back in Chile and here in Australia, thank you for your understanding, friendship and support during this period.

To Paulina, my beloved wife. Without your love and support I do not think I would be in the position I am at this moment. This has been a long walk that is finally coming to an end. Tomorrow we start our new path, but with you by my side I know that the wherever that path lead us, I am sure it will be filled with joy and hopes. Thank you for being there all the time.

Alejandro Flores

Publications

- Flores, A., & Win, K. (2007, August 20-24). *Analyzing the Key Variables in the Adoption Process of HL7.* Proceedings of the 12th World Congress on Health (Medical) Informatics (Medinfo 2007), Brisbane, Australia, pp 444-448.
- Flores, A., Win, K. T., & Susilo, W. (2010). Secure exchange of Electronic Health Records. In I. Apostolakis, M. A. Chryssanthou & D. I. Varlamis (Eds.), *Certification and Security in Health-Related Web Applications: Concepts and Solutions*, IGI Global: Hershey PA.
- Flores, A., Win, K., & Susilo, W. (2010). Biometrics for Electronic Health Records. Journal of Medical Systems, Volume 34, Issue 5. Available online at http://dx.doi.org/10.1007/s10916-009-9313-6.
- Flores, A., Win, K., & Susilo, W. (2009, November 22-24). *Securing Electronic Health Records: An Overview.* Proceedings of the Asia Pacific Association for Medical Informatics (APAMI), Hiroshima, Japan, pp 17-24.

- Flores, A., Win, K., & Susilo, W. Functionalities of Free and Open Electronic Health Records System. The International Journal of Technology Assessment in Health, Volume 26, Issue 04. Available online at http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7917209.

Contents

List of Figures

List of Tables

List of Abbreviations

ACR-MENA	American College of Radiology – the National Electrical Manufacturers' Association
ADT	Admission, Discharge and Transfer
AFL	Academic Free Licence
AMS	Abstract Message Syntax
ASCII	American Standard Code for Information Interchange
CCM	CORBA Component Model
CDA	Clinical Document Architecture
CEN	European Committee for Standards
COAS	Clinical Observation Access
COM	Microsoft's Component Model
CORBA	Common Object Request Broker Architecture
CORBAmed	CORBA-based standards for healthcare
C-RBAC	Contextual Role-Based Access Control
DAC	Discretionary Access Control
DICOM	Digital Imaging and Communications in Medicine
D-MIN	
DTD	Document Type Definition
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport
EHR	Electronic Healthcare Record
EHRA	Electronic Healthcare Record Architecture
EHCR-SupA	Electronic Healthcare Record Support Action
EPL	Eclipse Public License
FAR	False acceptance rate
FOSS	Free and open source software
FRR	False rejection rate

GCPR	Government Computer-Based Patient Records
GPL	GNU General Public License
HCU	Health Care Unit
HIPAA	Health Insurance Portability and Accountability Act, USA
HIS	Health Information Systems
HISB	ANSI Healthcare informatics Standards Board
HISPP	ANSI Healthcare Informatics Standards Planning Panel
HL7	Health Level 7 Protocol
HSSP	OMG Health Service Specification Project
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IOM	U.S. Institute of Medicine
ISO	International Organization for Standardization
ISO TC 215	ISO - Technical committees 215 - Health informatics
LGPL	GNU Lesser General Public License
MAC	Mandatory Access Control
MPL	Mozilla Public Licence
OCC	Original Component Complexes
OMG	Object Management Group
OSI	Open System Interconnection Reference Model
PDA	Personal digital assistant
PHR	Personal health record
PIDS	Personal Identification Services
PIN	Personal identification number
RAD	Resource Access Decision
RBAC	Role-Based Access Control
SOA	Service-oriented architecture
SOAP	Simple Object Access Protocol
S-RBAC	Situation Role-Based Access Control Model
SSL/TLS	Secure Socket Layer/ Transport Layer Security protocol
TQS	Terminology Query Services
UML	Unified Modelling Language
UMLS	Unified Medical Language System
UP	Unified Process
WSDL	Web Service Description Language
xDT	XML-based eXtensible Data Types definition protocol
XML	Extensible Markup Language

Chapter 1

Introduction

The incorporation of new technologies, specialization of health services the increasing mobility of patients have modified the form in which health care organizations provide their services. The concept of shared care, as well as the technologies that make it possible, have become fundamental in the modernization of the sector. In a shared care environment, remote access to distant data repositories along with the exchange of relevant electronic health records (EHRs) is essential not only for allowing communication among health providers but also in providing valuable information for the integral delivery of health care and related services. Under this reality, Internet becomes the natural platform to support such functionalities. However, the insecure nature of the network and the increased amount of health information transmitted through it raise the concern over the secure exchange of EHRs and, therefore, the need for

new methods and technologies to safely deliver highly sensitive information has it is with EHRs (Ohno-Machadoa, Silveira, & Vinterbo, 2004).

The disclosure, transmission and use of patient's data with the purpose of supporting the delivering health care services is an expanding practice that draws the interest but also the concern among patients, physicians and health institutions. The access and retrieval of sensitive information of individuals need to take into account the fact that any inappropriate disclosure of data could profoundly affect the personal or professional life of a patient. For this reason, health information systems (HIS) should consider the incorporation of safeguards to guarantee the confidentiality of the stored information. In a dynamic and demanding environment, such as health care, a patient's confidentiality can only be guaranteed by incorporating security services and mechanisms along with common security policies and/or conflict resolution policies to protect the data not only locally but also when information is shared with other health organizations (Lopez & Blobel, 2009). Additionally, EHR systems should guarantee the protection of patients' confidentiality and, at the same time, ensure the reliability and integrity of the information gathered by health care professionals (Conrick & Newell, 2006). Consequently, it is essential that health information systems consider the privacy and integrity of the data and also allow the safe retrieval of information for primary and secondary uses (Lusignan, Chan, Theadom, & Dhoul, 2007).

In the same line, projects centred in the interconnection and integration of health information systems, such as national health information initiatives or multi-

domain EHR systems, are expected to consider not only information and functional requirements but also requirements oriented to protect the privacy and confidentiality of the individuals. Protection of a patients' privacy and the secure disclosure of health information are crucial functionalities that should be embedded within the specifications of modern and reliable electronic health record systems (Conrick & Newell, 2006; Ohno-Machadoa, et al., 2004; Safran, et al., 2007). For this reason, the protection of a patient's privacy has to be understood as a complex issue which requires the consideration of a set of elements that include the correct authentication of users, access control methods, secure transmission of data and security policies, either at the point of origin or at the destination of the communication channel.

Access permissions could be violated even when transmissions have been between trusted parties. For example, let us consider a scenario in which health care institutions A and B are trusted parties that agreed in exchanging electronic health information. Using public key technologies both institutions can transmit information under a secure infrastructure. The secure channel guarantees confidentiality and integrity of the transmitted information. Nevertheless, the possible existence of different access policies may lead to a violation of access permissions either at the point of origin or when the information reaches its destination. Blobel (2006) has suggested the definition of common domain policies to address differences or conflicts generated by differences in the definition of security and access policies that would naturally emerge in a shared care environment (Blobel, Nordberg, Davis, & Pharow, 2006). However,

implementing this approach requires the existence of standardized vocabularies and common policy structures, which are rather limited within the existing health information infrastructure. Access permissions based on roles emerge as the main approach for protecting the data during the communication of medical information and posterior access to the records, access policies based on role-based access control models may facilitate the overcoming of possible violation of access permission (Blobel, et al., 2006; Gritzalis & Lambrinoudakis, 2004), however, role-based access control models also present issues that may increase the risk of unauthorized access to sensitive medical data (Alhaqbani & Fidge, 2007).

In summary, the secure exchange and release of electronic health records not only requires the existence secure transmission protocols but also the definition and implementation of adequate protocols and mechanisms for access and retrieve of information. This thesis aims to address the issues of secure transmission of data in a shared care environment and propose a specification for an information exchange model that allows a secure and safe transmission and release of EHR.

1.1 Background

Electronic health record should not only be considered as a replacement for paper-based medical records but also as a mean to facilitate the access to relevant health information. In addition, EHRs allow the implementation of information infrastructure, which provides support for shared care environments. Communication and the ability to exchange EHRs among the staff involved in providing care to a patient as well as the possibility to access remote data repositories are essential activities for shared care. Additionally, the current and

historical information maintained within the EHRs can also be used as knowledge repositories for continuing treatment of the patient, information for further treatment of the same patient, and for advanced research as well as medical education.

The inclusion of information and communication technologies has facilitated the emerging of software applications that support the activities and services provided by healthcare institutions. In this sense, EHR systems provide a complete information infrastructure that facilitates patient care services and also maintains historical and current data suitable to be used for other purposes such as medical research, development of public policies, medical education (Haux, 2006a) as well as the implementation of profound reforms to health care systems (Haux, 2006b). In a share care environment, EHRs play an important role in the delivery of an integral and professional health care. Nevertheless, sharing EHRs not only should observe the information and technological requirements but also the need for the protection of patients' confidentiality (Blobel, et al., 2006; Blobel & Roger-France, 2001).

New communication technologies such as mobile devices, 3G and wireless networks as well as the increasing interconnectivity provided by Internet facilitate the exchange of health information and allow the access to relevant health data at the point care. In the same way, standardized software make possible the integration and interaction of highly heterogeneous software applications, reducing the time required to exchange medical records through the health care system (Choe & Yoo, 2008). Nevertheless, the application of such communication

technologies carries new issues that need to be considered. In fact, Internet-based management of EHRs requires both common standardized messages, that facilitate the information exchange among heterogeneous electronic information systems, and effective data protection methods, which are needed to ensure confidentiality, reliability and validity of the exchanged information (Blobel, et al., 2006; Choe & Yoo, 2008). Even though, incorporating secure measures during the exchange of EHRs would protect the patient's privacy during the transference of the information it does not ensure the preservation of confidentiality at the communication end points. In effect, to ensure the confidentiality of the patient's information in a share care environment it is necessary to incorporate security services, security mechanisms and common privacy and security policies (Blobel, et al., 2006)

In a shared care environment, protecting the confidentiality of a patient's information is a task that could become rather complex. In fact, the correct identification of users, assigning of access permissions, and resolution of conflict are main points of interest in providing solutions for data exchange among health care providers. Traditional approaches such as Mandatory Access Control, Discretionary Access control and Role-Based Access Control policies do not always provide suitable solutions for health care settings, especially in shared care environments. These and other issues will be discussed in more detail in the following sections of this Chapter. In section 1.2, purpose of and significance of the study, a breakdown of the main issues regarding the access and exchange of electronic health records will be presented. A statement of the problem and its

ramifications is introduced and discussed in section 1.3. Finally, the research question and approach are presented and described in section 1.4.

1.2 Purpose and Significance of the Study

The replacement of the paper-based record by EHRs has been considered an important step forward in facilitating the delivery health services and the enhancement of patient safety and value of health care (Heard, 2006). EHRs have become suitable sources of information for healthcare professionals as well as an essential instrument for the delivery of quality health care (Bakker, 2004). Modern EHR information systems provide benefits such as the existence of reliable and accessible patients' data, the provision of support for logistic activities such as order entry, appointments, discharge information, event management, help and support for health professionals (Bakker, 2004), and information for secondary use (e.g. analysis, research and education, quality and safety measurement, public health and other business and commercial activities) (Safran, et al., 2007). Even though electronic health record systems are considered to be useful tools, there are issues that require to be addressed to gain their main potential in shared care settings. On one hand, functional and reliable inter-domain EHRs require the inclusion of shared concepts as well standardized terminology and standardized information architectures. On the other hand, the process of implementing EHR systems should also take into account the legal and ethical implications of accessing, modifying and sharing medical data, such issues refer to the protection of the confidentiality and privacy of the patient's medical information (Anderson, 2007; Conrick & Newell, 2006).

In a shared care environment, medical records are maintained by different Health Care Units (HCU) involved in the care process. In fact, in a modern healthcare environment different care services are offered by different HCU within the organization or in the healthcare network that involves multiple organizations (Gritzalis & Lambrinoudakis, 2004). Under these conditions, sharing medical record becomes an important task during the provision of care services. Internet is the environment that allows the exchange of EHRs and the interconnection of medical applications (Gritzalis & Lambrinoudakis, 2004). Health information systems developed under shared care environments require the ability of exchanging relevant health information needed to carry on patient's treatments within the health care network. However, the transmission of information under Internet is not free of risk. In fact, Internet was originally designed without the consideration of security measures, which makes the network unsecured by nature. Nevertheless, it is possible to add additional security layers for protecting the information when it is transmitted. Blobel and Roger-France used the concepts of secure connections (secure channels) and secure messages (secure objects) when referring to the use of well-known security technologies used over the transport layer such as the SSL/TLS protocol and security enhanced message technologies based on international health information standards (Blobel & Roger-France, 2001). Such technologies provide security during the transmission of the data but do not guarantee the confidentiality of the information when it reaches the destination point. In fact, the protection of confidentiality would depend on the existing security mechanism of both the sending and receiving applications respectively. Moreover, it would also depend on domain

specifications such as technology, environment and policies (Gritzalis & Lambrinoudakis, 2004).

The exchange of information also requires the consideration of common good practice policies of use and disclosure of medical records (Conrick, 2006; Safran, et al., 2007). Although protection of patient confidentiality is a legal and ethical issue observed by specific legislation, the technical dimension presents a challenge that changes of technology not always address rigorously (Conrick & Newell, 2006). The personal character and sensitivity of the information stored by EHR makes necessary security services that allow the access to authorized users whilst protecting the confidentiality of the patient's information (Blobel, et al., 2006; Blobel & Roger-France, 2001; Gritzalis & Lambrinoudakis, 2004). However, it is not a simple task to design and implement security measures for protecting patient's confidentiality and, at the same time, facilitate the communication of information between health professionals (Agrawal & Johnson, 2007; Gritzalis & Lambrinoudakis, 2004). Issues at this level are associated to the correct establishment of access rights and the development of common policies or conflict resolution policies for allowing the access to authorized users (Blobel, et al., 2006; Blobel & Roger-France, 2001; Gritzalis & Lambrinoudakis, 2004).

Consequently, it is essential to explore the issues associated to the implementation of EHR, especially those related to data security and protection of patient's privacy. This will allow the definition of guidelines for addressing these issues. This field of study provides the possibility to analyse critical issues such as the secured exchange of information among complex information repositories within

different aggregation levels, interoperability in inter-institutional scenarios and patient's privacy policies at local and inter-institutional levels.

1.3 Statement of the Problem

An important functionality provided by EHR is the possibility of access to pertinent health information at any time and location. In fact, electronic information can be easily stored, carried or accessed by a variety of technologies such as flash memories, smart cards and portable devices (laptop computer, PDAs, and cellular phones). Electronic transference among different information repositories also is possible through Internet. This technology facilitates the exchange of health information among health care providers as well as other actors of the health care system. Nevertheless, exchanging data and allowing remote access to EHRs present the need of protecting the information from being improperly released or accessed by unauthorized personnel. In other words, protection of data during the exchange process and protection of patient's confidentiality by the incorporation of security services and coherent policies for primary and secondary are essential in modern EHR Systems (Conrick & Newell, 2006; Ohno-Machadoa, et al., 2004; Safran, et al., 2007).

Secure disclosure and exchange of electronic health records over unsecured communication channels requires the implementation of comprehensive security technologies to allow the exchange of data whilst the protection of patients' privacy is guaranteed (Choe & Yoo, 2008). These technologies should provide mechanisms for access control and define access privileges for information management and protection of data privacy, but at the same time guarantee the

flow of information (Blobel, et al., 2006; Ohno-Machadoa, et al., 2004). At this point, two issues have to be considered for protecting patients' information in a share care environment: (1) secure transition of patient's data and (2) protection of patient's privacy at the communication end points.

During the electronic exchange of medical data, patients' information always has to remain protected, especially the information considered sensitive because the legal and ethical consequences that its unauthorized release could carry. Protection of patient's confidentiality also needs to be considered when the information reaches the destination point. Both security services and mechanism are essential for allowing access to authorized users as well for protecting sensitive health care information (Blobel, 2004; Blobel, et al., 2006). The unauthorized access and release of sensitive information is considered a breach of confidentiality and could lead to issues of public concern such as discrimination, embarrassment or economic harm (Ohno-Machadoa, et al., 2004). The secure exchange of information among different health providers not only depends on secure and standardized electronic mechanisms but also of standardized security policies. In fact, different health institutions might have different security policies, especially in terms of access privileges and release of electronic health records for secondary uses. Incongruent polices may also generate security breaches in the protection of patient's confidentiality and privacy (Choe & Yoo, 2008).

Standard infrastructures, protection of patient's confidentiality and coherent standardized security policies are key elements for the secure exchange of EHRs. A standard infrastructure provides the conceptual and technological framework to

develop data messages for effective exchange of information among actors of a health care network. The legal but also technological dimension of protecting patient's confidentiality is a challenge that has not been effectively addressed by the existing technology. Additionally, the establishment of good practice policies of patient privacy for allowing the protection of the information, even if the information is transferred from one health care provider to another, is also an issue that has not been completely addressed by the current state of the technology. Secure data exchange along with the protection of patient's privacy are two issues that electric health records need to address to make them reliable for an inter-institutional environment. This thesis has the purposes to research issues associated with the secure exchange of EHR and provide a suitable information exchange method for allowing the secure transmission and further use of electronic health records in an inter-institutional scenario whilst confidentiality of information is kept under protection.

1.4 Research Question

In shared care paradigms the access to different data repositories along with the exchange of EHRs becomes essential for providing efficient health care (Blobel, et al., 2006; Blobel & Roger-France, 2001). A shared care paradigm also imposes issues related to access control and protection of patient's confidentiality (Choe & Yoo, 2008; Gritzalis & Lambrinoudakis, 2004). In fact, secure transition of data does not protect against the unauthorized release of information either at the point of origin or destination. Patient's confidentiality can only be achieved by incorporating security services and mechanisms to protect the data against being

accessed by unauthorized users. Additionally, EHR systems not only should guarantee the protection of patients' privacy and confidentiality but also assure the reliability and integrity of the information gathered by health care professionals (Conrick & Newell, 2006).

Therefore, secure transmission of data, access control and user privileges are security requirements that modern EHR system should address. This research aims to address some of the issues described specifically the definition and specification of information exchange models that allow the secure and safe exchange of electronic health records over insecure channels and the incorporation of security mechanisms for protecting patient's privacy. More specifically, to determine:

> *How could the secure exchange and release of electronic health records be supported by incorporating security services in a shared care environment?*

1.5 Research Approach

This research will analyse different approaches used to protect information content in Electronic Health Records and determine which are consistent to be applied for protection of sensitive information. The research methodology is focused on the study of cases and will consider the following stages.

1. Conduct a literature review of the topics associated with the studied domain. The literature review will include the study of different approaches on

information security for electronic health records as well as currently used information standards for exchanging electronic health records, identifying security frameworks currently provided by standards.

2. To define and provide a conceptual proposal for secure exchange of electronic health record.
3. Analyse a set of Open-Source EHR systems in order to select suitable software that will be used during the analysis of the proposed solution.
4. Modify the selected software by incorporating a prototype version of the proposed security solution.
5. Define case studies in which the solution will be analysed and tested.
6. Run simulations and test the prototype based on the case study. The data collected by these simulations and tests will facilitate the validation of a proposal for secure exchange and release or electronic health records.

1.6 Research Scope

As it was discussed in the research question, the final aim of this research is to provide an information exchange model for the secure transmission and release of electronic health records in a shared care environment. Even though through the thesis both primary and secondary use of the health information will be discussed, the focus of the research is primary use and therefore the solution proposed will be primary use of information.

A prototype version has been implemented in order to evaluate the software specification been presented and discussed in the thesis. This implementation would be used to test the proposed solution in a simulated environment based on

case studies. Therefore the scope of this research is to provide a detailed software specification for secure health information exchange at a conceptual level rather than to provide completely functional software with that purpose.

1.7 Organisation of the Thesis

This thesis is organized in seven Chapters. Chapter one provides an overview of the research, with emphasis on the purpose, significance, research goals and scope of the research.

Chapter two gives background knowledge for the research topic through discussions of literature review in the relevant topic area. The literature review initially covers the concept, purpose and dimensions of Health Information System focusing on Electronic Health record Systems. Security and privacy of patient information as well as interpretatively of EHRs in a shared care environment are also addressed in Chapter 2. Health information standards as well as security requirements are the central point of discussion, which leads to a comparison of actual access control models used in healthcare to guarantee the secure access and retrieval of patients' medical information in a cooperative environment. Chapter three describes the methodological process used to undertake this research.

Evolving from this investigation was the development of a conceptual model that allows the electronic exchange of health records using a data encryption method based on attribute-based encryption. The conceptual approach is described in Chapter four.

Chapter five describes the implementation of a prototype based on open source libraries for the three elemental components: HL7 message interface, attribute-based encryption and electronic health record system. Chapter five also provides a set of scenarios for testing the proposed solution and later discussion. The set of scenarios has been developed in order to evaluate the performance of a prototype based on the proposed solution.

Chapter six provides a case study which is used to analyse the viability of the proposed solution under real world situation.

Chapter seven reports on the principal findings of the research as well as provides recommendations based on the research.

Chapter 2

Literature Review

As it has been discussed on sections 1.2 and 1.3 the secure transfer and use of electronic health records depends of the existence and use of standards messaging and data architectures, security services to protect the patient's information during the communication process and the existence of security services and coherent policies for primary and secondary use of information. In this Chapter, all the components will be discussed in detail as well as concepts of health information system (HIS) and electronic health record (EHR). Both, HIS and EHRs, are the basic conceptual elements for posterior analysis and study of secure exchange of information and retrieve in a shared care paradigm. Afterward, the discussion will be centred on standard initiatives for messaging exchange among different health information system, especial attention will be put on Health Level 7 messaging standard. HL7 has the focus of interest of this research on the basis that the proposed solution will be based on the secure exchange of HL7 version 3

messages. Finally, the discussion will be centred on the security services and mechanism for both secure transfer of data (communication security) and secure access and release of information (application security) which is the main focus of this research.

2.1 Health Systems

A system can be understood as an abstract representation of objects or processes, a model or a natural artefact in the real word (Alexander, 1974; Stair & Reynolds, 2009). Following this interpretation, health system could be understood as (1) an interpretation of the health system based on an abstract representation, (2) a descriptive model representing the functionalities of a health system, or (3) the technological, logistical and administrative infrastructure, which relates to the health system. Any of the three, combinations of them or all together can be considered as an interpretation of a health system (Coiera, 2003). A broad interpretation of health care system was proposed by Field in 1973, in this definition health system is understood as:

> *"... The aggregate of commitment or resources which any nation society "invests" in the health concern, as distinguished for the other concerns. The health system is viewed in a structural-functional perspective: it provides services to individuals whose role performance might be jeopardized by ill-health and it occupies a specific structural position in social space." (Field, 1973)*

This definition implies that a health system is a collection of resources (workforce, infrastructure and technology) with a functional structure put in place with the purposes of providing healthcare services to the community. The analysis of the complex structure of Health system is not part of the aim of this research; however, this definition provides a broad understanding of the role that the health system has within the society. In this line, Health Information Systems (HIS) and related technology are a crucial component of infrastructure of modern Health Systems. For this reason, before starting to analyse the central topic of this research it would be useful to understand the role of modern health information systems in a shared care environment.

2.1.1 Health Information Systems

Computer-based information systems have been commonly used in healthcare since 1960s. The principal focus of HIS between the 1960s and 1980s was limited to departmental software applications such as laboratory, radiology and management (Haux, 2006a). During the 1990s, the purpose of research and commercial applications moved to a patient-centred data processing approach as well as through the local and regional integration of health information systems (Haux, 2006a). Currently, the central point of interest is the development of secure and safe health care systems for maintaining electronic health records, exchange of information among health care providers and the generation of medical knowledge based on the health care information. According to Haux (2006), Health Information Systems are applications that collect, store, process and provide data, information and knowledge for the provision of multiple

services in the health care domain. Long and Long (2005) defined the purpose of health Information systems as:

> *"...to provide an organization with data processing capabilities, and knowledge worker with the information required to make better quality and more informed decisions."*

Modern health Information systems provide a variety of services that support all functions of health care institutions such as financial, management, resource management (e.g., supply, storage, and human resource), departmental management (e.g., laboratory, pharmacy, radiology and clinical services), decision support and health knowledge (Ayres, Soar and Conrick, 2006). If a HIS is able to interconnect more than one health care provider, it is known as trans-institutional or inter-instructional health information systems. Examples of trans-institutional HISs are regional health information systems. Regional HISs provide transactional and communicational services for the exchange health information among hospitals, general practitioners, clinics, pharmacies and medical centres. When the health information system process data information and knowledge related with national health indicators is known as a national health information system (Haux, 2006b). In both cases, the information is integrated and shared among several health related organizations.

Information is a critical element for the decision making process in health care. In fact, quality and timely information has become a value resource for the delivery of health care. A well structured and secure HIS provides access to reliable information, which can be used to benefit the health care consumer (patients),

clinicians, and management personnel. The information provided by a HIS could be used for clinical purposes (diagnostic, therapeutic and other procedures), supporting the decision making process, providing access to information needed for advance research and medical education, and facilitating the access to information required in the development of management public plans and policies (Conrick, 2006).

2.1.2 Patient's Health Records

Traditionally, information of patient events and treatments has been kept in paper-based records in order to maintain a historical record that can serve to multiple purposes (further visits, regional or national health indicators, research, etc.). In a paper-based system, most of the collected information is stored in cabinets organized by year, patient's names or other organization or classification method that help to locate the information when needed. The information maintained in this historical paper-based record is normally referred as patient's health records. Patient's health records made possible the service delivery with a focus on patient care in which member of the organization not only can retrieve the information but also can share it with those responsible of a patient's care (Heard, 2006). Although the fact that structured paper-based health records provide a method for maintaining relevant information and support in the delivery of health care, it has several setbacks:

- Historical information of a patient could become difficult to trace due to the increasing numbers of forms used to collect information, redundant record keeping and the loss or misplacement of records.
- There is no automatic mechanism that could be used to relate or retrieve relevant information.
- Any aggregated information might require an important amount of time to be generated.
- Illegible writing makes patient record difficult to understand.
- Misplacement of documents and the effect of environmental variables (humidity, temperature, etc.) over the paper can result in the loss of some or the complete historical information of a patient.

In contrast, the evolution of health information systems and the implementation of communication and information technologies have made possible the collection, storage, retrieval and transference of electronic health information. Patient's information can now be captured and digitally preserved by electronically generated health records. Electronic Health Records (EHR) systems are computer-based application that allows the storage of information collected during patients' events.

2.1.3 Electronic Health Records

EHRs have long been considered an important element in supporting the delivery of health care services. According to Murphy, Waters and Amotegacul (1999) Electronic Health Records can be defined as:

> *"... any information relating to the past, present, or future physical/mental health or condition of an individual which resides in an electronic system(s) used to capture, storage, retrieve, link, and manipulate multimedia data for the primarily purpose of providing health care and health related services."*

This definition is centred in the historical perspective of EHRs. The ownership of the information is not determinate. Moreover, according to the definition, the use of the information collected and stored in EHR is not only restricted to its primary purpose of supporting health care services. In fact, most of the information content by EHR can be used for other purposes such as research, health policies, education, and a variety of commercial activities.

The disclosure of information for primary and secondary uses presents a challenge for the development of secure EHR systems. Patient privacy and protection of data confidentiality have become the main concerns nowadays, especially when most of the information collected by EHR system may be used for other purposes rather than for the delivery of health care. This point will be discussed in more detail trough this chapter.

A definition provided by the Australian's Health Information Network (HIN) (2000) provides a different perspective of electronic health record:

> *"An electronic, longitudinal collection of personal health information, usually based on individuals, entered or accepted by health 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 stored and transmitted securely."*

This definition emphasizes the personal nature of EHR, and the fact that access to the information should be under the control of the patient which becomes the owner. In this case, the owner of the information becomes clear. However, this definition is close to the definition of Personal Health Records (PHR) rather than what would be expected of EHRs. At this point, it would be important to make a distinction between PHR and EHR. PHR could be considered as a variation of EHR in which individuals (patients) can access, manage and share their own health information in a private and secure environment (Tnag, Ash, Bates, Overhage, & Sands, 2006). The information within the PHR is at the disposal of the patient, who can share it with his health providers (Cheow & Win, 2007). More precisely, the access to the information contents in the personal health records would be provided by the patient when and where he is seeking for health care services. On the contrary, EHRs are not always at the immediate disposal of the patient, and they are collected, stored and maintained in the providers' health information systems.

The International Standard Organization (ISO) (2004) has published the following definition for EHRs:

> *"Electronic Health Record is a repository of information regarding the health status of a subject of care in a computer processable form, storage and transmitted securely, and accessible by multiple authorized users. It*

> *has a standardized or commonly agreed information model, which is independent of the EHR system. Its primary purpose is the support of continuing, efficient and quality integrated health care and it contains information which is retrospective, concurrent, and prospective."*

The ISO definition of EHR differs from the definition provided by the Australian HIN, in both the ownership of the information and the access restrictions to the stored data. The ISO definition does not establish a clear ownership over the information storage in an EHR, leaving this aspect open to the specific legislative requirement existing in the region where the health care system is implemented. However, it is clearly implied that the access and transmission of the health information should be protected and that access to medical data should only be allowed to users that have the appropriate credential and access permissions.

2.1.4 Purpose, Dimension and Functionalities of EHRs

The main purpose of EHR is to provide care information for its use in delivering of care services, treatment management, supporting of health care processes, financial and administrative processes, and patient self-management (Bakker, 2004; Safran, et al., 2007). Additional purposes of EHR are the development of quality management, use of the information for medical education and advanced research, support the development of public and population health policies (Heard, 2006).

According to the U.S. Institute of Medicine (IOM) electronic health record are more than a replacement for paper-based health records. In fact, EHRs improve

the accessibility to the health records, facilitate the communication between the staff managing the treatment of a patient, are a repository for all information collected during the treatment of the patient, are a supporting and knowledge repository for continuing treatment of the patient, are a repository of information for further treatment of the same patient, and are data source for advanced research and medical education (Coiera, 2003).

During the implementation of EHR the following ten dimensions should be considered: content of the health data, the captured information, the representation of the information, general dimension and data model, clinical practice, decision support, security, quality assurance, performance and applications.

The U.S. IOM identifies five criteria to define and determine the functionalities of a modern and efficient EHR: (1) improvement of the patient safety, (2) support the delivery of effective patient care, (3) facilitate the management of a chronic health condition, (4) improve the efficiency of health care services, and (5) define feasibility of implementation (Reel and Mendel, 2006). Some of the basic core functionalities of EHR proposed by the U.S. IOM are (Reel and Mendel, 2006; Englebardt and Nelson, 2002):

- Management of complete and accurate patient data and information, ability to study patient outcomes, continuous access for patient care support, practitioner reminders and alerts, result management and clinical Decision Support Systems
- Electronic communication and connectivity to scientific knowledge, institutional databases, registers and other external sources and integration of

data of data and information for multiple health care disciplines and multiple sites.

- Administrative processing of data, data reporting and population health management.
- Facilitation of the use and access for patient, families and practitioners.
- Strong protections of data, confidentiality, and privacy of patients.

2.1.5 Architectural Approaches of Electronic Health Record

One of the most important changes introduced by the modernization of the health care sector is the ability of exchanging medical records using communication and information technologies. An integrated networking electronic health records (EHR) system facilitates the exchange of medical records across the health care system. However, in order to make that possible, the implementation of a unified, clear and standardized architectural model is required. Different approaches have been proposed to assure the secure, efficient and standardized exchange of medical information. In general, the Object-Oriented Methodology and Document-Oriented Methodology are the two major approaches that have been used in the development of standardized health electronic record architectures (Takeda, et al., 2000).

The Object-Oriented Methodology is based on the object-oriented modelling and developing of software. Synapse, Electronic Healthcare Record Support Action (EHCR-SupA), CORBAmed, Government Computer-Based Patient Record US (GCPR) and Health Level 7 (HL7) are some of the standards, which currently use an Object-Oriented approach. Due to its architecture based on object and

components that can communicate through messages, this methodology allows the exchange of data residing in different health care platforms.

The Document-Oriented Methodology is focused on developing a common and standardized architecture for different types of health care documents that can be associated to the patient. A patient medical record contains different types of documents (medical reports, test results, images, prescriptions, diagnosis, etc.) which are associated to the type of service provided. The Document-Oriented Methodology is utilized by the HL7 Clinical Document Architecture (CDA) and by the Japanese MML (Dolin, et al., 2006; Guo, et al., 2005; Guo, et al., 2004; Takeda, et al., 2000).

Another approach is proposed by Blobel (2006), according to his definition, a system that supports the exchange of electronic health record should be under an independent open platform, capable to be scalable, flexible and portable with Internet access, and using international standards that guarantee security and privacy (Blobel, 2006a). In order to accomplish that, Blobel has proposed a Model–Driven Architecture. An approach based on the Model–Driven Architecture and the ISO reference model which would support the entire life cycle needed to develop a scalable and flexible EHR system. The model-drive architecture supports both the Object-Oriented and Document-Oriented methods, depending on what information is shared or exchanged.

Finally, on March 2005, the HL7 consortium group and the Object Management Group (OMG) introduced the Health Service Specification Project (HSSP). This initiative was derived in the development of a new paradigm for health care data

exchange known as the Service Oriented Architecture (SOA). The concept of SOA is not new in the IT domain and has been used in other information domain and software architectures (Atman, 2006). Nevertheless, its incorporation to the health information domain is rather recent. Normally, the architectures used with SOA applications are web services. A web service is a piece of software (component) that has a service behaviour which allows it to provide a diversity of services upon request of client software (Dogac, et al., 2006). The web services are designed to provide a platform for exchanging data based on existing information and system architectures.

In summary, robust EHR architecture should consider the implementation of international standard. The Object-Oriented, Document-Oriented, and Model–Driven methods are the actual basis architecture for much of commercial healthcare software. Moreover, in order to achieve the increasing necessity of information exchange, the development of new health care systems should consider the implementation architectures and interfaces suitable to communicate with different medical software.

2.2 Security and Privacy of Patient's EHRs

The nature of medical records can be described as information provided by a uniquely vulnerable human being, worried in some manner about the core of his very existence, to a trusted person with superior knowledge (Eddy, 2000). In fact, modern electronic health records contain extremely personal and sensitive information regarding not only health history but also the dietary habits, sexual

orientation, sexual activities, employment status, income, eligibility for public assistance and family history of a patient (Choi, Capitan, Krause, & Streeper, 2006). Therefore, maintaining EHRs not only deals with the technological requirements but also with the legal and ethical implications associated. Any unauthorized access and release of personal information contained within a EHR could cause harm on the private life of the patient (Anderson, 2007; Conrick & Newell, 2006). Patients understand the importance of retaining medical information to support and improve the delivery of health care even when they recognize both the sensitive nature of the collected data and the fact that information contended by computerized health information systems becomes more accessible to health professionals, administration personnel, medical staff, and third parties (Conrick & Newell, 2006). For these reasons, patients expect secure health information systems in which personal data is protected and any disclosed information would be used only for health care and related purposes (Grain, 2006).

Even though protecting the confidentiality of patients' information has become a fundamental requirement for modern electronic health record systems, the implementation of security measures could become a rather difficult task. Safe access and exchange of electronic health information requires not only the secure transmission of data but also to ensure that information will be disclosed only to those with the correct access privileges. This implies that protection of patients' privacy needs to be guaranteed during the whole process, this means at the source point, when it is transmitted and when it reaches the destination. In order to protect sensitive medical data, the principles of "need to know" and relevance

apply. Under these premise users should be allowed to access a patient's EHR in order to obtain the relevant information to carry out a task. This access should be provided in concordance with the access and security policies of the organization in which the patient has been treated (Blobel, 2004; Garson & Adams, 2008). The principle of need-to-know is driven by the relevance that the accessed information has in supporting the care of the patient. However, relevancy is an ambiguous concept that depends on the context in which the information is generated and the purposes for which the data has been released. Consequently, the information accessed by a physician should be relevant but also sufficient to provide health care services (van der Linden, Kalra, Hasman, & Talmon, 2009).

Securing medical information is not only a social, ethical and technological matter, but is also about the establishment of well defined privacy policies and legislation. The legal duty of confidentiality is embedded within the professional relationship between physician and patient, and therefore, it has become an essential aspect to be considered when exchanging medical records. In a shared care paradigm, the traditional view of this relationship changes to a relation in which several specialists share sensitive information of an individual. From a perspective in which the mobility of patients as well as the exchange of information becomes more common, the definition of means to efficiently protect the privacy and confidentiality of the patients becomes even more necessary.

Both security services and mechanisms are essential for allowing access to authorized users as well as for protecting sensitive medical information during the exchange of data (Blobel, et al., 2006). Therefore, it is essential for health

information systems to consider both the protection and privacy of patient's data but also the safe and authorized retrieval of information. At this point, it is important to consider that adding excessive security measures could lead to inefficient, more time demanding and less user friendly access control methods. In consequence, defining the correct balance between security requirement and availability of information is a critical goal in a complex environment such as health care (Lopez & Blobel, 2009).

2.3 Social, Ethical and Legal Perspective of Protecting Patient's Privacy

The benefits of electronic health records and how the use of this technology could impact in society are subjects still open for discussion. Nonetheless, the general perception is that incorporating EHRs to medical practice provides a better support in the delivery of health care than paper-based systems by facilitating the access to historical and current medical data of patients (Agrawal & Johnson, 2007; Anderson, 2007). EHR systems are instrumental in maintaining non-fragmented and actualized health information. Therefore, it is essential that health information systems not only be centred in protecting the confidentiality of patient's data but also in allowing the safe retrieval of information for primary and secondary uses.

The incorporation of EHRs and computer networks benefit different actors of the healthcare industry. Studies indicate that fragmented and inaccessible paper-based clinical information affects both the cost and quality in the delivery of health care

and related services (Anderson, 2007). Therefore, information technology is expected to be a necessary tool in solving these issues and supporting the delivery of health care. Nevertheless, incorporating communication and information technologies to support healthcare and related services raises concerns over how privacy and confidentiality of patient information would be protected, especially considering that information stored by EHR systems is extremely personal (Choi, et al., 2006; Goldschmidt, 2005). In this sense, concern over protection of privacy and confidentiality of patients' information has also become a barrier for the adoption of Electronic Health Records. According to Anderson (2007) and Rash (2005), many health professionals and patients fear that electronic health records may present security breaches and that stored data, especially those data collected by web-based EHR systems, may be easily accessed by unauthorized users (Anderson, 2007; Rash, 2005). Having the complete medical history of an individual within a highly accessible electronic format increases the public concern regarding the protection of privacy of the individuals. Moreover, allowing access not only to local user but also external parties has modified the traditional approach regarding confidentiality of medical information. Traditionally, protecting the confidentiality of the information has been the responsibility of the physician and/or the institution that holds the patient's medical records. In a shared care setting, the provision of health care services becomes a multitask activity in which the interaction of multiple actors is required not only for providing health care but also for keeping records and protecting the confidentiality of health information (Blobel, et al., 2006).

Table 2.1: Comparison of Data Protection Principles

General principles of health informatics ethics (1)	European convention for the protection of human rights, Article 8 (1)	Convention: automatic processing of personal data (ETS)(1)	The European Data Protection Directive (1)(3)	Australian Privacy Principles Act 1998/ Summarise Privacy Amendment Act 2000 (2)
All persons have a fundamental right to their privacy, and use of data about themselves	Everyone has the right of respect for his private life, his home and his correspondence	Data subjects should be able to defend their rights in relation to their automated data files	Personal data shall be processed in accordance with individuals' rights	Sensitive Information: Limits on the use and disclosure of personal information
Manipulation of a subjects' data must be disclosed in an appropriate and timely fashion		Data subjects should have knowledge about the existence of an automated data file and its contents		Use and disclosure: Solicitation of personal information from individual concern Identifiers: Alteration of records containing personal information
Any data legitimately held about a person must be assured every available security		There should be specific security measures for each individual file that are suitable to its content and format	Personal data shall have appropriate security measures in place	Data Security: Stored and security of personal information
The subject of any set of data has every right to amend said set of data if appropriate		Subjects should be able to rectify erroneous or inappropriate information	Personal data shall be accurate and up to date where necessary	Data Quality: Solicitation of personal information generally Access and correction: Access to records containing personal information
The fundamental right of control over manipulation of personal data is conditioned only by legitimate and appropriate needs	No interference by a public authority except in accordance with the law and interests of national security			Collection: Manner and purpose of collection of personal information Openness: Information relating to records kept by record-keeper Anonymity: Record-keeper to check accuracy of personal information before use Transformer Data: personal information to be use only for relevant purposes
Any infringement of a person's privacy may only occur in the least intrusive fashion	Qualified disclosure of data does not map to data protection principles			
Any infringement of a person's privacy rights must be disclosed and justified in an appropriate and timely fashion	Qualified disclosure of data does not map to data protection principles			

Sources:

1. Lusignan S. d., Chan, T., Theadom, A., & Dhoul, N. (2007). The roles of policy and professionalism in the protection of processed clinical data: A literature review. International Journal of Medical Informatics, vol 76 p. 263.
2. Conrick, M., & Newell, C. (2006). Issues of Ethics and Law. In M. Conrick (Ed.), Health Informatics: Transforming Healthcare with Technology. Melbourne: Thomson Social Science Press. pp. 327-329
3. Agrawal, R., & Johnson, C. (2007). Securing electronic health records without impeding the flow of information. International Journal of Medical Informatics, vol. 76, No. 5-6 p. 471

The disclosure and reuse of patient data for purposes other than health care delivery is also an expanding practice that concerns the interest of patients. The information provided by historical records is a potential source of data for research and knowledge generation that can be used for improving the delivery of health care (Lusignan, et al., 2007). Moreover, electronic health records could also be used for commercial purposes. Security's issues have reached the public concern, especially considering the variety of uses that the stored medical data could provide and the personal, legal and ethical effects that the unauthorized release of information could have (Ohno-Machadoa, et al., 2004). In any case, access to medical data repositories for either primary or secondary purposes has become an essential functionality of modern health information systems.

2.3.1 Privacy Protection from a International Perspective

Under this complex scenario countries such as U.S., Canada, Japan and the member of the European Union have incorporated laws and regulations that aim to reduce fraud and abuse as well as protect patients' health information (Anderson, 2007). International regulations such as that imposed by HIPAA (Health Insurance Portability and Accountability Act) in the United States and the European Data Protection Directive (Agrawal & Johnson, 2007; Lusignan, et al., 2007) demand the highest level of security and protection during the access, processing and exchange of information that involve sensitive data of individuals (see Table 2.3).

The international principles and approaches regarding privacy protection can be related the regulations and legislation that have been implemented by the national

Australian Government as well as the governments of the states and territories. In fact, Australia also possesses a set of privacy principles that regulates the collection, use and disclosure of personal information. Additionally, Australian legislation protects and provides a legal body for people that have suffered harm as a product of unauthorized disclosure or use of private information. In the following sections the more relevant regulations and legislations related to privacy protection in Australia will be presented.

2.3.2 Australian Legislation for Privacy Protection

There are different legal bodies that apply to individual's information that is collected and stored within Australia's private and public sectors. At the federal level, the Federal Privacy Act covers the collection, use, disclosure, quality and security of personal information. Privacy Act 1988 applies to the management of information by Commonwealth public sector agencies. It provides a framework for complaints concerning violations of privacy as well as defines and establishes the role of the Federal Privacy Commissioner. The Federal Privacy Act also applies to the private sector covering large organization, companies and banks as well as small businesses that trade in personal information.

Several amendments have been made since its first publication in the year 1988, especially regarding the management of information by the private sector. The handling of information by private industry is regulated by the Privacy Amendment (Private Sector) Act 2000 (PPIPA, 2009). Both legal bodies are based on a set of privacy principles that should apply during the collection, handle and disclosure of personal information (HealthConnect, 2002). The current

version of the act, promulgated on November 2008, contains 12 information privacy principles that regulate the management of personal information by Commonwealth and ACT government agencies whilst information managed by health service providers and private sector businesses with an annual turnover of over $3 million is governed by 10 national privacy principles. These privacy principles are classified accordantly to (ComLaw, 2006; PPIPA, 2009):

a) Collection: establishes the approach and reasons of collecting individuals' personal information. It also describes the kind of information that organization should provide during the data collection.

    1. Lawful: The information mas be collected for a lawful purpose and directly related to the activities of the agency collecting the data.

    2. Direct: the information must be collected from the individual, unless consent as been given otherwise.

    3. Openness: establishes the responsibility that organizations have in providing access to policies regarding the protection and use of collected information as well as informing individual the reasons for which the information has been collected.

    4. Relevant: the information collected mas be relevant, up-to-day and not excessive.

b) Storage

5. Security: defines the obligation held by organization regarding the protection of personal information.

c) Access: Access establishes the reasons for which access to information could be granted or denied.

6. Transparent: the individual must be provided enough details about the personal information that has been stored, the reason for why the information has been stored and the right that the individual has to access the information.

7. Accessible: the agency must allow access to the information been stored.

8. Correct: the agency must allow updating, correcting or amending personal information if necessary.

d) Use

9. Accurate: institutes the responsibility set by organizations regarding the integrity and accuracy of the collected, used and disclosed data.

10. Limited: information can only be used for the purpose for which it was collected, for a directly related purpose, or for a purpose to which consent has been given. Information can be used without consent in cases of

e) Disclosure: describe the reason for disclosure of information (primary and secondary uses). The Act makes especial reference to the secondary use of Health information.

11. Restricted: information can only be disclose with the consent of the individual. The agency can disclose information for a related purpose and they don't think that individual would object. Information can be disclosed without consent in cases of serious and imminent threat to any person's health or safety.

12. Safeguarded: sensitive information cannot be disclose without the individual consent. Information can be disclosed without consent in cases of serious and imminent threat to any person's health or safety.

2.3.3 Australian States Privacy Legislation for Health Information

Specific legislations regarding privacy of health information have been implementing in different Australian States and territories. For example, the Health Record Act 2000 is a legal body that governs the collection, use and disclosure of individuals' medical information in the State of Victoria (HRAVIC, 2000). In the Australian Capital Territory, the Health Record (Privacy and Access) Act 1997 is the main regulatory body regarding the management of individual's personal health information, data integrity, data accessibility and description of health information (HRPAACT, 1997). Although the Health Service (Conciliation and Review) Act 1995 of Western Australia is not a specific regulation concerning privacy and confidentiality of health information, it establishes liability in those cases in which health providers deny access to personal health data, disclosure information or use health records in means that could compromise the confidentially of a patient (HSCAWA, 1995).

The Health Records and Information Privacy Act 2002 (or HRIP Act) is a normative created to protect the privacy of health information in New South Wales. The HRIP Act establishes regulations concerning the collection, use and disclosure of personal health information in both public and private sectors. The HRIP Act covers the management of personal information by public or private hospitals, physicians, other health care organizations and other organizations that could have access to any type of health information such as universities, gymnasiums, companies and government agencies (HRIPNSW, 2002). Unlike the Privacy Act 1988 and Privacy Amendment (Private Sector) Act 2000 which are based on 10 principles for the private sector, the Health Records and Information Privacy Act 2002 Act contains 15 health privacy principles. The principles establish how health data must be collected, stored, used and disclosed so these activities do not compromise the privacy and confidentiality of the individual from who the information has been collected. These principles are established to regard and regulate the purposes for collecting health information, the relevance and accuracy of the data, the source of the information, openness, retention and security, held information reporting, access, amendments, integrity, limitation of use, limitation of disclosure, use of identifiers, anonymity, transference and data flow and linkage of health records. The Health Records and Information Privacy Act 2002 Act also provides for a number of legal exemptions in which these principles may not apply (HRIPNSW, 2002).

The Federal Privacy Act, along with each of the Acts for privacy protection that actually apply in the Australian territory, provides the principles for securing health information. These principles should be considered when implementing a

health information system that will manage highly sensitive information. In the following sections the concept of security and privacy in shared care environment will be introduced. At this point it is important to understand that each of the principles previously discussed in this section provide the legal framework for exchanging EHRs in a shared care scenario.

2.4 Security and Privacy in a Shared Care Environment

As it was mentioned in section1.2, in a shared care environment, different health care units (HCU) are involved in the care process as well as in maintaining accurate medical records. This requires the communication and cooperation among all actors involved in the administration of patients' care (Choi, et al., 2006). The responsibility of protecting the confidentiality of patients' information is also reflected on the cooperation among the involved HCUs. As in paper-based health records, physicians have an ethical and legal obligation of protecting information of patients in order to prevent potential harm to individuals (Conrick & Newell, 2006). Nevertheless, the nature of EHRs makes the duty of physician-patient confidentiality a task even more complicated. Despite the personal nature of health records, EHRs make patient's information potentially available to anyone that has access to a health information system. Moreover, the current technology also allows the remote access to data repositories in a matter of seconds which intensify the concern regarding the security of electronic transaction involving medical records (Anderson, 2007). This trend would eventually alter the nature of the doctor–patient relationship and threat the quality of health care (Choi, et al., 2006). These apprehensions are also shared by the

public whose primary concern is the security, privacy, and confidentiality of their personal health information (Goldschmidt, 2005; Rash, 2005).

In a shared care environment defining what is considered sensitive information as well as what access permissions are granted to users become uncertain. In fact, each participating institution of a health network would have different approaches when defining the level of sensitivity associated to the information, access rights and the level of security required to protect privacy of patients (Blobel, et al., 2006). Those approaches not only depend on legal restrictions but also are built based on the accumulated experience and the culture of organizations. Since the conception of security and protection of patient's privacy differ from one organization to another, methods for interconnecting health information systems should consider a comprehensive understanding of the complexity of requirements involving the secure exchange and release of medical data. In general, an electronic health record system able to secure and protect the confidentiality of patients should not only incorporate security requirements but also guarantee the flow and availability of the information.

Implementing a shared care environment has several implications not only in how the information is managed or which technology can be used but also in the way in which information is collected, stored and accessed. The exchange of information in a shared care environment exceeds the needs of a locally integrated health information system and calls for the definition of a new set of requirements. Even more, it requires a different approach to overcoming the technical, legal and ethical issues that rise from exchanging highly sensitive

information. In a shared care paradigm, the number of specialist that can have access to EHRs increases and the information contained by EHRs can be broken down among different health information systems within the organization or among different healthcare providers. This disaggregation of information increases the possibility of a security breach. In general, the implementation of the share care paradigm not only requires the support of standardized information system architectures, data exchange protocols and common vocabularies but also protecting the privacy of patients, guaranteeing the authorized access to stored data and protecting the integrity of the information (Blobel, et al., 2006).

2.4.1 Interoperability of EHRs

Achieving interoperability is a main goal of modern EHR systems. The inclusion of the of Information and Communication Technologies (ICT) in the health care sector has permitted the improvement of services, reduction of costs as well as facilitated the flow of information between different actors of the health sector (hospitals, clinics, physicians, researchers, patients, students, insurance offices, general practice and government offices, etc.)(Hebda, Czar, & Mascara, 2005; Shine, 1996). Moreover, the modernization of the health care sector, not only in Australia but also in many developed and developing countries, has imposed the necessity to exchange medical records among different participants of the health care system (Grimson, 2001). However, the complexity of the health information and different methods and systems used for obtaining and storage data have increased the level of complexity in the development of systems capable of sharing and exchanging medical data (Ammenwertha, et al., 2004; Grimson,

2001). In this new scenario, the definition and adoption of national and international standards has turned into a necessity (Blobel, 2006b; Brandt, 2000). Therefore, the understanding and knowledge of those standards is essential in the development and implementation of robust and functional medical information systems. According to the National Health Information Management Advisory Council of Australia (2001) a standard can be defined as:

> *"A published document which sets out specifications and procedures designed to ensure that a material, product, method or service that is fit for its purpose and consistently performs the way it was intended to."*

This definition establishes that standards are specifications of what it is intended to do, the method used to do it and what should be its result. In the health care sector, information standards are used to provide frameworks that support the accomplishment of a diversity of purposes depending on the type of information and the health care domain. For instance, medical informatics standards are used to specify data structure and representation, establish requirements of performance and robustness of information systems, and state methods for the generation, storage and flow of different types of information (management, financial, medical, laboratory, studies, research, patient records, etc.) among health information systems. The concept of information standard and its use in health care information systems will be explored through this Chapter. Principal interest will be centred in standard used for exchange of information, especially in Health Level Seven (HL7) standard.

2.4.2 Standardization and Interoperability in the Health Care Sector

As it has been discussed before, health information systems have become instrumental in providing support to health care activities, reducing the cost of health care, improving the quality of the service, enhancing the health care delivery and providing information for research and education (Haux, 2006a). Furthermore, electronic health information systems facilitate the access to medical information and reduce the time required to exchange medical record through a health care system (Langer, 2002). However, the development and adoption of non integrated health information systems, where implementation has been based on different architectures, information structures and communication standards had increased issues regarding the interoperability and compatibility of medical records, and limited the collection of integrated patient and medical information (Coonan, 2004). In fact, data collected by different health care providers, at different moments and in different places are difficult to interpret and share without considering an efficient information infrastructure based in consensus standards.

The gradual incorporation of medical informatics standards allows the development of adequate infrastructure for health care and overcomes the limitation produced by the adoption of heterogeneous information systems (Hammond, 1995). Additionally, standards facilitate the storage, indexation, processing, and exchange of health care registers. The use of international

standards also permits the achievement of important benefits such as integration of medical information systems (decision support, record-keeping, order entry, etc.), efficient and accurate exchange of medical records, accomplishment of government and local requirements of information, the accessibility to medical data under almost any circumstance and reduction of redundant and erroneous information (Coonan, 2004). In general, the use of standards facilities interoperability, increase the efficiency and effectiveness of the data exchange process, and increase the information flow between applications in the health care sector. Brandt (2000) has defined information standards in the health care sector as:

> *"... a commonly agreed-upon manner of collecting, maintaining, or transferring data between computers systems. Until health care providers collect and maintain data in a standard format according to widely accepted definition, it is nearly impossible to link data from one site to another"(Brandt, 2000).*

This definition emphasizes the use of the data generated during the accomplishment of medical activities and procedures rather than in the implementation of robust and integrated health information systems. In fact, medical information standards provide a common and agreed framework for the development and implementation of integrated software solution.

Standards in health informatics differ according to their purpose and the specific health domain. Hammond (1995) identified four broad categories of standards based on their main purpose: (1) vocabulary, (2) structure and contents, (3)

messaging and (4) security. Another classification establishes that standards are grouped accordantly to the specificity of the standard: (1) general standards, (2) specific standards, (3) contents standards, and (4) clinical vocabulary standards. General standards provide a broad framework for representation, management and exchange of health data. Specific standards afford specific needs related to particular health domains (radiology, clinical care, clinical instruments, etc.).

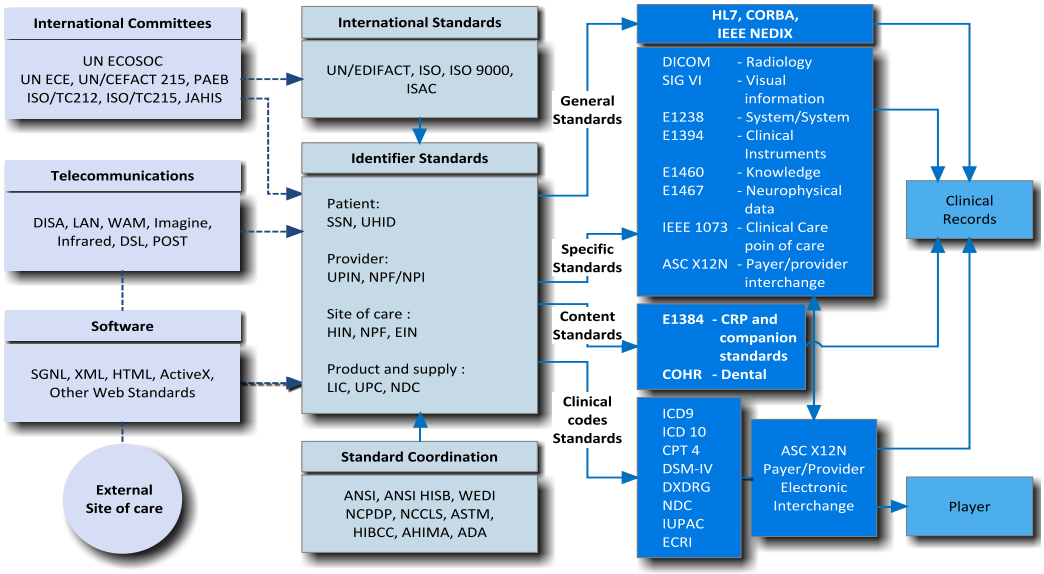


Figure 2.1 : Health Information Standards (Source: Bloom A (2000), Context and Lead-up to health reform: Health Reform in Australia and New Zealand, p. 25)

Content standards are used to provide specific support in the development of software such as dental information systems and electronic health records systems. Clinical code standards provide code and vocabulary used to storage, manage, and exchange health data. The main information standards used by health information systems are shown in the Figure 2.1.

2.4.3 International Standardization Initiatives

2.4.3.1 American National Standard Institute

The American National Standard Institute (ANSI) is an administrative and coordinator institute that promotes and facilitates the voluntary agreement of standards in the U.S. private sector. ANSI is an accreditation institute and does not develop standards. However, the ANSI supports and encourages the development of national and international standard by qualified groups (Englebardt & Nelson, 2002). The ANSI has implemented two instances to promote the development standards for the health care sector:

1. ANSI Healthcare informatics Standards Board (HISB) which provides an open and public forum that coordinates the development of health care information standards organization in United States.
2. ANSI Healthcare Informatics Standards Planning Panel (HISPP), which helps in the coordination of standardization work developed by specific group.

The ANSI is not a standard developing institute, but it provides a framework and support for the development of private standardization initiatives(Hammond & Cimino, 2001).

2.4.3.2 The International Standard Organization

The ISO Technical Committee (TC) 215 was established in February 1998 in order to facilitate the achievement of standards for the Healthcare Sector (Englebardt & Nelson, 2002). The ISO TC-215 activities are divided into five

working groups with specific orientations: (1) Health records and modelling (WG 1), (2) messaging and communications (WG 2), health concept and vocabulary representation (WG 3), security in health information (WG 4), and (5) health cards (WG 5). In 2004 the ISO TC-215 released the technical document 18308:2004: "Health informatics - Requirements for an electronic health record architecture". The ISO technical document 18308:2004 is a compendium of 124 clinical and technical requirements for a standardized Electronic Health Record Architecture (EHRA) that supports the storing, use, sharing and exchange of EHR across different models of health care. It is important to note that the ISO/TS 18208 provides a set of requirements for an EHRA but not establishes the architecture itself (ISO/TC-215, 2004). By 2005, the ISO TC-215 released the technical report 20514: "Health informatics - Electronic health record - Definition, scope, and context". The ISO technical report 20514 establishes the definition scope, context, and a set of categories for electronic health records. Additionally it provides a set of basics characteristics, classification and functional descriptions for electronic health records systems (ISO/TC-215, 2005).

The ISO has developed the Open System Interaction (OSI) Model that provides a basis for coordination and development of standard for interconnection of computer systems (Englebardt & Nelson, 2002).

Due to the complexity of the distributed systems, the ISO recommends the use of the object-oriented methodology (ISO/IEC, 1998). Object-oriented permits modelling and developing robust and well defined applications based on objects and components capable to communicate and exchange information with each

others. CEN, DICOM and HL7 are examples of approaches that use object-oriented methodologies for modelling and implementing standards.

2.4.3.3 The European Committee for Standards

The European Committee for Standards (CEN) was founded with the mission to promote the voluntary technical standardization and harmonization in Europe (Englebardt & Nelson, 2002).

The CEN had created the Technical Committee 251 in 1991 with the purpose of developing information standards for the health care domain. Its principal focus is the development of communication standards for data exchange as well as medical records, code and vocabulary, imaging, security, privacy and confidentiality through the health care system in Europe (Hammond & Cimino, 2001).. Additionally the CEN has developed the ENV 13606 ‘‘EHCR communication’’ that is a communication standard development initiative divided into four components:

1. Extended architecture
2. Domain term list
3. Distribution rules
4. Messages for the exchange of information

2.4.4 Commonly Used Information Standards in Medicine

2.4.4.1 Common Object Request Broker Architecture

The Common Object Request Broker Architecture (CORBA) is standard set developed by the Object Management Group (OMG). The CORBA is a collection of specification orientated to provide a framework for developing distributed and heterogeneous applications (Englebardt & Nelson, 2002).

The CORBA Component Model (CCM) was designed to improve the development and implementation of new distributed applications. Additionally, CORBA definitions have been designed to support different types of platforms (hardware and software), programming languages, and network architectures (Englebardt & Nelson, 2002). One of those specific definitions is CORBAMed, which has been designed to support and use existing health care standards and applications such as HL7, Unified Medical Language (UMLS), and CEN TC 251.

The design of CORBA is based on the ISO standard translation for common middleware technologies such as DICOM, JAVA, CORBA, and XML (Englebardt & Nelson, 2002).

2.4.4.2 Digital Imaging and Communication in Medicine

The Digital Imaging and Communication in Medicine (DICOM) is an industrial standard used to storage and transfer radiological digital images. The DICOM was developed by the American College of Radiology – the National Electrical Manufacturers' Association (ACR-MENA) in 1983 (Hammond & Cimino, 2001).

DICOM establishes the message format and standards for communication of diagnostic images (Englebardt & Nelson, 2002).The DICOM provides a complete network capability and incorporates an object oriented data model and support for ISO standard communications. It also includes specification for related-image information management and exchange. Additionally, DICOM has the capability of interaction with management information systems and radiology information systems, facilitating the access to radiological documents and images (Hammond & Cimino, 2001).

2.4.4.3 Unified Medical Language System

The Unified Medical Language System (UMLS) is a product published by the National Library of Medicine since 1986. The UMLS contains technical medical terms used in the development of medical information applications in order to interpret user's queries, to draw terms for appropriate medical vocabulary used in schemas and to provide a basis for data structured (Engelbrecht, Ingenerf, & Reiner, 2006).

The UMSL contents 800.000 concepts descriptions and around of 1.9 millions of concept names that have been collected from different source vocabulary. It also contains linguistic information of medical terms, syntactic and spelling information that permit the language processing(Engelbrecht, et al., 2006).

2.4.4.4 Health Level 7 Messaging Standard

Health Level seven (HL7) consortium was founded in 1986 to research and develop a set of standards for electronic data exchange in the heath care domain

(Huang, Hsiao, & Liou, 2003). Level seven refers to the application layer, the highest level of the ISO Communication Model. This layer provides the software infrastructure responsible for the data exchange, establishes the time required during the exchange of information, and communicates certain errors generated during the exchange process (Beeler, 1998; Tanenbaum, 2003).

After years of research and development, HL7 has become the most widely used messaging standard for clinical and administrative data exchange among health care applications (Henderson, 2003). The aim of HL7 is to produce standards for particular health care domains and allow the development of specifications for messages model and implementations of software interfaces (Beeler, 1998). To accomplish this aim, HL7 has established a set of standardized information and message models, document architectures and health information vocabulary for the development and implementation of health information software interfaces. As a result of this effort, HL7 standard has become a structured framework for the communication and transmission of medical data among heterogeneous health information systems (Henderson, 2003; Hinchley, 2005).

Since its beginning, the HL7 standard has pursued the improvement of communication and information exchange in the healthcare domain. In more detail, HL7 has provided standards and frameworks that support the exchange of information among systems implemented in a wide variety of software environments, facilitate the immediate transference of single or multiple data transactions, achieve the best possible degree of standardization, and support evolutionary growth of the standard as new requirements are incorporated. HL7

has been built considering existing production protocols and accepted standard protocols suitable to define new message formats and protocols for computer applications in the healthcare domain. It also considers the diverse nature of business processes and information generated during the healthcare delivery, and facilitates the collaboration with other related healthcare standards efforts (HL7, 2006).

2.4.4.4.1 HL7 Version 2

The HL7 version 2.x series have provided a complete and structured framework for both the development of common and well defined communication interfaces and the design of new message specifications. The scope of HL7 version 2.x messages have been the development of evolutionary message specifications for the exchange of medical information through the health care domain (Henderson, 2003). This section contains a description of HL7 version 2.x standard series, codification rules for both ASCII encoding and XML encoding, and its potential limitations.

2.4.4.4.1.1 HL7 Version 2.x Messages

In the HL7 version 2 standard the information contents in the message is combined into logical groups or segments delimited by ASCII characters. Each segment, which may be defined as required or optional, begins with a literal value compounded by three identified characters. Some of the segments or segment groups may repeat. An example of a HL7 version 2.x message is presented in Figure 2.2 (Beeler, 1998; Henderson, 2003).

The message exchange process is initialized by a trigger event, which indicates the cause of the message generation (Henderson, 2003). When the trigger event is activated the information is mapped according to its correspondent Abstract Message Syntax (AMS). The AMS provides segment identifiers and indicates the Chapter of the segment (Beeler, 1998; Henderson, 2003). When the computer application establishes the contents required by the trigger it sends the message through the network. Finally, the message is received and interpreted by the software application located in the destination node.

```
MSH | A\&| MegaReg | UABHospC | ImgOrdMgr | UABImgCtr | 200105290901
31-05001| |ADT^AO1|010S2901|P|2.3.1
EVN | | 20010529090 | | | | 1200105290900
PID| | | 56782445^^^UAReg^PI~999855750^^^USSSA^SS| |IKLEINSAMPL
E^BARRY^Q^JR| |196209101M1 2028-
9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST
DRIVE^^BIRMINGHAM^AL^352O9^^H|| | | | | |0105I30001^^^99DEF^AN
PV1| |I|W^389^1^UABH^^^^3| | | |
1234S^MORGAN^REX^J^^^MD^0010^U
AMC^L| |67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED| | | |AO
| |13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L
OBX|1|NM|^BOdy Height| |1.8O|m^Meter^ISO+| | | | |F
OBX|2|NM|^BOdy Weight| 79|kg^Kilogram^ISO+| | | | | F
AL1|1| |^ASPIRIN
```

Source: Henderson M. (2003). HL7 Messaging: The HL7 Message structire, p. 23

Figure 2.2: HL7 version 2 message

Figure 2.3 presents an Abstract Message Syntax definition for ADT. Some of the trigger events for ADT are admit/visit notification, patient transference, discharge/end visit, patient registration, patient pre-admission, changing outpatient into inpatient, changing inpatient into outpatient, patient information update, admit/visit cancellation, transfer cancellation, discharge cancellation, pre-admit cancellation and merge patient and patient identifiers listing.

ADT^A01^ADT A01	ADT Message	Chapter
MSH	Message Header	2
EVN	Event Type	3
PID	Patient Identification	3
[PD1]	Additional Demographics	3
[{ KM1 }]	Next of Kin / Associated Parties	3
PV1	Patient Visit	3
[PV2]	Patient Visit – Additional Information	3
[{ DB1 }]	Disability Information	3
[{ OBX }]	Observation/Result	7
[{ AL1 }]	Allergy Information	3
[{ DG1 }]	Diagnosis Information	6
[DRG]	Diagnosis Related Group	6
[{	--- PROCEDURE Begin	
PR1	Procedures	6
[{ ROL }]	Role	12
}]	--- PROCEDURE end	
[{ GT1 }]	Guarantor	6
[{	--- INSURANCE Begin	
IN1	Insurance	6
[IN2]	Insurance Additional Information	6
[{ IN3 }]	Insurance Additional Information – Cert.	6
}]	--- INSURANCE end	

Source: ANSI/HL7 V2 XML Encoding Syntax, Release 1 (2003). p. 9

Figure 2.3: Abstract Message Syntax definition for message type ADT_A01

2.4.4.4.1.2 HL7 version 2.x Message Rulers

The HL7 version 2.x family standard states the following structural and encoding rules that should be accomplished by any HL7 message:

1. The abstract message representation uses brackets **[]** to indicate that a segment or segment group can be considered optional (Henderson, 2003). This implies that a segment or segment group included within the brackets is considered a required element. For example, according to the ADT^01 abstract message syntax the segment MSH, EVN and PID are required elements during the message exchange.
2. The abstract message syntax uses braces {} to indicate that a segment or a segment group may be repeat (Henderson, 2003). This implies that a segment or segment group without braces may be not repeated.

3. Segment or segment group should be included in the message in the same order that is specified in its correspondent Abstract Message Syntax (Henderson, 2003).
4. Local variations should consider that the only required fields are those logically required in the corresponding Abstract Message Syntax, other fields must be considered optional (Henderson, 2003).
5. New transactional data elements or fields included to the HL7 standard or to local variation that are implemented in the data source or sender system, should be considered optional fields to avoid conflicts reviving systems not yet updated (Henderson, 2003).

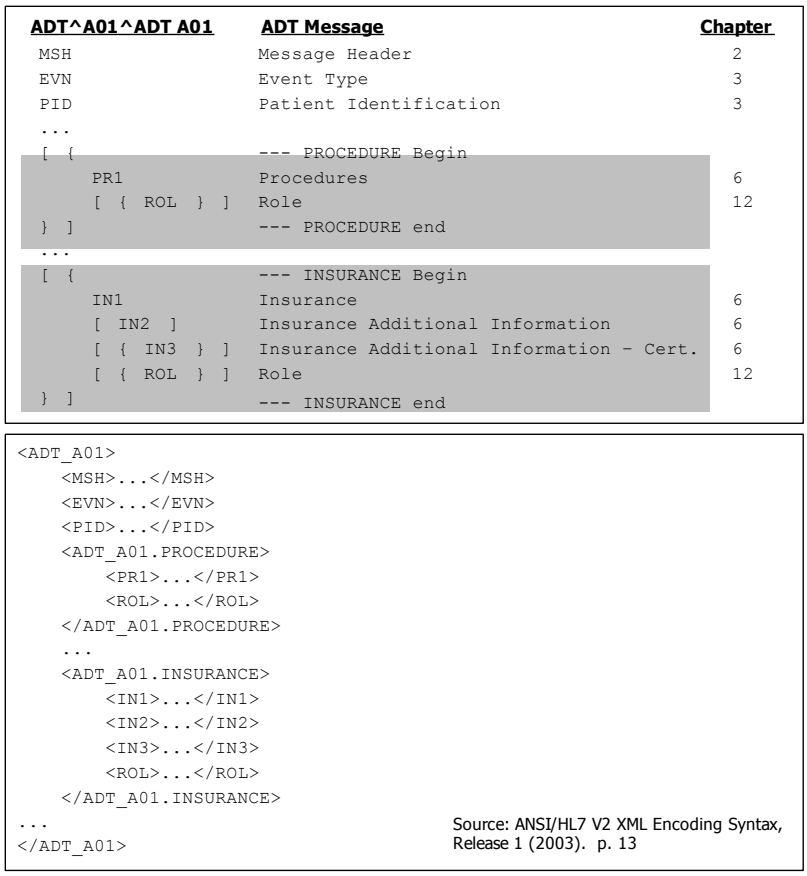
2.4.4.4.1.3 HL7 version 2 XML Encoding Syntax

The HL7 has introduced a second encoding normative based on the Extensible Mark-up Language (XML) for version 2.x messages. The new encoding normative has been developed in the basis that XML provides an explicit representation of HL7 requirement, facilitates the generation of messages, and allows the exchange of messages not only within the healthcare sector but also with other business areas (Heitmann, 2003).

Table 2.2: Abstract Message Syntax Notation and corresponding DTD specification

HL7 Abstract Message Syntax	Equivalent Cardinality in XML Schema (minOccurs .. maxOccurs)	Equivalent XML DTD Occurrence indicator
[]	0..1	?
{ }	1..unbounded	+
{[]}=[{}]	0..unbounded	*
No bracket or brace	1..1	No occurrence indicator (one exactly)

The HL7-XML encoding rules state that HL7 segment identifiers are represented as XML elements, and optional or repeated fields are represented with cardinalities within the XML schemas or document type definition (DTD) (Table 2.2).



ADT^A01^ADT A01	ADT Message	Chapter
MSH	Message Header	2
EVN	Event Type	3
PID	Patient Identification	3
...		
[{	--- PROCEDURE Begin	
PR1	Procedures	6
[{ ROL }]	Role	12
}]	--- PROCEDURE end	
...		
[{	--- INSURANCE Begin	
IN1	Insurance	6
[IN2]	Insurance Additional Information	6
[{ IN3 }]	Insurance Additional Information - Cert.	6
[{ ROL }]	Role	12
}]	--- INSURANCE end	

```
<ADT_A01>
    <MSH>...</MSH>
    <EVN>...</EVN>
    <PID>...</PID>
    <ADT_A01.PROCEDURE>
        <PR1>...</PR1>
        <ROL>...</ROL>
    </ADT_A01.PROCEDURE>
    ...
    <ADT_A01.INSURANCE>
        <IN1>...</IN1>
        <IN2>...</IN2>
        <IN3>...</IN3>
        <ROL>...</ROL>
    </ADT_A01.INSURANCE>
...
</ADT_A01>
```

Source: ANSI/HL7 V2 XML Encoding Syntax, Release 1 (2003). p. 13

Figure 2.4: Abstract Message Syntax for message Type ADT_01 and HL7-XML message encoding

The structure of a HL7-XML encoded message follows the same patterns of its corresponding ASCII Abstract Massage Syntax representation. This implies that an HL7-XML message contains the type, trigger event, and message ID of the AMS. As in the ASCII representation where messages with the same structure refer to a basic AMS, then all HL7-XML messages with the same structure refer to a singular XML schema. The segments are represented as XML elements with

a three-character literal that identifies the element. Group of segments are represented as a sequence of elements grouped by an identifier complex type element. Figure 2.4 shows an Abstract Message Syntax and its corresponding XML message encoding for ADT.

2.4.4.4.1.4 HL7 v.2.x limitation

Regardless of the spread use of the HL7 v2.x family, this has presented the following limitations (Beeler, 1998):

1. The complexity of the standard generates difficulties during the implementation.
2. The communication system should consider the same semantic interpretation of the data elements content message. Additionally, the systems should be agreed in how to use and how to interpret the optional fields.
3. Without the correct analysis, an HL7 message could present inconsistencies either inherent on the standard or in the interpretation of the standard.
4. The HL7 version 2 has a large number of optional segments that require a rigorous testing process. This fact could enhance the complexity of the system and increase the time required for its implementation.
5. The amorphous developed process makes collaboration difficult.
6. The standard cannot be implemented in alternative communication protocols.

Additionally, the use of different version of the HL7 standard has generated incompatibility problems in the communication process between different health care systems (Bicer, Laleci, Dogac, & Kabak, 2005).

Despite the problem presented with the use of the HL7 v2.x standards, the adoption of HL7 provides a baseline platform that simplifies the interoperability between different healthcare systems (Berler, Pavlopoulos, & Koutsouris, 2004). However, the level of interoperability has not yet reached the three levels of interoperability recognized by the US National Committee on Vital and Health Statistic in 2000 (Heitmann, 2003). Additionally, a more depurated methodology is required to develop truly interoperable software applications (Hinchley, 2005).

2.4.4.4.2 HL7 Version 3

As a response to the limitation of the previous version and considering the technologies available, a new version of set of HL7 standards have been developed. This new version reflects the actual trends in software interoperability, diminishes the optional use of segments generated during the development of previous version of the standard, includes international paradigms and facilitates its implementation. As a result of these new requirements, the HL7 Task Force released the HL7 version 3, which considers an Information Model, Interaction Model, Message Design Model, Clinical Document Architecture (CDA), and a framework for HL7 message implementation, making the standard compatible with modern development techniques and reduction of its implementation costs (Beeler, 1998; Hinchley, 2005).

1. HL7 is based on a set of principles that provides a development philosophy to the standard.
2. The new version provides mechanisms and specification that support the design and development of software application throughout the world.

3. HL7 version 3 provides capability support for previous version of the standard (version 2.x family).
4. HL7 framework has been designed to provide a maximum degree of interoperability among software applications implemented within different version of the HL7 standard.

2.4.4.4.2.1 HL7 Components

HL7 version 3 provides a set of component developed to facilitate both the incorporation of new message definitions and the development of new software interfere for data exchange in the health care sector. These components are:

1. The Information Model: it recognizes three interrelated information models.
2. The Reference Information Model (RIM) is the basis for the HL7 message development process. The RIM is an object-oriented data model which contains the basis structure for clinical data domain. It also identifies the life cycle of events that a message or group of messages will carry (Beeler, 1998). Additionally, the RIM provides a coherent information structure, consistent data and concept needed to develop messages to share medical information between different applications in the health care domain (HL7, 2006).
3. Domain Message Information Model (D-MIM) is a subset of the RIM that includes the relevant data structure, based on classes, required to create a message in a specific domain (Hinchley, 2005; HL7, 2006).
4. Reference Message Information Model (R-MIM) is a subset of a D-MIM used to represent the data contented by a message or set of messages. It also contains the specific annotations and definitions that facilitate the

implementation of the messages or set of messages (Hinchley, 2005; HL7, 2006).

5. The standard HL7 framework: it states the principles for the development of new messages in an international collaboration scenario. The Framework is based on the following elements: communication adaptability, collaboration standard development, adoption of codes and vocabulary, and specialization to meet region or nation-specific requirements.
6. Clinical Document Architecture (CDA): the CDA is a header and body document specification. The header identifies and classifies the document and provides information regarding the encounter, patient and provider. The body contains clinical records, which are organized in sections (Dolin, et al., 2006; Morrison, 2000). Both header and body are RIM derived contents. In summary, the CDA is a complete information object to standard mark-up document that provides the structure and semantics to a clinical document with the purpose of interchange (Dolin, et al., 2006). The CDA document is encoded in Extensible Mark-up Language (XML) developed by the World Wide Web Consortium in 1998 (Morrison, 2000), which allows to share multimedia information (text, images, sound and video).
7. Vocabulary Domain: it provides a common and standard vocabulary used in coded fields for HL7 messages. The principal source of codes is the pre-existent standards terminology, when there is not a standard term for a single entry HL7 should provide a correct solution.

2.4.4.4.2.2 Adoption of HL7

The main characteristics of HL7 Messaging Standard were discussed and presented through the previous sections. The intention of this section is to provide an analysis of variables that could affect the adoption of HL7. This analysis will permit to identify benefits of the use, understand the adoption process and recognize limitation and barriers that should be considered during the implementation of HL7 standard.

The use and adoption of HL7 allows the implementation of integrated health care systems. In addition, HL7 provides a native and robust interoperability framework for software development and deployment. Moreover, HL7 reduces the cost of moving existing documents to new standards (Müller, ÜCkert, Bürkle, & Prokosch, 2005) and enhances the work flow between health information systems (Marcheschi, Mazzarisi, Dalmiani, & Benassi, 2004). For these reasons most authors explicitly agree that HL7 is a recommended and required standard for information exchange among health care applications. They also suggested the adoption and use of the different components of HL7 (Message models, RIM, CDA and vocabulary) could generate an important reduction of time and cost in the health care delivery service.

However, adoptions of HL7 have to consider several issues that should be addressed to better implementation plans. Some of them are adoption limitation over ad hoc UML modelling of HL7 (Fernandez & Sorgente, 2005), complexity of the implementation over large information systems, high cost, restrictions of vocabulary and the consideration of other communication standards that provide

better support over a specific domain, e.g. The Digital Imaging and Communications in Medicine (DICOM) for radiology exchange of information (Um, Kwak, Cho, & Kim, 2005).

2.4.4.4.2.3 Technical Barriers for Adoption of HL7

HL7 provides a wide range of guidelines and specification for the implementation of data structures and messages for health software interfaces (Henderson, 2003). Instead, HL7 has several technical limitations that increase the complexity and cost during the implementation process. Some of these limitations are related to information model specifications, message definitions, document structures and vocabulary applied to specific health care domains.

According to the definitions of HL7 standard, messages should contain a basic set of fields, which must hold the critical information required for exchange; additional information should be provided using optional fields (Beeler, 1998; Danko, et al., 2003). This fact does not represent a real inconvenience for local implementations (Bilykh, Jahnke, McCallum, & Price, 2006; Heitmann, Schweiger, & Dudeck, 2003). However, the optional use of fields and segments could increase time, costs and efforts required to implement HL7 messages in inter-institutional scenarios (Müller, et al., 2005).

The Reference Information Model has structural limitations for representing and mapping data and information for some health care domains (Liaw, et al., 2003; Lyman, Boyd, Dalton, & Egybazy, 2003). According to Danko et al. (2003), the RIM class Act is unable to represent complete model structures for nursing information systems. Moreover, they suggested that, to ensure a correct message

definition for nursing activities, the RIM should be adapted to include additional attributes to the Act class and the HL7 vocabulary should be enhanced to include nursing information. Furthermore, the limited representation and limited vocabulary also affect the development of software interfaces and data mapping in other domains such as general practice (Liaw, et al., 2003), and the exchange of referral and discharge letters (Heitmann, et al., 2003).

The CDA provides a framework for developing document representation and communication message based on HL7 standards. However, the CDA framework is in a development process. This implies that CDA does not provide a complete data representation for some specific health domains or local requirements (Heitmann, et al., 2003). Moreover, limitations of HL7 vocabulary and data structure make necessary the development of local solutions, which are not totally compatible for inter-institutional information exchange (Danko, et al., 2003; Heitmann, et al., 2003). In addition, software's vendors do not provide complete support for certain external data integration, and local implementations are restricted to internal needs (Müller, et al., 2005). These issues add levels of complexity to the development process and increase the cost of implementing HL7-CDA message interfaces for inter-institutional health information systems.

Additional limitations are related the cost and time required for implementation and the complexity of the existent HL7 artefacts (Um, et al., 2005). The implementation of HL7 messages based on CDA-XML requires an important amount of time and cost of development. Moreover, the implementation of CDA templates increases the cost and efforts (Heitmann, et al., 2003). In addition, the

deployment of large health information systems, under HL7 message standard and related components, makes the development and implementation process highly difficult and requires additional resources (Katirai & Sax, 2005; Langer, 2002; Sakamoto & Nakaya, 2005.).

In conclusion, HL7 offers a helpful framework for developing and implementing health information message interfaces. However, there still exist some issues to address in order to improve the standard. First, HL7 message implementation for large or inter-institutional health information systems requires a considerable amount of time and costs. Second, the RIM has provided structural basics for the definition of messages; however, it is limited for representing and mapping data for specific domain such as nursing and general practice in-formation systems. Finally, the CDA has become a basic requirement for clinical document representation and message implementation but, has presented limitations in the representation of specific local health information domains and inter-institutional information.

2.4.5 Challenges of Securing Electronic Health Records

Securing electronic health records, in a scenario where information is potentially accessed by multiple actors, could become a complex and costly activity. To provide a framework for secure maintenance and release of health care information, the European Committee for Standardization has released a set of information security standards for health information systems (CEN-ENV, 2000a, 2000b, 2000c). CEN standards recognize four global security needs that any health information system should accomplish. The four global security need

described by the CEB standards are: availability, confidentiality, integrity and accountability (CEN-ENV, 2000a). The definition of a secure model for data exchange would reuire the application of these principles. With that purpose the relation between the global security needs and their application are described and discussed in this section.

Availability of the information refers to the level of accessibility of the information upon request from a user. In healthcare, availability of the information is essential in the provision of integral health services. However, availability of information should be provided under a secure scheme in which confidentiality of information is also guaranteed. To protect the confidentiality of the information, access to patient's data should be carried out under the principles of relevance and need-to-know (Garson & Adams, 2008). The principle of relevance prevents the information overload and protects the patient's privacy by restricting the release of information to the relevant data required to support the health care process (Berner, 2008; van der Linden, et al., 2009). In the same way, the principle of "need-to-know" guarantees that only personnel who required the information and have the access privileges will be allowed to extract the data. Defining the correct balance between availability and security of information is a critical goal in a complex environment such as health care.

A security breach poses a threat for protecting the integrity of electronic health records as well as for providing reliable information for accountability purposes. Integrity of the information is not only guaranteed by incorporating additional security mechanisms within the system or for securing a communication channel,

when information is exchanged between systems, but also by ensuring that only authorized user can have access, add or alter stored data (Blobel, et al., 2006; Blobel & Roger-France, 2001). In a shared care environment controlling who is accessing the information turns into complex and time demanding task. Accountability of information also becomes less accurate when non-authorized users are able to access and manipulate data regardless of the fact that they do not have the privileges to execute such activities (Shin, Lee, Shin, & Choi, 2008). The solution proposed would need to address the four global security needs. As it will be discussed in the following sections, the availability of the information becomes essential in a shared care environment. A software specification will be required to observe the principles of relevance and "need to know" as a method to guarantee the correct access to the information. The challenges discussed on this section are analysed in more detail in the following sections. The section 2.4.6 presents a general analysis of the requirements for allowing data exchange in a shared care setting, the analysis is made considering a bi-dimensional view of the information shared in a health care environment.

2.4.6 Securing the Exchange of EHRs

Health information standards provide the basic framework to developing robust interconnected health applications. However, the secure exchange and disclosure of electronic health records over insecure channels such as internet also requires the implementation of comprehensive security technologies that allows the exchange of data (Choe & Yoo, 2008). Security technologies should provide mechanisms for access control and define access privileges for protection of data

privacy and information management (Blobel, et al., 2006; Ohno-Machadoa, et al., 2004). Patient's sensitive information always has to be protected during the electronic exchange of medical data; especially the information considered sensitive. The unauthorized access and release of sensitive information are considered a breach of confidentiality and could lead to issues of public concern such as discrimination, embarrassment or economic harm (Ohno-Machadoa, et al., 2004). At this point, the following issues need to be taken under consideration:

- Origin of the information
- Reason for its release and destination
- Secure transmission of data
- Protection of patient's privacy

Table 2.3: Overview of communication and security requirements

	Local	**Inter-Institutional**
Primary	• Standards domain software interfaces • Standard domain message definitions • Import/Export functionalities for compatible applications • Local access and security policies • Role-based Access control policies • Local Communication security • Application security (availability, identification and authentication, confidentiality, data integrity, accountability and traceability)	• Standards multi-domain software interfaces • Standard multi-domain message definitions • Standardized access and security policies • Common definitions for role-based access control policies • Access and security policy agreements • Inter domain communication security (Authorization and access control, confidentiality, data integrity, accountability and traceability)
Secondary	• Ambiguation and anonymization of electronic health records • Security policies for secondary release and use of EHRs • Security policies for third party release and use of EHRs • Local application and communication security	• Data integration, Ambiguation and anonymization of disseminated EHRs • Common and agreement policies for access and release for secondary use of EHRs • Common / agreement policies for third party release / use of EHRs • Inter domain application and communication security

The origin of the information refers to who and where the data has been collected. Health information can be collected by different organizations and can serve a variety of purposes, and its storage can be local or external. Information locally stored can be promptly available and can be accessed by a user at any time and location within the organization. On the contrary, external health data is usually retrieved from information systems that do not provide direct access rights to users. In this case, access rights are provided based on common agreements between the organizations involved (Lopez & Blobel, 2009; van der Linden, et al., 2009).

The reason for the disclosure of information is an important element in defining an efficient security strategy. Detailed information is normally required to support primary services such as the treatment of a subject of care. On the contrary, information required for secondary uses should not be linkable to the patient (Agrawal & Johnson, 2007). The destination of the information also affects the definition of a security strategy. Local security needs substantially vary from the requirement of a shared care scenario (van der Linden, et al., 2009). Locally, standard security measures and standardized messages allow the secure access and disclosure of information. However, the secure exchange and release of information among different health providers not only depend on secure and standardized electronic mechanisms but also on standardized security and access policies (Lopez & Blobel, 2009). In fact, different health institutions might have different security policies, especially in terms of access privileges and release of electronic health records for primary and secondary uses. Incongruent security polices could generate security breaches which compromise the confidentiality

and privacy of patients' medical data (Choe & Yoo, 2008). The Table 2.3 presents an overview of the requirements that need to be fulfilled depending on the use of the information and its destination. In the following section each one of the quadrant of the table will be analysed in more detail.

2.4.6.1 Local Data Exchange and Security for Primary Use of Information

Local EHR implementations have become a key element in supporting health care activities, reducing the cost of health care, improving the quality of the service, enhancing health care delivery and providing support for primary and secondary use of information. In order to facilitate the access to information storage in local EHRs, health information systems should be interoperable in a secure fashion. In general, local EHRs implementations should consider the existence of heterogeneous sources of information, security requirements for protection of patients' medical data and the implementation of security policies for access and release of the data.

The existence of heterogeneous health information systems has increased issues related to interoperability and compatibility of medical records, and limited the collection of integrated patient and medical information from local information architectures (Coonan, 2004). The incorporation of medical informatics standards allows the development of adequate infrastructure for health care (Hammond, 1995; Hammond & Cimino, 2001) and overcomes the limitation generated by the adoption of heterogeneous information systems. Standard domain software

interfaces, standard domain message definitions and importing/exporting functionalities for compatible applications are the keystones for allowing local communication and interoperability of health information systems and providing access to electronic health records.

Security requirements for accessing and protecting patients' medical information are also crucial components for integrated local health information architectures. Local communication and application security should ensure availability of information, confidentiality, user identification and authentication, data integrity, accountability and traceability of accessed information. Availability of the information is another important element in obtaining functional electronic health record systems. Users with the right to access information should be allowed to do so in order to perform their duties (Blobel, 2004; Garson & Adams, 2008). As information happens to be more available for all users within the organization the concern over the protection of patients' privacy becomes an important factor that drives the implementation of security measures (Anderson, 2007; Blobel, 2006a).

Integrity, reliability and accountability are also crucial requirements that a health information system should meet in order to ensure the maintenance of a secure electronic health record platform.

Under these circumstances, management of security services for authentication and assigning access privileges is a critical task for securing EHRs (Blobel, 2004). Consequently, accurate authentication of the user as well as a correct assignation of access privileges become crucial in order to guarantee that information is accessed, added and modified only by individuals with the privileges to perform

such activities (Blobel, 2004). The role-based access control (RBAC) model has been presented as an appropriate solution for granting access privileges to patient's information. RBAC provides a solution for the indirect assignment of access privileges based on the role of the individual within the organization (Blobel, 2004) but also allows grained customization of access privileges for users under specific circumstances (Peleg, Beimel, Dori, & Denekamp, 2008). RBAC model their benefits and limitations will be discussed in more detail later on in this Chapter.

Domain and sub-domain access and security policies should cover legislation and regulations regarding secrecy and confidentiality of personal information by providing an internal normative concerning the release of data. In order to prevent an unauthorized release of information, health information systems should provide a security infrastructure for protecting the principles embedded within organizational security policies (Agrawal & Johnson, 2007; Conrick & Newell, 2006; Lusignan, et al., 2007).

2.4.6.2 Shared care data exchange and Security for Primary Use of Information

Electronic exchange of EHRs requires both common standardized messages that facilitate the information exchange among heterogeneous electronic information systems and effective data protection models, which need to be established to ensure confidentiality, reliability and validity of the exchanged information (Blobel, et al., 2006; Choe & Yoo, 2008). Even when incorporating secure

measures to protect the exchange of EHRs may guarantee the secrecy of the patient's information during the transference of data, it will not ensure the preservation of confidentiality at the communication end points. In effect, it is necessary to incorporate standard message definition, security services, security mechanisms and common access and security policies in order to protect the confidentiality of the patient's information in a shared care environment (Blobel, et al., 2006).

Health information systems developed under the premises previously mentioned, require the ability of exchanging relevant data to carry on patients' treatments within the health care network. According to the International Organization for Standardization, a standardized electronic health record system should include the ability of exchanging a complete EHR or a part of it and provide support for serialization of databases under standard messages and data architectures. Moreover, the system should facilitate the semantic interpretation of merging data from an extracted EHR; include support for audit trail of exchange processes; provide rules covering the exchange of an extract of the record; and allow the semantic interoperability of clinical concepts (ISO/TC-215, 2004). Exchanging health information could be achieved by importing/exporting records in the case of compatible software application or by using standardized messages in a scenario with a heterogeneous use of both information architecture approaches and software platforms (Danko, et al., 2003; Müller, et al., 2005). Health Level Seven (HL7), the ASTM International, formerly the American Society for Testing and Material, and the European Committee of Normalization (CEN) have provided standard frameworks and message definitions that facilitate the

development of software interfaces for the exchange of electronic medical information using public networks such as Internet (Blobel, 2006a; McDonald, Overhage, Dexter, Takesue, & Suico, 1998).

In a shared care scenario, the responsibility of maintaining confidentiality over information is shared among the different organizations participating in the health network. This responsibility not only should be considered but also reflected in the selected health information architecture. Meeting confidentiality and security needs is vital for electronic health records systems in order to provide a secure, safe and reliable environment for co-operation and communication among healthcare providers. Security may not only consider the services that will be put in place to avoid the unauthorized access to sensitive information but also mechanisms that will be used to protect the patients' data and prevent an unauthorized release of information at any point in the communication channel (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001).

Communication security and application security are the two main elements that require special attention when sensitive information is transmitted. Communication security describes all components required for a safe exchange of data between software applications whilst application security refers to security measures used by information systems in order to protect the information contented on database and documents. A set of standardized mechanisms and services can be used to protect the information during the exchange; however, the main issue is how to ensure the safe release of the information when it reaches its destination.

The exchange of information also requires the consideration of common good practice policies of use and disclosure of medical information (Conrick, 2006; Safran, et al., 2007). Although protection of patient confidentiality is a legal and ethical issue regarded by specific legislation, the technical dimension presents a challenge that changes of technology not always address rigorously (Conrick & Newell, 2006). The personal character and sensitivity of the information stored on EHR makes necessary the consideration of security services that allow the access to authorized users whilst protecting the confidentiality of the patient's information (Blobel, et al., 2006; Blobel & Roger-France, 2001; Gritzalis & Lambrinoudakis, 2004). However, it is not a simple task to design and implement security measures for protecting patients' confidentiality and, at the same time, facilitate the communication of information between health professionals (Agrawal & Johnson, 2007; Gritzalis & Lambrinoudakis, 2004). Problems at this level are not only associated with correctly assigning access rights for transmitted information; but also are linked to the development of common policies or conflict resolution policies for allowing the access to authorized users (Blobel, et al., 2006; Blobel & Roger-France, 2001; Gritzalis & Lambrinoudakis, 2004).

A solution proposed by Agrawal and Johnson states the use of a "sticky policy" which is endorsed to the exchange of information. The endorsed policy contains the original access control policy that is enforced over the transferred data (Agrawal & Johnson, 2007). However, this not only requires the use of standardised policies languages for the correct interpretation of the transferred policies but also poses the inconvenience that local policies could eventually be in disagreement with an endorsed policy. In addition, access control and privacy

policies are managed by each institution separately based not only in legal bodies and regulations but also in the ethical principles that govern the culture of an organization (Choe & Yoo, 2008). Blobel proposed a multi-domain policy model in which common domain policy agreements are defined. Common domain policy agreements are policy definitions established between health organizations to solve inconsistencies between policies during the exchange of information (Blobel, 2004). In this case, the interpretation of policy will depend on syntax, semantic, vocabulary and operation of policies that may present issues when information is exchanged between domains that do not share similar technological infrastructure and policies definitions (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001). Normalization of policies as well as a common definition of vocabulary and interpretation of policies are essentials for the implementation of this approach. However, a formal framework for policy definitions has not been defined within the health care sector (Gritzalis & Lambrinoudakis, 2004). Neither normalization and/or standardization of policy definitions have been formally proposed.

2.4.6.3 Data exchange and Security for Secondary Use of Information

Even though the scope of this research is to provide a data exchange specification for secure transition and release of primary health information in a shared care environment, the discussion of secondary use of information and its security requirements would provide a better understanding of the Table 2.3. Secondary information obtained from electronic health information systems is not only useful for the improvement of health delivery but also can be used as historical source of

medical data for research and educational purposes (Haux, 2006b). Nevertheless, as secondary data is obtained from patients' electronic information, a release of it without the proper privacy and confidentiality protection could eventually result in harming individuals. Thus, any association of data that can eventually lead to the identification of patients should be avoided in order to protect the privacy and confidentiality of individuals.

Ambiguation and anonymization of data are the fundamentals for protecting privacy and confidentiality of patients whilst the flow of information for secondary uses is maintained (Ohno-Machadoa, et al., 2004). Techniques and software applications that provide answers to securing anonymity of the patient data are already under development. However, there is no consensus on what constitutes an anonymized data set, and how the degree of anonymity can be quantified in order to provide mechanisms for formalizing the problem, or even more which information should be considered to be sensitive. This issue has an important impact in distributed systems and data repositories. Since there is not a common concept for anonymization and it is not clear which data is considered sensitive, the information collected from different data repositories could eventually contain data sets with information that can be linked to individuals (Ohno-Machadoa, et al., 2004). In the case of multi-domain scenarios, in which not all involved organizations share the same technology, the secure access and release of information could not be entirely guaranteed (Agrawal & Johnson, 2007). For example, in wide range studies, in which information is collected from a variety of data repositories, the existence of different approaches for both establishment of sensitive data sets and technologies for ambiguation and

anonymization could turn into security risks that would threaten the privacy and confidentiality of patients' information.

The use of EHRs for secondary purposes also has a normative component which requires consideration. Legislation and regulations define who accesses information and how the information could be released. Furthermore, it serves as a framework from which access and security policies are established. Policies for secondary release and use of information as well as policies for third party release and use of EHRs are not only defined according to the relevant legislation and normative but also are based on the culture, experiences and ethical values of the organizations. Additionally, the technology used to maintain policies and define access to the stored data differs from one organization to another. Considering these facts, it is clear that any sharing of secondary information between organizations would eventually face incompatible or contrasting polices (Agrawal & Johnson, 2007). The Implementation of policy agreements could provide solutions to issues regarding the existence of differences between policies during the collection and exchange of the stored data. Nevertheless, as it has been discussed previously, the interoperability of release policies will also depend on how well information systems are able to interpret them (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001). Normalization of policies as well as common definition of vocabularies for interpretation is a key factor for the secure release of secondary health information not only for local environments but also in inter-institutional scenarios.

2.4.7 Analysis of Authentication and Access Control Methods

In a shared care context, the concepts of privacy, confidentiality, and security become fundamentals for secure exchange of electronic health records. In order to provide a secure, safe and reliable environment for cooperation and communication, several security requirements need to be taken into consideration. Security may not only consider the services that will be implemented to avoid the unauthorized access to sensitive information but also should incorporate mechanisms that prevent unauthorized access and release of patient's data.

2.4.7.1 Traditional Authentication Methods

Existing authentication and access control models require safekeeping PINs, passwords or smartcards in order to provide access to restricted facilities and information. However, the nature of the activities executed by physicians and medical personnel requires mobility and multiple accesses to different terminals within the organization or even remotely in the case of web based health information systems or integrated multi-domain systems (Garson & Adams, 2008; Shin, et al., 2008). Considering that access to different systems may require multiple authentication methods, it is usual to find that PINs and passwords are maintained stored on the computer terminals used by physicians, stick papers on the office, laboratories, medical consult or at home, or become a simple combination of well known numbers or digits such as phone extension, date of birth or pseudonyms, which are easy to remember but also relatively less efficient in avoiding security breaches (Garson & Adams, 2008; Shin, et al., 2008). The

use of smartcards also may present certain disadvantages such as deterioration and accidental lost. Additionally, if physicians forget their PIN/passwords or misplace their smartcards a reissuance process must take place (Shin, et al., 2008). Consequently, existing models become inappropriate and less reliable for a medical environment.

The other issue associated to the use of traditional models is medical disputes generated by delegation of authentication codes (Chen, et al., 2008; Heckle & Lutters, 2007). Delegation of private authentication codes is generated when a member of a hospital's medical staff delegates his PIN/password or other authentication feature to another physician or nurse to access, modify or add information on behalf of the owner of the private authentication codes (Heckle & Lutters, 2007; Shin, et al., 2008). The delegation of access rights may grant access to sensitive information to non-authorized users by breaking established policies of information privacy and confidentiality (Heckle & Lutters, 2007; Shin, et al., 2008). This also may have legal implications when restricted information is leaked to third parties without the proper authorization of the patient or when the addition of erroneous information compromises the safety of patients.

2.4.7.2 Authentication Based on Biometric Technology

In healthcare, biometric technology has been gradually introduced as a method to secure and restrict access to medical facilities, protect and manage confidential information, identify patients and reduce fraud in healthcare programs (Marohn, 2006). As biometric technology uses unique physical features of a person, the

level of security is increased by preventing the fraudulent access to restrict information. In this context, biometric technology provides a mechanism for identification or identity verification depending on what organizations need in order to protect their resources and information. Using biometric to provide security services can be a noteworthy alternative considering the flow of sensitive information presents in large software applications and the resources required to manage complex information systems that can be accessed by hundreds or thousands of local and remote users. Biometric technology presents several advantages in comparison to traditional methods such as providing a friendly and easy to use access control method, the restrictions in the delegation of access rights, increase of security and discourage fraudulent access to restricted information.

Even though biometric technologies offer a more compiling and secure method for restricting the access to health facilities and health information than traditional technologies, it has not been addressed as a suitable alternative for protecting patient's privacy and confidentiality (Shin, et al., 2008). Technology based on biometric provides a suitable and more secure method for identification and access control than traditional technologies as well as the ability of encrypting sensitive information for local applications or in a shared care environment (Gates, 2007; Shin, et al., 2008). Additionally, international regulations and legislations that promote protection of patient confidentiality have pushed forward the concern regarding unauthorized access and release of information (Agrawal & Johnson, 2007; Conrick & Newell, 2006; Lusignan, et al., 2007). In this scenario, biometric technology provides a reliable solution for ensuring that only authorized

personnel have access to patient's information. Biometric technology also could be used to protect patient's privacy in share care scenarios by making information network systems more secure (Atkins, 2000; Marohn, 2006).

Approaches based on biometric technology have demonstrated to be reliable mechanisms by restricting the delegation of access rights as well as discouraging fraudulent access or impersonation of users (Shin, et al., 2008). Biometrics features are almost impossible to reproduce and user can be easily identified based on their physical or behavioural characteristics (Delac & Grgic, 2004). In addition, the use of biometrics dramatically reduces the chances for unauthorized delegation of access rights as well as facilitates the maintenance of appropriate access privileges, positioning this technology as a suitable solution for guaranteeing security and accessibility to electronic health records (Gates, 2007; Shin, et al., 2008). In the same way, biometric allows the elimination of end-user generation of passwords as primary source of information for system security, which has become a main security issue for current information systems (Gates, 2007; Shin, et al., 2008).

Implementation of biometric authentication technology also facilitates the remote access to electronic health records by using a biometric feature as a method of authentication. This has become beneficial in the management of treatment for aged patients in remote areas, as well as allowing patients to update their online personal health records (Marohn, 2006). Additionally, it also has been used to reduce fraud in health insurance, protect facilities, reduce costs of maintenance,

promote and protect patient privacy, help in the management of confidential data and identify patients (Marohn, 2006).

In general, using biometric technology as an authentication and access control method enhances the protection of patient privacy by adding an accurate authentication technology, eliminates costs associated to password maintenance, reduces unauthorized access to sensitive information by restricting delegation of access right and impersonation of individuals, reduce fraud associated to insurance claims and become a long term solution for access system management (Gates, 2007).

2.4.7.2.1 Uses of Biometric in Healthcare

2.4.7.2.1.1 Remote Access for Patients

A specific application of biometric technology is identification of patients for remote access to personal medical information. In this case, patients can have access to their personal information by using a biometric feature such as fingerprint. In this context, a biometric scanner would be able to capture an image of the biometric feature and send it to a centralized system for verification purposes. The image is matched with the stored biometric profile of the patient. When the identity of the patient is verified the system sends back the information originally requested by the patient (Flores Zuniga, Win, & Susilo, 2009).

Authentication technology other than biometrics does not guarantee that the person remotely accessing personal records is who claims to be. In the previous section, it was discussed several security issues regarding the use of personal key

(passwords and PIN) normally generated by the end-user (Gates, 2007; Shin, et al., 2008). Although, patients, who are accessing medical records, are not allowed to modify medical information, the unauthorized access to the remote repository could have personal, legal or social repercussions. Biometric technology helps to prevent the unauthorized access to remote repositories by avoiding impersonation of individuals (IBG, 2008; Shin, et al., 2008). Biometric technology could also be used to encrypt the medical data. In this perspective, patients would be able to access personal data remotely; the system would be able to encrypt the information using the biometric profile of the patient and then transmit the encrypted data to the patient's computer.

Experiences using this model have been implemented in the United Kingdom and South Africa. In United Kingdom a web based application with fingerprint technology has been developed to allow the remote identification and access to aged patients' electronic health records. Patients in this program are able to access their medical records, prescription and medical procedures as well as indications made by physicians. A similar system has been implemented and used in South Africa to facilitate the patient identification and provides access to historical electronic health records (Flores Zuniga, et al., 2009; Marohn, 2006).

2.4.7.2.1.2 Verifying Patient Identity

Biometric identification and verification of patient's identity have been used mainly to prevent fraud in insurance claims and for the application of healthcare programs. Several experiences have reported successful results in countries such as USA, Australia, the United Kingdom and South Africa. Identification of both

healthcare provider and patients has been the primary purpose of the use of such technologies. For example, in Texas (USA) a biometrics-smartcard program has been implemented for recipient authentication at the attention point to reduce fraud associated to the provision of healthcare services, in Australia a retina verification system has been employed to support the treatment of patients addicted to heroin (Marohn, 2006).

Fingerprint biometrics also can be used for purposes of patient registration and identification. Under a biometric identification system, a non-registered patient entering healthcare service may place a biometric feature (iris, fingerprint, etc.) on a biometric scanner to generate a biometric profile. The biometric profile is then used for identity verification purposes during patient's further visits. The technology could also restrict the access to electronic health records, unless the identity of the patient has been verified. A system with these characteristics has been implemented and used at Lourdes Hospital in Kentucky, USA (Atkins, 2000; Flores Zuniga, et al., 2009).

Biometric profiles also have been used to identify patients in emergency situations. When biometric profiles are linked to the electronic health records the information can be accessed even when no information or identification of the patient can be provided. For example, if unconscious patients are brought to a health service they could be identified based on their biometric profiles and then linked to their personal records. The data would be released providing to the medical staff with the information required to offer an efficient medical care service. Furthermore, the released information may prove to be beneficial for

other purposes such as contact the family of the patient. The Ballard Hospital, Washington, has used this method to identify unconscious assault victims that are received in the emergency services. Moreover, after the devastating effects of the hurricane Katrina, emergency services used biometrics' profiles to identify unconscious patients and victims (Marohn, 2006).

The attention at the point of care also may be benefited using biometric identification methods. The remote access to electronics health records by PDA, smart phones or laptop computers also is possible by using biometric for security purposes. A biometrical sensor, which is used to capture a biometrical sample of the patient, can be added to a portable devise. The image captured by the sensor is sent to a centralized system that matches the image with the stored biometric profile. When the identity is verified the patient information is released and sent to the portable device. The portable device displays the information that is used to provide a better health service. This technology has been used in USA to provide better medical care to patients and victims during emergency situations such as car accidents, fire incidents, and natural disasters (Flores Zuniga, et al., 2009; Marohn, 2006).

2.4.7.2.2 Limitation of Biometric Technology

Even though, biometric technology offers several advantages in comparison to traditional authentication methods, it also presents usability setbacks. In fact, there are technical and usability issues to be considered when selecting and using biometric technology such as accuracy of the biometric lecture, technological

obsolescence of the scanners, the existence of the biometric feature, enrollability and suitability for the medical environment.

The accuracy of the biometric technology depends on the ability of the system in obtaining a good initial image of the biometric feature as well as the ability of matching individual with their original templates. The false acceptance rate (FAR) and false rejection rate (FRR) can be affected by factors such as incorrect placement of the biometric feature, dirt, humidity and changes in the biometric feature (Garson & Adams, 2008; Pierce, 2003). Degradation of the biometric feature also affects the accuracy of the matching system (Pons & Polak, 2008) and raises the necessity of maintenance and re-enrolment of existing users. Enrollability of user is also the other issue that can affect the accuracy of the matching system. For example, optical fingerprint scanners fail to read a significant portion of the population such as older people with dry skin and children (Pons & Polak, 2008). It is also the possibility of damage or inexistence of the biometric feature which is generated by injuries or mutilation (Garson & Adams, 2008).

Users require placing their biometric feature in a specific position, heat, cold and perspiration can affect the accuracy of the lecture, which makes the technology unsuitable for certain cases. For example, fingerprint technology can be easily implemented for accessing electronic health records in several health care settings. However, the fact that many health care staff would be usually wearing hygienic gloves becomes a usability problem in this case (Garson & Adams, 2008). Iris recognition is more accurate technology and also provides a solution to several

usability issues. However, the high cost, reticence of users and the fact that this technology has not been tested for large implementation makes it less suitable for several health care settings (Reynolds, 2004).

Additionally, biometric implementations assume that electronic health records are applications based on private, and most of the time, local networks that do not need external communication (Shin, et al., 2008). This assumption is not entirely accurate for a shared care paradigm (Blobel, 2004, 2007; Blobel, et al., 2006). Nowadays, it is common to observe that patient's medical information is shared among different health providers or used not only for primary purposes but also for secondary reasons (Safran, et al., 2007). However, sharing sensitive information brings the concern that the overall security will be as strong as the weakest system within the network. Therefore, to become a valid alternative, biometric technology requires the consideration of multi-domain environments, where information is transferred among different domains within the organization or among health care providers.

In general, biometric technology does offer several advantages over traditional method, especially in matters related to security and authentication. However, several issues rise from the usability perspective that could affect the accuracy of the technology and that needs to be considered to reduce the rates for false acceptance and false rejection.

2.4.7.2.3 Biometric Technology and Secure Exchange of EHRs

The solution proposed, which is discussed in chapters 4 and 5, would also allow the use of biometric technology for the authentication of the medical staff. In fact, the model is based in a attribute security model which also has been applied as fuzzy-attribute based encryption scheme for biometric technology. This approach and it related model will be discussed in Chapter 5.

2.4.7.3 Traditional Access Control Models

In the following sections traditional access control models, such as DAC, MAC, RBAC, will be presented. In order to do so, a paradigm will be used, where a doctor needs to acquire information regarding a patient's medical history from external institutions in order to handle the patient's case. This case is described in more detail in section 4.1.

2.4.7.3.1 Mandatory Access Control

Mandatory access control polices (MAC) govern access based on classification of subjects and objects within a system. The decisi**o**ns regarding access control are made by a centralized authority that determines, on one hand, the level of security required for each object and, on the other hand, the trustworthiness level of subjects for accessing the protected information (R. S. Sandhu & Samarati, 1994). Access control is based on comparing security levels, which indicate how sensitive data is and it is performed by assessing security clearances, which indicate the entities that are allowed to access such data. To access the information a subject should have at least a level of security clearance equal to the

security level of the object being accessed (Stallings & Brown, 2008). MAC policies established that users cannot delegate access rights in this way enforcing protection of the data “level”, this guarantees the confidentiality of the accessed data (Stallings & Brown, 2008). MAC policies also allow the establishment of fine-grained access rights over data and, at the same time, reinforce established access restrictions. However, MAC policies are rather rigid, which make them unsuitable for a shared care environment, especially considering that in MAC more than one security level cannot be assigned to the same data object (Hafner et. all, 2008).

For example, and considering the case study presented in section 5.3.1.2.2, a situation where information of patient 'A' is maintained under MAC policies, doctor 'DC' will be required to provide the necessary clearances to retrieve the data from clinic 'CL' and hospital HB information systems. In this case, the data fields confining patient 'A' information would be maintained labelled with different levels of security accordant with the sensitivity of the information. Doctor 'DC' would be able to retrieve the data that reflect the access right provided by the clearances that he possesses. In fact, to maintain the principles of need-to-know and relevance 'DC' would only have access to the relevant information needed to perform the task. However, a physician with the same security clearances to 'DC' would also be allowed to access the retrieved data, which would not reflect the consent provided by patient 'A' to doctor 'DC'. MAC policies are centred on the level of sensitive of the information rather than rights

and permissions that users or user groups have to access the data, which does not allow discriminating among users with the same clearances.

Furthermore, in a shared care context where data can be exchanged between multiple organizations, delegated and accessed by multiple individuals, users can play different roles and have access to information under different contexts (Alhaqbani & Fidge, 2007). However, delegation of information and establishing hierarchies of access permissions are not allowed by MAC policies. In general, although MAC policies are less complex to define and allow the establishment of fine-grained access permissions based on the sensitivity of the information, they are extremely rigid for a health care environment, especially in managing users and user groups and delegation of access permissions (Hafner, Memon, & Alam, 2008)

2.4.7.3.2 Discretionary Access Control

Discretionary access control (DAC) is based on the identity of the requestor (user or system process) and on access rules, which establishes what the requestor is allowed to do. Access will be granted to the user accordantly to the permissions that the user has over the object at the moment of accessing it. DAC policies allow users to provide access permissions to another entity (user or system process). However, they do not impose restrictions in how information will be managed when it is received by a user. In fact, a user could pass the data to another user not authorized to access it.

A key element of DAC is the ownership of the information, especially because owners are allowed to grant access to the stored data. However, in health care

ownership of the information is not always clear. In fact, EHRs belong to a patient but are created and modified by health care professionals and the information is not only shared but also could be maintained by different health organizations, which could claim ownership of the data (Alhaqbani & Fidge, 2007; Hafner, et al., 2008). Considering the situation of patient 'A', the data retrieved by doctor 'DC' from clinic 'CL' and Hospitals 'HA' and 'HB' correspond to her personal health information; however, ownership of the data is not clear. In the case of patient 'A', contents of her electronic health records have been created and accessed by physicians of the three organizations as well as information has been collected from other external sources (radiology results and postmenopausal symptoms in the case of clinic 'CL'). Additionally, patient 'A' electronic health records is distributed in the information systems of all three organizations that, in principle, would have different access principles and security policies. The example shows that information could be created by various collaborative partners that could not claim complete ownership of the data.

Although, access policies are flexible, the model lacks the ability of supporting dynamic change of access rights. Additionally, fined grained access privileges are difficult to be managed, especially when users are allowed to grant access rights to other users. DAC is centred in users rather than user groups; however, if the model is extended by including categories or group definitions, group management is possible.

In general, DAC policies are less complex to implement if compared to RBAC, they are also flexible but still restricted for a shared care environment and increase

the complexity of defining fine-grained access to stored data. Implementing DAC in shared care settings could result in additional security problems (R. S. Sandhu & Samarati, 1994; Stallings & Brown, 2008).

2.4.7.3.3 Role-based Access Control and Exchange of EHRs

Role-based access control (RBAC) has been used as a mechanism to guarantee authorized access to electronic health resources, especially during the exchange of EHRs. Role-based access control (RBAC) is used to protect information resources from unauthorized access based on the roles that user could have or perform within an organization. RBAC was first introduced by David Ferraiolo and Richard Kuhn in 1992 as a mean to provide manageable access privileges to identifiable groups of users (Ferraiolo & Kuhn, 1992). The Ferraiolo-Kuhn model was later integrated with the framework proposed by Sandhu et al. (Sandhu, Coynek, Feinsteink, & Youmank, 1996) and published as the NIST RBAC model in 2000 (Sandhu, Ferraiolot, & Kuhnt, 2000). The integrated framework proposed by Ferraiolo, Sandhu and Richard was adopted as ANSI/INCITS standard in 2004.

The central idea of the RBAC model is that users can perform multiple roles and roles can be associated to multiple access permissions. In RBAC permissions are represented by the relation existing between resources and operations over those resources (Lee, Kim, Kim, & Yeh, 2004). In practice, RBAC models are based on access policies defined in terms of permissions that are associated with roles assigned to users. Permissions will determinate the operations that a role is able to

perform on information resources and, therefore, all users that have assigned that specific role (Kim, Ray, France, & Li, 2004).

RBAC has been proposed and used to provide access privileges to information contained within electronic health records. Hoverer, even when RBAC models provide simple mechanisms for granting or restricting access to information by associating each user to roles, it faces the issue that role definitions (descriptions as well as access privileges) could differ significantly from one organization to another (Peleg, et al., 2008). The definition of access privileges not only depends on the conceptual definition of roles but also of intrinsic practices within the organization. Consequently, a role-based access control model may not entirely provide a suitable solution for inter-institutional scenarios. In fact, RBAC models are established according to particular requirements defined for each institution in the network. Therefore, it is expected that conflicts and ambiguity would take place when agreement policies are stated (Blobel, 2000; Blobel, et al., 2006; Blobel & Roger-France, 2001). Common and agreement policies regarding role-based access privileges could prove to be an efficient way to solve this issue in the short term. However, standardized role definition and access privileges at the conceptual and practical levels will be required in order to solve ambiguity issues in the definition of roles in the long term (Blobel, 2004).

2.4.7.3.4 Role-based Access Control Model

Constrains associated to role-base access control model (Figure 2.5) can be classified as core RBAC, hierarchical RBAC (RH), static separation of duty (SSD) RBAC and dynamic separation of duty (DSD) RBAC. Core or flat RBAC

requires that user be assigned to roles to obtain access to information resources. At this level user can be assigned with access to multiple roles without specifying constrains regarding the relation between the user and the roles assigned to him. Hierarchical RBAC provide features for hierarchical representation of the structure of roles in an organization. Static and dynamic separation of duty RBAC constrains relations aim to avoid conflicts of interest that may rise when more than one role is assigned to a user (Kim, et al., 2004; Sandhu, et al., 2000).

In general, roles are defined accordantly to the structure of the organization or based on the functional role or roles that the user may perform. Role based on organizational structures are static rigid and represent a structural and hierarchical relationship between entities within the organization. In contrast, functional roles are highly dynamic and reflect functional aspects of relationships between entities (Blobel, et al., 2006).

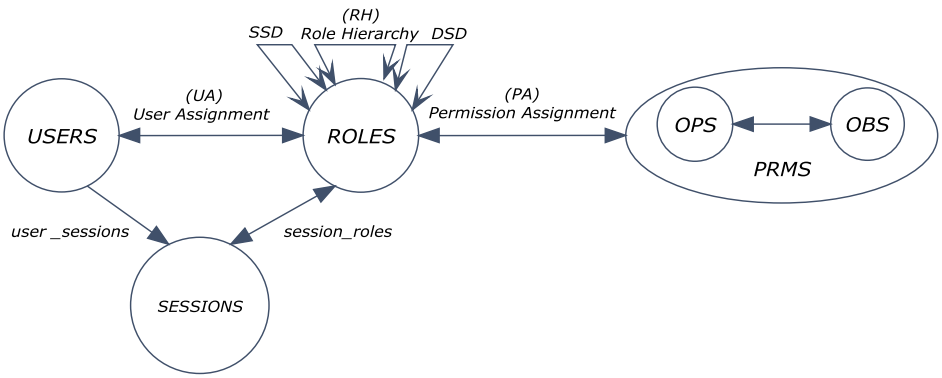


Figure 2.5: RBAC model (source Kim, Ray, France, & Li, 2004)

An important feature of RBAC is its ability to be used in a multi-domain environment. Mapping the security access policies of two domains can be used to

define integrated or multi-domain policies that facilitate the access control and secure interoperation between the domains (Blobel, et al., 2006; Joshi, Aref, Ghafoor, & Spafford, 2001). However, the inherent disparity of roles as well as access permission, which can be expected when working with multiple domains, can limit the effectiveness of using a role-based access control model in a shared care environment. This is discussed in more detail in the following section.

2.4.7.3.4.1 Limitations of Roles

As it was previously presented, roles can be defined based on the structure of the organization or functions that members perform within the organization. This could lead to an ambiguous definition of access permission that can generate security issues when information is exchanged among organizations. Since in RBAC models operations are generically assigned to roles, it is difficult to separate into individual access permissions. However, when the patient 'A' is admitted to 'HA', the assignation of the access permission is done based on the consent given by the patient and not by the access privileged that could be associated to roles. For example, the patient will be treated by Cardiologist 'CA-A' but not the Cardiologist 'CA-B'. Therefore, even though both Cardiologists could have the same role, only cardiologist attending A should be allowed to access the patient's information. Furthermore, in a shared care environment the team of physicians taking care of patient A should be the only ones with access to his medical records. In this case, roles are not sufficient to determine access privileges, but the function of the physician within the team or been part of the team would provide a clear discriminator. In reality, access to the health

information is given to the members of the 'team' treating the patient and not to all physicians with similar roles within the organization. Under these conditions, role-base access control will not provide a suitable solution to the problem of restricting access to those users that are not taking part of the patient treatment.

Since in role-based access control models access permissions are determined by the role assigned to a user, the control that the patient has over the access to specific and sensitive information will be intrinsically limited. In fact, in a conventional RBAC model patient A would not have control whatsoever over permission assigned to his medical records.

2.4.7.3.5 Combining and Extending Access Control Models

Alhaqbani and Fidge proposed a security access control protocol based on a three level access security model. The proposed protocol combines Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based access control in hierarchically layered security mechanism, which determine access to data depending on a set of rules and policies evaluated at each level (Alhaqbani & Fidge, 2007). According to the access hierarchy of the model, access to sensitive information will be determined by a Mandatory Access Control Policy, which provides a solution to the previously described scenario. However, implementation of this model in a shared care environment would be rather complex. In fact, the complexity of EHRs would limit the usability of DAC in a shared care setting since role definition can differ among health providers. Moreover, the complexity of all models could be reduced by reinforcing the policy that allows/restrict access to information stated as sensitive.

Motta and Furuie proposed a Contextual Role-Based Access Control (C-RBAC) model, which extends the conventional RBAC definitions by including contextual information to determine access permissions to patients' data (Motta & Furuie, 2003). In this case, the model allows the statement of pacific restriction by adding contextual data to restrict the access to the information. Context information such as physicians assessing of patient, location and time can be used to determine if a user can be granted with access to information. The model was developed to be flexible in granting fine-grained access privileges in large health care centres using RBAC. Nonetheless, its definition and structure limits the model to local environments, which made the model unsuitable for shared care environments with participation of multiple health care providers.

Peleg et. al proposed a solution based on contextual RBAC model, which considers the definition of scenarios, which are called situations, in which user would be allowed to access EHRs. Situations are described and classified, and each classification would define a pattern that can be applied when a user is requesting access to information (Peleg, et al., 2008). The Situational Role-Based Access Control (S-RBAC) model could also be used to manage access permissions over remote repositories by applying patterns that define situations in which inter-institutional exchange of information is allowed. However, the model was developed using a patient centric approach which did not directly consider requirements of all possible stakeholders. Additionally, since the model is based on RBAC, conflicting roles and access policies would be expected when data is exchanged among different health care providers, which will increase the

complexity in defining situational patterns for data exchange and release. Also, if additional health providers and all possible stakeholders' scenarios are described and included, the number of pattern would potentially increase as well as the complexity of managing access permissions.

Table 2.4: Comparison of access control policies

	MAC	DAC	RBAC	C-RBAC	S-RBAC
Complexity	Low	Low	Medium	High	High
Multiple users	Restricted	Restricted	Possible	Possible	Possible
Policy management	Rigid/Restricted	Flexible/Restricted	Applicable	Applicable	Applicable
Fine-Grained access	Applicable	Restricted	Restricted	Applicable	Applicable
Pros	Guarantees protection over accessed data Allow Fine-Grained access restrictions	Policies are Flexible	Allows management of access right at group level Facilitate the management of access right in large organizations	Considers the contextual information to determine fine-grained access to medical records	Considers the contextual information to determine fine-grained access to medical records Is designed for share care settings
Cons	Protection policies are centred on the information rather that user or user groups. Difficult to implement in large organization with multiple user and groups accessing the data	Establishment of ownership over the data is rather difficult in shared care environments. The model lack the ability to support dynamic change of access right It is limited and difficult to manage in a shared care scenarios	Lacks the ability to specify fine-grained access right for users Constraints are not flexible Different role definitions could be present when information is exchange among health providers	Is not designed for share care settings	Model is mainly patient centred, and does not consider all stakeholders Level of complexity potentially increase with the inclusion of additional situations Different role definitions could be present when information is exchange among health providers
	All models require memorization of PIN or passwords. Inherent security issues related to the use of PIN, passwords or Smartcards such as allow unauthorized share and delegation of access rights, impersonation and accidental lost of access credential. In each case it is more likely that users would be able of refuting electronic transactions. Current research and implementation are exploring share care environment scenarios. Higher maintenance costs				

2.5 Chapter summary

In this Chapter, the concept of health information systems was introduced on section 2.1. Special focus was put on Electronic health record systems and their significance for shared care environments. Security and privacy of Electronic health record along with the ethical and legal implications of protecting the privacy and confidentiality of patients were discussed on sections 2.2 and 2.3.

Section 2.4 introduces and discusses the concept of shared care environment and interoperability of electronic health record systems. A broad introduction to standard for interoperability is also included in this section. HL7 its use and limitation are largely discussed in this section; this is because this standard has been selected in the implementation of a prototype based on the proposed solution. The prototype and its description is disused later in Chapter 5.

Security issues for interoperable electronic health records in a shared care environment have been discussed through sections 2.4.5. An analysis of information and security requirements for data exchange in different health care settings is discussed on section 2.4.6. At this point it is important to understand that any solution, and therefore the solution proposed in this thesis, should consider the four global security needs with their implications. Availability of the information should not only guarantee the access but also ensure the principles of relevance and “need to know”. On one hand, the principle of relevance would warranty that only the required information is released. On the other hand, the principle of “need to know” would guarantee that those that require the access

would be allowed to retrieve the information. In this way, in a shared care environment the confidentiality of the information not only applies to the transmission of information but also at any point in which the information can be accessed.

Section 2.4.7 present the traditional authentication and access control approaches used by modern health information systems to protect electronic medical data. Biometric technology and it use in health information is presented as an approach used to increase and facilitate the protection of health information. The security technologies that have been reviewed are: Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and extended Access control models (The three Level Access Security Model, Contextual Role-Based Access Control Model and Situation Role-Based Access Control Model). A comparative analysis which points out the main characteristics as well as limitations of each approach is also discussed in this section. In fact, form this analysis can be implied that actual access control methods do not provide a solution for a share care environment. Access controls, security, interpretatively of EHRs are essentials in shared care. In the same way, organization policies and consent are necessary to protect the information confidentiality when patient data is share among health care units. The solution proposed in Chapter 4 collects these elements and provide a specification that guarantees the confidentiality of the information.

In the next Chapter, a privacy protection approach which uses attribute-based encryption mechanism to grant access to transmit electronic medical records is presented.

Chapter 3

Research Design and Methodology

The methodological approach and research stages will be introduced and described in detail. The research will be undertaken considering an analytic generalization of a case study. A prototype implementation followed by test and simulation would be conducted to analyse the proposed solution.

3.1 Research Design

The exploratory research has been based on the analytic generalization of a case study. The research will be focused on the analysis of case studies, modelling of a software specification and the controlled simulation and test of a security mechanism. The security mechanism will be design as a communication interface which will allow the exchange of medical records between electronic health record systems. The cases studies will provide scenarios in which information is exchange among health care units. The simulated case study described in Chapter

5 will be used to analyse and test a prototype implementation of the proposed solution. Meanwhile, Chapter 6 will provide a real situation in which the proposed solution can operate.

The simulated case will be based on a standardized representation of an Electronic Health Record system and will consider the following requirements:

1. The simulated scenario will consider both data exchanged within a single unit and an inter-institutional prospective.
2. The data will be exchanged using HL7 messaging standard.
3. The data does not have any level of aggregation.

The selected unit of analysis will allow an in depth study of how proposed security approach can be implemented under a complex health care environment.

3.2 Research Methodology

This research is based on the analysis of case studies and the development of software components as a method of study. The development of a prototype software interface will facilitate the analysis of security measures for data exchange under a shared care environment. Therefore, the assumptions obtained would be based on an analytical generalization of the data collected through the different stages of this research.

The prototype development is a useful method to study the effective design, delivery, use and impact of information technology (Keen, 1987). System development approach is considered an applied research method which is used to test the validity and limitations of a proposed theory (Burstein, 2002). In this line,

system development method allows both the implementation of application used to illustrate a theory and the refinement of the proposed theory based on the data obtained from observations made during its implementation and testing (Burstein & Gregor, 1999; Parker, Wafula, & Swatman, 1994). Therefore, system development could be a central component of a multi-Methodological research cycle (Nunamaker, Chen, & Purdin, 1991). In order to conduct the software analysis, a prototype version of the proposed architecture would be implemented. The prototype will be configured as a set of integrated libraries and components based on a conceptual approach for secure exchange of electronic health records, this is described in chapter 4.

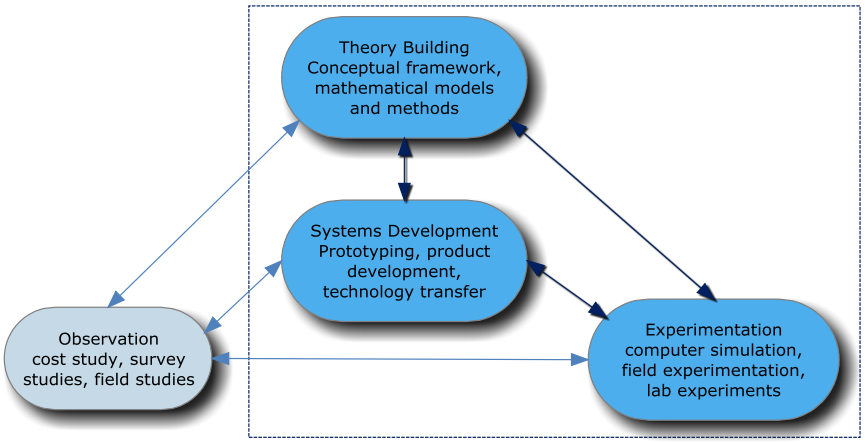


Figure 3.1: Software development-Methodological research cycle (adapted from Nunamaker et al. 1991, p.94)

The conceptual approach as well as the prototype implementation and testing of the proposed solution are discussed in Chapter 4 and in Chapter 5 respectively. The conceptual component if this research will be centred in literature review and conceptualization obtained by the analysis of case studies which are included in Chapter 2, 5 and 6. As it is shown in Figure 3.1, the prototype component of

research will centred in theory building and the development of a conceptual framework (requirements for a shared care environment) based on system development and experimentation, and it will not include observations such as cost studies, survey studies or field studies.

3.3 Research Stages

The research has been divided into six stages and four supporting activities and methods. The first stage, Literature Review, has the purpose of analysing the state of art regarding to the security mechanisms and approaches used to protect the access and exchange of electronic health records, with special interest in the protection of patient's confidentiality. A discussion of the standards used in Australia for definition and exchange of Electronic Health Records is also included at this stage. The importance of this discussion is the later establishment of the minimal requirement of a standard data repository that would be used during simulations. Finally, determining security issues that current approaches may present and how these issues may affect the protection of patient's confidentiality during the exchange of medical records are also included in this stage.

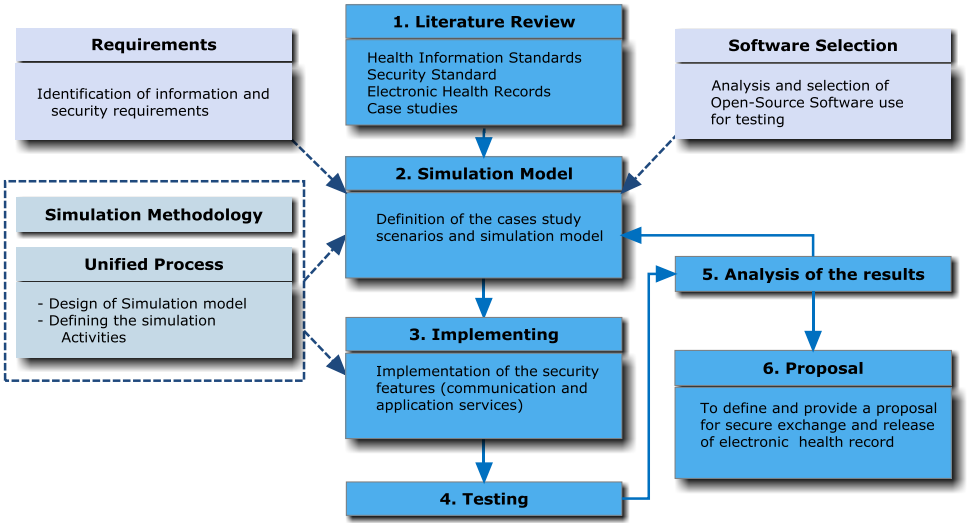


Figure 3.2: Research Method

The second, third and fourth stages consist in the definition of the security features required for the secure exchange and release of the information. At this stage an approach for secure exchange of data will be described. At this point, an analysis of open-source EHR applications in order to select a software application is conducted (section 5.1). A prototype interface which incorporates the basic features of the proposed architecture and uses the selected open-source EHR system would be implemented at this stage (section 5.2). A set of scenarios based on a case study are used as test of simulation models (section 5.3 and Chapter 6). The analysis of the tests will help to determine the performance of the proposal for protecting health care information (section 3). In stage five, the data collected from the tests and simulations of the scenarios will be in the analysis (section 5.3.1.3). At this point the data collected will allow the understanding of the behaviour of the proposed security implementation. The result generated from the tests will help to determine the viability of the proposal for secure exchange and release of electronic health records (stage 6).

The supporting activity of "Requirements" will be conducted to identify the information needed for a secure electronic health record system (section 4.2.1). This activity will be conducted considering the requirements and principles for patient's privacy and confidentiality. A simulation methodology will be used to follow the experiment procedures.

Finally, the Unified Process (UP) of Software Development will be employed as a main methodology for the design, development of both the simulation case and the final proposal (sections 4.2, and 4.3). The Unified Modelling Language (UML) will be used as the visual language for modelling the components of the prototype (Arlow & Neustadt, 2005).

3.4 Chapter Summary

The methodological process used to undertake this research has been described in this Chapter. The research has been divided into six stages from literature review through the final proposal definition. In order to conduct the research case studies will be used and a software prototype will be implemented and tested against the case studies. The design and implementation of the prototype are described in Chapters 4 and 5. The case studies are described in Chapter 5 and Chapter 6.

In the next Chapter, a privacy protection approach which uses attribute-based encryption mechanism to grant access to transmit electronic medical records is presented.

Chapter 4

Conceptual Approach

This Chapter describes the conceptual approach of the proposed solution for secure access in a shared care environment. The proposed approach uses Attribute-based encryption to encrypt a codified HL7 message which is transmitted through an insecure channel. To explore and describe the proposed model a generic case is presented and discussed through the Chapter. The requirements and analysis that describe the model definition and the further implementation of a prototype interface for secure exchange of HL7 messages as well as the security components are also included in this Chapter. The aim is to provide a specification of software that allows the exchange and release of information in a share care environment. This includes not only the secure transference of the information but also the observation of the policies and consent provided by the patient. This concepts have been largely discussed in

chapter 2, moreover Chapter 6 provide a real case scenario in which this is exemplified in more detal.

4.1 Generic Scenario

As a simplification of the problem and with the purpose of providing a framework for the analysis of the requirements let us assume the following generic scenario. A common activity in a shared care environment is sharing information among the team involve in the care of a patient. Considering the existence of an integrated multi-institutional health information system in which access can be granted to all members of the team and information can be remotely requested and retrieved. The generic scenario is the remote information request and access of partial or complete electronic health record of a patient. The first component to be described is the formatting of the message. Has it has been disused in Chapter 2, HL7 will be used for the generation of a standardized message. Therefore, The HL7 message module for data exchange between two Electronic Health records Systems is the first component of the proposed specification. In this case, the information of the message will be mapped from the original databases into standard HL7 messages for data exchange. The information is collected from an external data repository, encrypted accordantly to a set of attributes (policies) and securely transmitted to the requested destination. Once the message is received the encrypted data can be retrieved only by users that have a secret key with a minimal set of attribute values that overlap those of the encrypted data as it is described in section 4.2.4.

4.2 Proposed Architecture

4.2.1 Main Functionalities

The proposed interface should be able to play three roles: requesting, sender and receiver. In this sense, the system should be able to,

- Accept an information request from a local user and redirect the request to a remote repository (information system). In this case, the system plays the role of a requesting process.
- Receive, process and answer requests posted by remote processes (system). In this case, the system plays the role of a sender application.
- Accept and process information received from a remote sender application. In this case, the system plays the role of receiver application. The information will be processed and stored on local files or/and databases.

In addition, the interface should guarantee the authorized access to remote EHR repositories and be able to secure the information during the transference and release of the message.

4.2.2 Use Cases for Functional Requirements

As it was explained previously, the functionalities have been divided into three families depending of the role that the interface will play during the transference of messages. The starting role is requesting; the local user will require to the interface the sending of a request for partial or complete EHR regarding a subject of care. In this case, the interface will play the role of a "requesting process". The remote interface will process the request and return a standard HL7 message to

fulfil the request; in this case, the remote interface plays the role of "sender". Finally, the local interface will receive the message and inform to the user that the information has been received; the user will be able to access the HL7 standard document received and save the data within the message in the local database or document in a local directory (or both).

Figure 4.1 shows an overview of the communication between system interfaces, and how user and system will interact with each other. This abstract representation of the system considers the users and processes. A user is the person who is requesting the information, such person is an authorized user that has accessed the local system. In a multi domain environment it is assumed that role policies may vary in definition and scope from one domain to another and, therefore, the access permission for specific roles also may differ. For the purpose of this abstract representation, it is assumed that a policy controversy model has been considered. Therefore, it is understood that any request of information made by an authorized user will be processed considering the credentials used by the user at the time of the request.

The actor process is an abstract generalization of the local and remote interfaces, this generalization has been represented as a method to simplify the representation of the system and, therefore, facilitate the understanding of the problem. It also assumes that both interfaces may perform similar tasks at certain given time. For example, considering interfaces A and B, A represents the local interface that will be accessed by the user to request information from a remote system; B is an interface located at the remote system. In this case, A will send a message that

includes the information requested by the user; B will process the request and return a message with the information originally requested. For the contrary, if interface B request information to interface A, B will submit the request and A will process and send back the information requested by the user. This analogy can describe any pair of interfaces that are exchanging information at any given time.

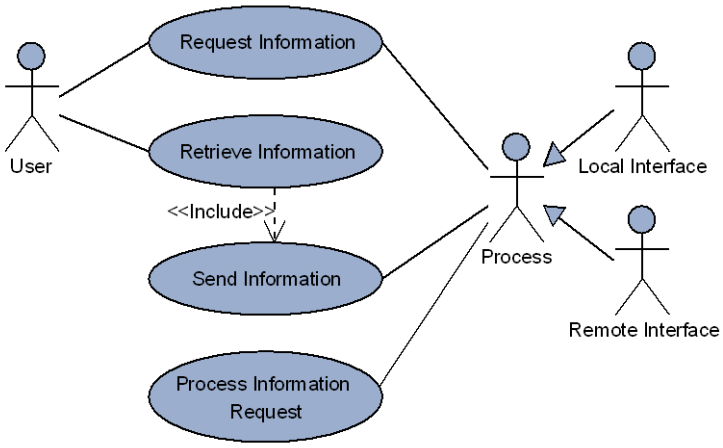


Figure 4.1: Process Overview

This model representation provide the conceptual communication infrastructure for data exchange. In the following sections, both roles requesting and sending are described in more detail.

4.2.2.1 Interface Requesting Role and Use Case Model

Five use cases describe the requesting and receiving roles of the interface. In this case, the interface behaves as a remote client that requests a set of data from an electronic health record repository (Figure 4.2). The use cases are described as:

- Information Request (`InformationRequest`): Local user request a message from a remote repository (remote Electronic Health Record System) according to the following flow:

  1. The user requests a partial or complete electronic health record from a remote information repository.
  2. The system asks for request criteria.
  3. The user enters the request criteria.
  4. Systems send a message request to a remote process (remote interface).
  5. System changes state of message requests to Requesting Information.
  6. Remote process accepts the request.

- Information Replay (InformationReplay): Local system retrieves information sent by the remote process according to:

  1. The remote process sends an encrypted message that contains the required information to the local system interface.

  2. The system interface recovers the message with the information sent by the remote system.

  3. The message is temporarily stored.

  4. The system flags the user to indicate the availability of requested information (change the status of the request message to receive a message)

- Access to Information (`InformationAccess`): Local user recovers the receive a message that contains the information originally requested from a remote repository.

1. The user receives a flag indication that the information is available for retrieval.
2. The user requests access to the information.
3. The system will retrieve the message to the user as a medical document containing the original requested information. To allow the access to the encrypted data the user provides a secret key with the minimal set of attributes for decrypting the data. More detail of this process is provided in the following sections.
4. The system displays the medical document on the screen.
5. System changes the status of the request message to Read.

- Save information in database (`SaveInDatabase`): Local user recovers the received message and request to store the data in the local database.
  1. The user selects the option saved in the database.
  2. The interface formats the data within the received HL7 messages to fulfil local database requirements (vocabulary and structure).
  3. The interface accesses the local database.
  4. The interface stores the data.
  5. The system sends a successful status message to the local user and changes the status of the request message to saved.

- Save Message as a file (`SaveAsDocument`): Local user recovers the message received and requests to sore the message as medical document in a local directory.
  1. The user selects the option to save as medical document.
  2. The interface saves the document in a predefined local directory.

3. The interface accesses the local database.
4. The interface stores a link to the medical document.
5. The system sends a successful status message to the local user and changes the status of the request message to saved.

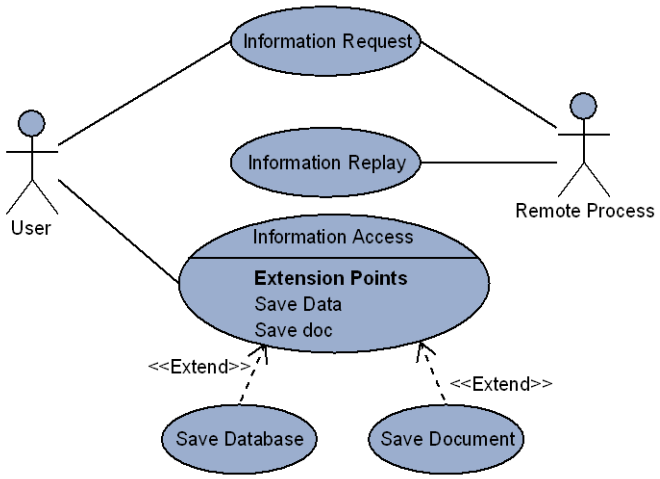


Figure 4.2: Interface requesting and receiving roles

4.2.2.2 Interface Sending Role and Use Case Model

Five use cases describe the sending role of the interface. In this case, the interface performs as a remote service that accepts remote requests and returns standard HL7 messages (Figure 4.3). The use cases are described as:

- Information Request (`InformationRequest`): Remote process requests medical information (partial or total electronic health record of a patient).
  1. A remote process triggers a request to the local interface system.
  2. The software interface accepts the request.
  3. The software interface returns an acceptance request message to the remote system.

4. The local system changes the state of the status of the message request to processing.

- Process the request (`ProcessRequest`): The system processes the information request.
  1. System checks information for availability.
  2. System maps the information required to define a standard message.
  3. The system interface formats the collected data accordantly to standard HL7 vocabulary.
  4. The system instantiates a message based on standard HL7 definitions.
- Replay to request (`SendReplay`): The system interface replies to the remote request.
  1. Include (ProcessRequest).
  2. The system interface serializes message content.
  3. The system interface sends the message.
- Validation of the remote process (`ValidateUser`): The system interface verifies the credentials provided by the remote process requesting the information.
  1. The system interface verifies the user credentials.
  2. The system interface determines that the client process has the rights for accessing the requested information.
- Verification of the request (`VerifyRequest`): The system interface verifies the request.
  1. The system interface verifies if the local database has the critical information required to create the standards HL7 messages.

2. The system accepts the request and proceeds processing the message replay.

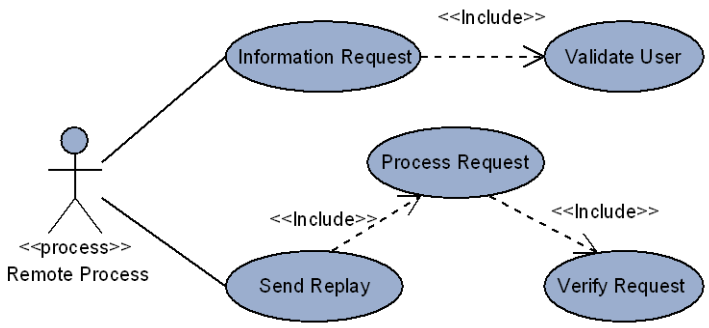


Figure 4.3: Interface sending role use case model

4.2.3 Components

The proposed architecture is described by a set of components that conforms a software interface. The interoperation between interfaces is provided as remote services. In a communication between electronic health records systems both interfaces will operate first as coding or decoding HL7 messages, second encrypting or decrypting a message using attribute-based encryption and finally sending or receiving the message using internet as a communication platform.

It is understood that both interfaces would be independent and can operate with other interfaces of the same nature as well as other electronic health record systems. Figure 4.4 presents a graphical representation of each one of the components as well the information flow of the proposed interface.

In the model, the local system describes the existing software platform which includes an electronic health record systems and a data repository. The electronic

health record system provides the user interface for both requesting information from an external repository and retrieving information received form an external repository. The data repository is the source of information used to generate the messages as well as the local storage unit where the received messages will be maintained.

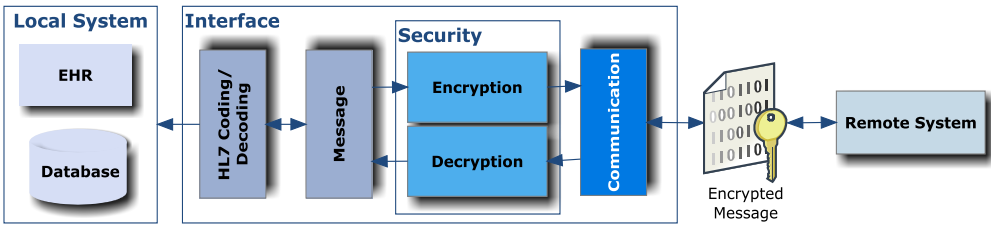


Figure 4.4: Proposed Architecture

The second component of this generic architecture is the interface which is divided into four subcomponents. Each subcomponent has been specified to perform a specific task. The first component is the HL7 coding and decoding module. The HL7 module is a set of libraries based on the HL7 application programming interface (HAPI). The HAPI library is an open-source, object-oriented HL7 parser library for Java applications. The HAPI project was initiated by University Health Network in Toronto, Canada. Message, is the resultant object of encoding a set of records retrieved from an electronic health record repository. In the model, the module is used to produce HL7 messages that will be produced upon request as well as to decode messages that have been received from an external application.

The security module is divided into two subcomponents. The first component is used for encrypting the generated HL7 message based on a set of attributes (policies). The second component is used for decrypting the received encrypted HL7 message. Attribute-based encryption is used as the security mechanism to

encrypt and decrypt the message. The encryption procedure is described in detail through the section 4.2.4. The final component of the interface is the communication module. The communication module provides a connection with an external source in order to request or receive an encoded and encrypted message.

4.2.4 Attribute-Based Encryption Component

4.2.4.1 Overview

Attribute-based encryption (ABE) has its origins in Identity-Based Encryption (IBE) schemes, firstly, proposed in (Boneh & Franklin, 2001). The IBE scheme allows a sender to encrypt a message using an identity without the use of a public key infrastructure (Sahai & Waters, 2005; Shamir, 1985). In this case, the identity is viewed as a string of characters that represent a certain number of attributes (e.g. user's name, an email address, or telephone number) that serve as a user's public key (Liu, Guo, & Zhang, 2009). A secret key, which is provided by a trusted private key generator (PKG), is used to decrypt the data. The secret key is provided only if the user has been successfully identified by the PKG (Au, et al., 2008)

Sahai and Waters introduced the notion of attribute-based encryption (ABE) as a security approach for reinforcing access control (Sahai & Waters, 2005, 2008). The attribute-based encryption approach allows a ciphertexts to be decrypted by more than one recipient, unlike the traditional public key cryptography methods (Bethencourt, Sahai, & Waters, 2007). In its place, both the users' secret keys and

ciphertexts are associated with a set of attributes or policies that are used to grant access to the encrypted data. Attributes are defined as set of strings, in this case represented by access policies, which are associated to an access structure or access tree that is applied to the encrypted data. A user would be able to decrypt an encrypted data only if he/she possesses a secret key with attributes that overlap the attributes used during the encryption of ciphertext (Bethencourt, et al., 2007; Ibraimi, Tang, Hartel, & Jonker, 2009). In other words, to allow a user to decrypt a ciphertext, at least *k* attributes must overlap between the identity used to generate the ciphertext and his secret keys. Note that not all but *k* attributes are sufficient to grant access to the encrypted data, which is represented as an error-tolerance in the model (Sahai & Waters, 2008). This error-tolerance would also allow the implementation of Fuzzy Identities or Attribute-Based Encryption schemes for biometric technology (Sahai & Waters, 2005). Fuzzy Attribute-based encryption is not disused on this thesis; however, the paper "Biometric for Electronic Health Records" provide more details in how this approach can be used in a health environment (Flores Zuniga, et al., 2009). In this section, we will present and describe an Attribute-Based Encryption scheme and how it can be applied to protect the information of parties during the exchange and release of EHRs.

4.2.4.2 Description of the Data Encryption Process

Considering the scenarios previously described, the exchanged information is maintained encrypted until an authorized user, with the sufficient *k* attributes, proceeds to decrypt the message completely or partially. In this case, a secret key, *SK*, is used to decrypt the ciphertext encrypted with the initial attribute set (access

policies), *Ap*, if and only if the attributes that the user possesses are sufficient as measured by the "set overlap" distance metric for the security policies used to encrypt the data (Sahai & Waters, 2005). The scheme requires of a trusted authority, known as the Private Key Generator (*PKG*), with the task of generating the secret key (*SK*). The *PKG* will provide such a secret key only after the user has been successfully identified (Au, et al., 2008). The generated key can then be used to decrypt the ciphertext originally received from the sender. In the Figure 4.5, *k* denotes the minimal number of attributes that the user must have in order to decrypt the message or part of it.

This approach guarantees that only users that have access privileges (appropriated attributes) would be allowed to access the encrypted data. The access privileges are described by the security policies used to encrypt the data. A user that does not have the attributes required to decrypt the data will not be able to access the information. If the security policies attached are hierarchically associated to information, the access could be provided at different levels for different users. In this case, user will be able to access different level or contents within the encrypted data depending on the attributes associated to their access privileges. This is known as access tree.

The access tree indicates the different levels in which the encrypted information can be accessed by the authorized users. Each node of the tree represents a set of attributes and the conditions required to decrypt the message. The access tree provides to the proposed solution the required flexibility in the definition of the

access privileges needed in a shared care environment. The implication of the access tree is discussed in Chapters 5 and 6.

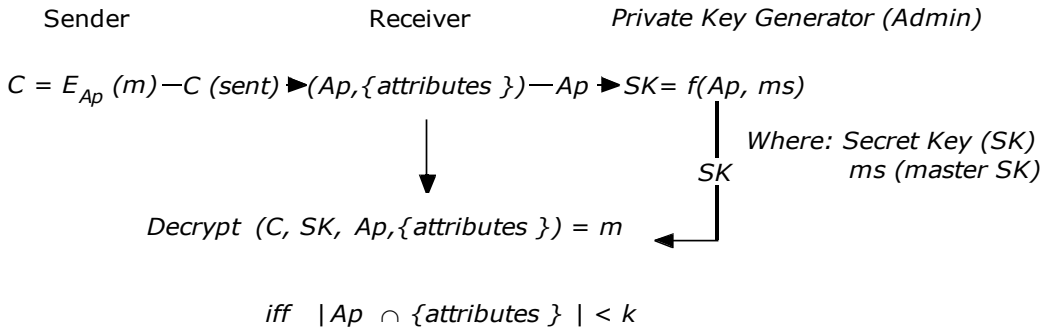


Figure 4.5: Attribute-based encryption

4.2.4.3 Security Module

The security module has been implemented based on an open source encryption tool kit developed and distributed under GNU General Public License (GPL) by John Bethencourt (Bethencourt, et al., 2007). The selected toolkit is available under the Advanced Crypto Software Collection website of the Department of Computer Science at University of Texas at Austin. The model of the module assumes the following construction.

Let $\mathbb{G}$ be a bilinear group of prime order p, and let g be a generator of $\mathbb{G}_0$. In addition, let $e: \mathbb{G}_0 \times \mathbb{G}_0 \rightarrow \mathbb{G}_1$ denote the bilinear map. A security parameter, κ, will determine the size of the groups. The Lagrange coefficient is defined as $\Delta_{i,S}$ for $i \in \mathbb{Z}_p$, and a set, S, of elements in $\mathbb{Z}_p$: $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$ and the hash function $H : \{0,1\}^* \rightarrow \mathbb{G}_0$ which is modelled as a random oracle.

The function will map any attribute described as a binary string to a random group element.

Setup. The setup algorithm chooses a bilinear group $\mathbb{G}_0$ of prime order p with generator g. Next it chooses two random exponents $\alpha, \beta \in \mathbb{Z}_p$. The public key is published as:

$$PK = \mathbb{G}_{0,g,h} = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha}$$

And the master key MK is (β, g^{α}).

Encrypt (PK, m, Ap). The encryption algorithm encrypts a message *m* under the tree access structure *Ap*, which describes the set of attributes (polices) that will be applied. The algorithm first chooses a polynomial q_x for each node *x* (including the leaves) of the access structure. These polynomials are chosen following a top down approach, starting from the root node *R*. For each node *x* of the access structure, set the degree d_x of the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$.

The algorithm chooses a random $s \in \mathbb{Z}_p$ staring at the root node R and then sets $q_R(0) = s$. Afterwards, it chooses d_R other points of the polynomial q_R randomly to define it completely. For any other node *x* of the access structure, the algorithm sets $q_x(0) = q_{parent(x)}\big(index(x)\big)$ and chooses d_x other points randomly to completely define q_x.

Let, *Y* be the set of leaf nodes of the access structure *Ap*. The ciphertext is then constructed by giving the tree access structure *Ap* and computing

$$C = \Big(Ap, \tilde{C} = me(g,g)^{\alpha s}, C = h^{s},$$

$$\forall y \in Y\colon\ C_y = g^{q_y(0)} \cdot C'_y = H\big(att(y)\big)^{q_y(0)}\Big)$$

KeyGen(MK, S). The key generation algorithm takes a set of attributes S and provides as output a key which identifies with the attribute set. A random r ∈ $\mathbb{Z}_p$ is first chosen by the algorithm, and then a random $r_j \in \mathbb{Z}_p$ for each attribute j ∈ S is selected. The key is provided accordantly to

$$SK = \left(D = g^{(\alpha+r)/\beta}, \quad \forall j \in S: \quad D_j = g^r \cdot H(j)^{r_j}, D'_j = g^{r_j}\right)$$

Decrypt (CT, SK). The decryption is managed by a recursive algorithm that takes the ciphertext $C = \left(Ap, \tilde{C}, C, \forall y \in Y: C_y, C'_y\right)$, a secret key SK, which is associated to a set of attributes S, and a node *x* from the access stricture.

If the node x is a leaf node, then let $i = att(x)$ and define as follows: If $i \in S$, then

$$DecryptNode(C, SK, x) = \frac{e(D_i, C_x)}{e(D'_i, C'_x)} = \frac{e\left(g^r \cdot H(i)^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})} = e(g,g)^{r q_x(0)}$$

If $i \notin$ S, then define DecryptNode(CT, SK, x) = ⊥.

When *x* is a non-leaf node the algorithm DecryptNode(CT, SK, x) proceeds as follows: For all nodes *z* that are children of *x*, it calls DecryptNode(CT, SK, *z*) and stores the output as F_z. Let S_x be an arbitrary k_x-sized set of child nodes *z* such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns ⊥.

Otherwise, it computes

$$F_x = \prod_{z \in S_x} F_z^{\Delta_{i,S'_x}(0)}, \qquad where \begin{matrix} i = index(z) \\ S'_x = \{index(z) : z \in S_x\} \end{matrix}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_z(0)}\right)^{\Delta_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_{parent(z)}(index(z))} \right)^{\Delta_{i,S'_x}(0)}$$

$$= \prod_{z \in S_x} e(g,g)^{r \cdot q_x(i) \cdot \Delta_{i,S'_x}(0)}$$

$$= e(g \cdot g)^{r \cdot q_x(0)}$$

Finally the decryption algorithm is started by a simply calling of the function on the root node R of the access structure. If the access structure is satisfied by S $A = DecryptNode(CT, SK, R) = e(g,g)^{rq_R(0)} = e(g,g)^{rs}$ is set. Then the algorithm decrypts by computing

$$\tilde{C}/(e(C,D)/A) = C/\left(e\left(h^s, g^{\frac{\alpha+r}{\beta}}\right)/e(g,g)^{rs}\right) = m$$

4.3 Information Flow during the Data Exchange

The activity diagram is an UML artefact that provides an overview of the different activities contained within a complex process (Arlow & Neustadt, 2005). For the proposed solution, the activity diagram represents the information flow during the request and retrieves of electronic health records. To provide a better understanding of the situation, the diagram has been partitioned in two swim-lines that represent both the local and the remote system. A swim-line represents the information flow between subsystems or, in this case, systems. Each swim-line includes a defined set of activities that each interface will perform during the process of information exchange. The process of requesting/retrieving information has eleven activities six executed by the local interface and five by the remote system interface.

The activities associated to this particular process are described as follows:

1. `Information request`: the local user requests information from a remote data source. After the user is validated at the local system, he will request information that is available on a remote source. To make the request the user should introduce a request criterion. The request criteria will be used to recover the information at the remote system. The criteria introduced by the user will depend on the type of information that will be requested, in any case the criteria will be used by the remote application in order to search and retrieve the specific information requested by the user.
2. `Verify user`: this activity verifies the validity of the request in terms of access rights that the user may have. If the user does not have the appropriate rights to access the request information the remote system will reject the requests. Otherwise, the system will proceed with the request.
3. `Check Availability`: the remote system will check if the requested information (based on the criteria provided) is available or not. If the information is available the system will proceed with the request, otherwise the system will reject it based on the fact that the information is not available.
4. `Send rejection message`: the remote system interface will send a message to the local system in the case that the request has been rejected. The two possible reasons of rejection are that the user does not have the rights to access the information or that the information requested is not available.
5. `Inform rejection`: this activity only will be executed if the original request has been rejected. The local system will be informed that the

request has been rejected by the remote system. The message will also include the reason why the request has been rejected.

6. `Process request`: the remote system will proceed by processing the request, this activity involves: 1) retrieving the necessary information from the database (map the database) and generating the standard HL7 message.
7. `Send replay`: a replay with the standard HL7 message will be returned to the local interface.

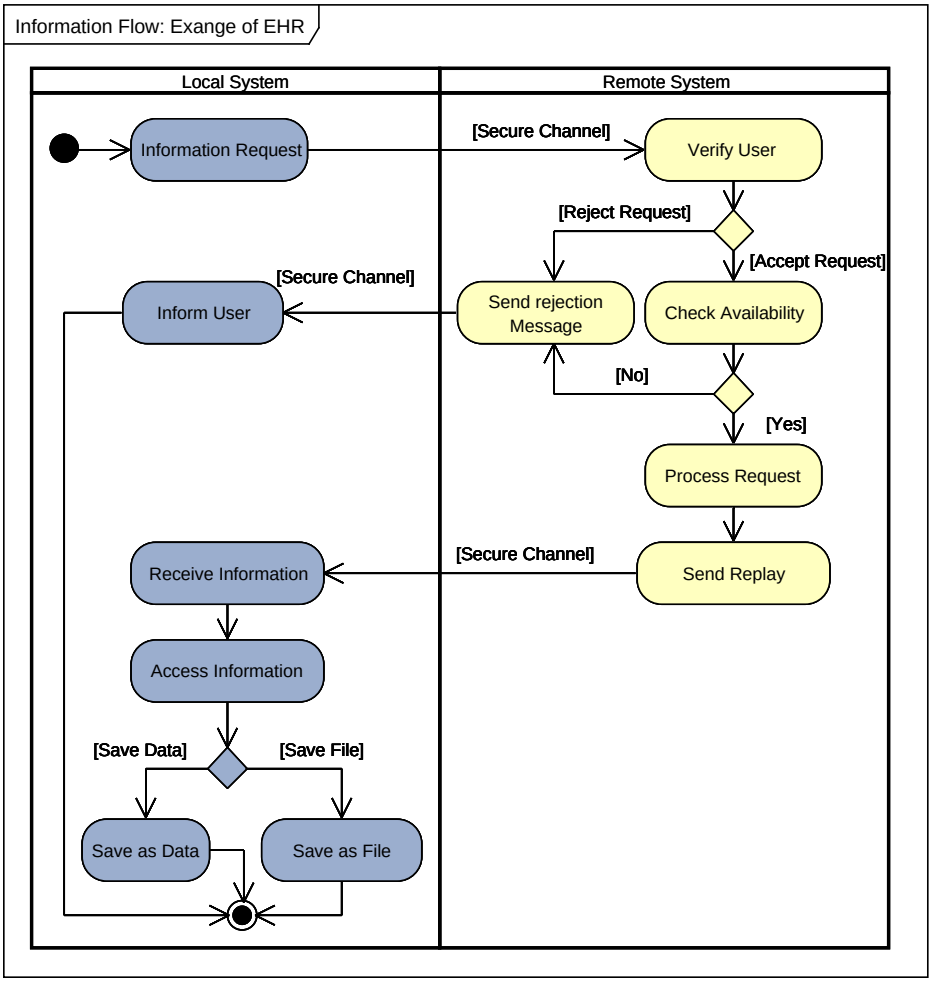


Figure 4.6: Information flow during the data exchange

8. `Receive Information`: The information will be retrieved and saved temporarily by the local interface. The interface will signal to the user informing the availability of the message.
9. `Access Information`: The user will request the recovery of the Hl7 message; it will be displayed on screen.
10. `Save data`: The user may select save the information as data in the local database or as an associated file within the system. In case that the data is stored on the local database, the system interface will proceed with restructuring the data accordantly to local requirements. Finally, the information will be stored on the local data repository.
11. `Save as Document`: this option will allow the local interface to save the information as a file in a local directory.

4.3.1 State Machine for Data Request

The state machine is a UML artefact that provides a dynamic behaviour of the life cycle of a simple object, represented as a finite number of states (Arlow & Neustadt, 2005). The state machine diagram for the information request shows the different states of a single request message. At any time the object of the state diagram is associated to a specific request. Even though during the request and retrieve of electronic health records, there will be several object interacting `MessageRequest` will be considered as a single object that will be changing states and signalling during the process of information exchange.

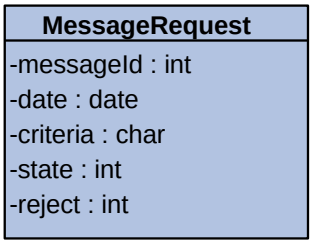


Figure 4.7: Abstract Class MessageRequest

The classification `MessageRequest` represents persistent objects that have the following attributes:

- `messageId`: an integer number that is used as an identification of the message request.
- `date`: stores the date of the request
- `criteria`: a multi-value attribute that maintains the selection criteria used during the retrieved of information.
- `state`: an integer attribute that maintains the actual status of the request
- `reject`: an integer attribute that maintains the rejection value associated to: 1) rejection based on insufficient user rights and 2) rejection based on unavailability of required information.

Seven possible states, that cover the complete life cycle of requesting-retrieving process, have been defined for the Message Request object. They are described as follows:

1. Requesting information (`RequestingInfo`): during this state, the user will post a request partial or complete retrieve of information of a patient's electronic health record. To proceed with the request the user will introduce request criteria (identification information) for data retrieve. The

software interface will retrieve the request criteria, prepare the requested and send the message request to a specific remote system interface.

2. Processing (`Processing`): if the request for information is accepted, the remote software interface will start processing the request. At this point, the `MessageRequest` objects will change state to possessing and the software interface will signal the change of state. During the processing state two possible outcomes can be generated. If the required information is available on the system a standard HL7 message will be produced. Otherwise, the system will reject the request in the basis that the information required is not available.
3. Rejecting request (`RejectingRequest`): the rejection of a request can be generated under two circumstances 1) unauthorized access to requested information and 2) unavailability of the information. In the first case, the system will reject the request based on the fact that according to the local requirements, local and common policies and security restrictions, the user who has requested the data does not have the required credentials to access the information. The second case, the request will be rejected based on the unavailability of the requested information. In both cases, the remote interface will signal the circumstances in which the rejection was produced. In this case, the signal will contain a message request Id, date and rejection circumstances.
4. Replaying request (`ReplayingRequest`): before sending the standard HL7 message the remote interface will precede with the encryption of the message in order to generate a secure message.

5. Receiving message (`ReceivingMessage`): this is a control state in which the local interface will signal the user to inform that the request message as arrived or that the request as been rejected by the remote system.
6. Read (`Read`): this is a control state in which the local user will indicate that he/she has read the message. If the message is a rejection it will become the final stage of the associated `MessageRequest` object.

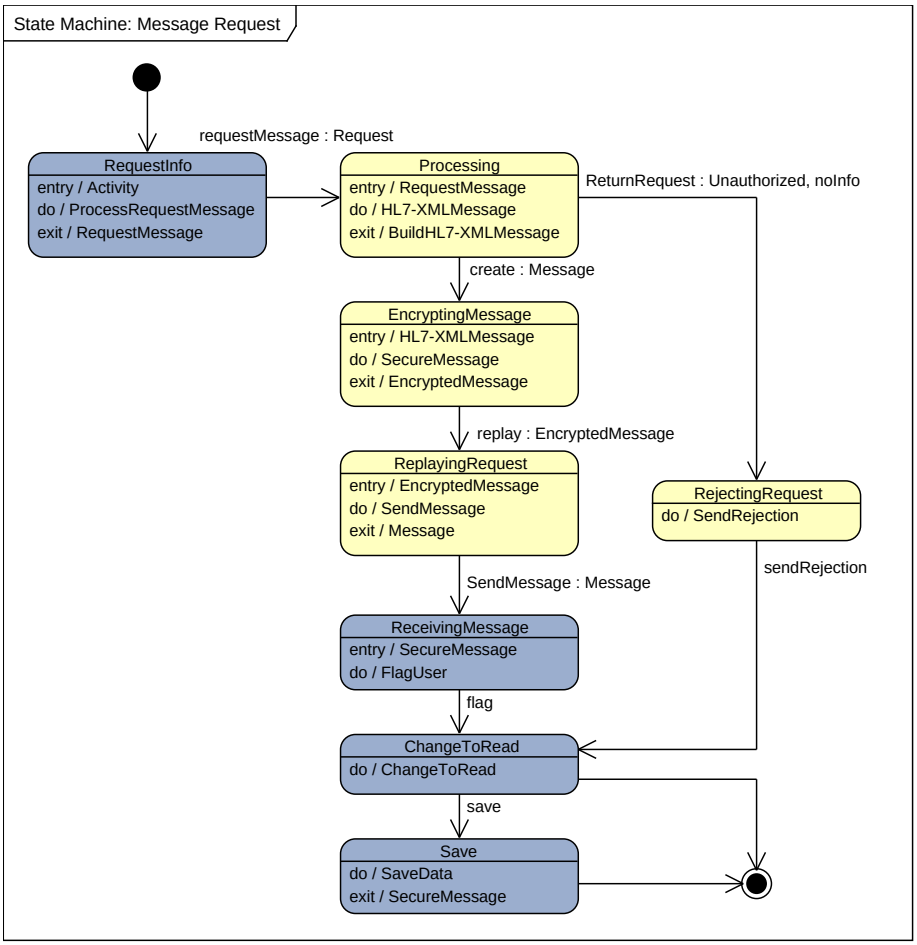


Figure 4.8: State Machine - Message Request

7. Save (`save`): this is the final state of a success message request. The user will be allowed to save the information as an Electronic Document and/or

as records in the local database. The local interface will change the state of the associated "Message Request" object to indicate that the information received has been stored by the user.

4.4 Chapter Summary

In this Chapter, a conceptual approach for access control which reinforces access policies using attribute-based encryption schemes has been presented and discussed. Attribute-based encryption allows the encryption and decryption of data based on policies, which are represented as attributes associated to the information. The approach allows an independent but secure method to protect the privacy and confidentiality of patients' information transmitted over insecure channels. The model is flexible in providing access to multiple users based on security policies, which describe the access permissions over encrypted data. This characteristic is essential to provide a suitable secure access solution for a shared care environment. The applicability of the access tree will be conceptually and practically described in Chapters 5 and 6 respectively.

A detailed description of the proposed model and the flow of information is also presented and discussed in this Chapter. The description of the state machine for a message request, and the possible states that a message request could have, are described in the section 4.3.1.

The next Chapter will describe the implementation and testing of the prototype interface. Several scenarios are described and later implemented with its analysis and results.

Chapter 5

Implementation and Testing

The purpose of this Chapter is to provide an overview of the implementation and the behaviour of a prototype interface for secure exchange medical data. The use of prototyping techniques allows testing the viability of the proposed solution by using a simulated environment. The implementation is a prototype version which uses HL7 messages and Attribute-based encryption to securely transmit standardized messages containing health records in a shared care environment.

The selection of the software platform (electronic health record system and data repository) that will be used during the implementation is explained at the beginning of the Chapter. Secondly, the description of the components used to generate message requests, standard HL7 messages and encrypt/decrypt the information will be presented and discussed in section 5.2. Then, a scenario that will facilitate the understanding and testing of the interface behaviour is presented

and described in section 5.3. Finally, test results regarding the performance of the software interface are also presented and discussed in section 5.3.

5.1 Selection of EHR Systems

The first step of the implementation was the selection of the electronic health record systems that would be used to implement and test the proposed solution. Several open source electronic health record softwares were selected and then analysed with that purpose. From the selected software only two were used to provide a suitable scenario for implementing and testing the prototype.

The purpose of the analysis has been the examination of open-source EHR systems to determine how their functionalities and architectures conciliate with international standards. To reach that goal, the analysis was based on the level of accomplishment of a set of standard requirements contends in the ISO/TR 20514 and ISO/TS 18308 reports. The ISO/TR 20514 report states standard definition, scope and context for Electronic Health Record Systems (EHRS) meanwhile the ISO/TS 18308 establishes a set of standard requirements for Electronic Health Record Architectures (EHRA) (ISO/TC-215, 2004).

To conduct the analysis twelve active open-source FOSS projects of electronic health records systems (alternatives) were selected[1]. The data used to analyse the software was gathered from the project's web pages, existing product review and documentation, accessing to the source code, and exploring the software

[1] Software analysed: CHITS, Cottege Med, Elexi, FreeMED, GNUmed, MedClipse, MirrorMed, OpenEMR, OpenMRS, OSCAR, PatientOS and Tolven.

functionalities by accessing installed practice sites and the installation of the softwares in testing computers.

Table 5.1: Families or requirement accordingly to the environmental context

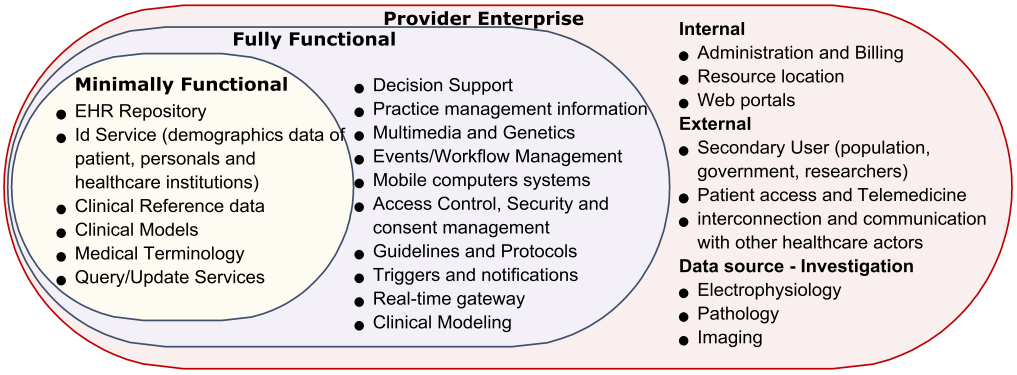
Main classes	Sections	Sub-sections	MF	FF	PE
Structure (n=50)	Record organisation	Sections	1		
		EHR format	1		
		Portability			1
		Secondary uses			1
		Archiving	1		
	Data organisation	Structured data	5		
		Non-structured data	4		
		Clinical Data	1		
		Administrative data		6	
	Type and form of data	Data types	11		
		Support for different types of data	1		
		Reference data	1		
		Contextual data	7	1	
		Links	2		
	Supporting health concept representation	Support for multiple coding systems	3		
		Unique representation of information	2		
		Representation of text	1		
Process (n=24)	Clinical processes	Support for clinical processes		4	
		Problems/issues and health status	3		
		Clinical reasoning		1	
		Decision support, guidelines, and protocols		3	1
		Care Planning		1	
		Orders & service processes		2	
		Integrated care			1
		Quality assurance		1	
	Record processes	Data capture	3		
		Retrieval/query/views of data	1		
		Presentation of data	1	1	
		Scalability	1		
Communication (n=7)	Messaging	Support for messaging			1
	Record exchange	Support for record exchange			6
Privacy and security (n=15)	Privacy and confidentiality	Support for privacy and confidentiality		3	
	Consent	Support for consent		4	
	Access control	Support for access control		4	
	Data integrity	Support for data integrity		1	
	Auditability of access	Support for auditability of access		3	
Medico-legal (n=20)	Support for legal requirements	Support for legal requirements	2		
	Actors	Attestation of entries	2		
		Author responsibility	2		
		Clinician identification	1	1	
		Patient identification	1		
		Subject of healthcare	1		
		User Identification	2		
	Clinical competence/governance	Support for clinical competence/governance		1	
	Faithfulness	Support for faithfulness	2		
	Preservation of context	Support for preservation of context	2		
	Permanence	Support for permanence	1		
	Version control	Support for version control		2	
Ethical (n=1)	Support for ethical justification	Support for ethical justification			1
Consume/cultural (n=4)	Consumer issues	Support for consumer issues			3
	Cultural issues	Support for cultural issues			1
Evolution (n=3)	EHR architecture and EHR system evolution	Support for EHR architecture and EHR system evolution		3	

Two computers were used as testing machines. For Linux based applications a compute with Pentium IV 2.4 Mhz. processor, 500MB RAM, and GNU Debian 4.0r3 Linux Distribution was used. Applications that run under Windows operative system were tested in a computer with Core Duo 2.1 Mhz. Processor, 2G RAM and Windows OS.

Web applications were implemented on Linux, accordingly with the recommendation of the software developers and available documentation, and tested in both machines using Internet Explorer and Mozilla Firefox respectively. The selection of the twelve alternatives was made considering that the project provides software and source code under an open-source licence (GPL, LGPL, Academic Free Licence (AFL), Mozilla Public Licence (MPL), or Eclipse Public License (EPL), has been developed to manage information regarding the health status of a subject of care, and has demonstrated the capability of managing clinical data.

As a starting point the data obtained was organized in order to explore the environment context of each of the analysed alternatives. The first step was the elaboration of a classification table associating each of the 124 requirements contained in the ISO/TS 18308 within one of the three contexts that describe the environment of an integrated EHR system (Table 5.1). Finally, each requirement was classified in one of the three environmental contexts as it was described in Figure 5.1. According to this categorization, a total of 64 requirements were classified as minimally functional, 44 as fully functional and 16 as provider enterprise.

The analysis of the result was conducted considering two methods that reflect the approach used to collect the data and facilitate the interpretation of the results obtained. First, an initial analysis was done considering both dimensions separately. Even though the initial analysis does not combine both dimensions, it provides a comparative view of the environmental context of each application as well as the families of requirements in which each FOSS project has concentrated their development efforts. Meanwhile, the cross analysis combines both dimensions to provide a comprehensive and integral analysis of the level of accomplishment for each alternative within each environmental context. The environmental context classified each one of the requirement within three classifications. Minimal functional requirements will include the core requirement of an electronic health system environment, e.g. the storage and management of medical records. Fully functional include high level requirements, e.g. management of aggregated information, system security, etc. Provider Enterprise includes additional requirements at the business and interconnection level, e.g. billing, provision of aggregated information for research and governmental requirements, etc.



Sources: - ISO/TC 215 (2005). ISO/TR 20515 Health Informatics - Electronic Health Records - Definition, scope and context (pp. 20-21)
- Beale, T. (2001). Health information system Manifesto (pp. 3-7)

Figure 5.1: Health Information System Environment

5.1.1 Contextual Analysis

Table 5.2 presents the assessment of the twelve alternatives based on the environmental classification of requirements. The average evaluation for minimal functional (MF) requirements showed that in average 42 of the 64 (65.6%) requirements were present. For fully functional (FF) and provider enterprise (PE) the averages were 16 (36.4%) and 4 (25%) requirements have been incorporated respectively. This result implies that in general the analysed FOSS EHR projects have concentrated their development efforts in the core functional features of EHR systems. Exceptions to these results are the alternatives A02 (MF=77.8%, FF=40.9% and PE=53.1%) and alternative A10 (MF=81.7%, FF=54.5% and PE=71.9%) that not only emphasised the development on minimally functional requirements, but also presented a relevant incorporation of fully functional and provider enterprise functionalities in comparison to the remaining analysed software. The alternative A12 has 52.3 (83.3%) minimally functional requirements implemented, which was the highest value obtained at this context. It also has accomplished 24 (47.7%) requirements at the fully functional context, which is the second highest value. However at the provided enterprise context it only accomplished 5 of the 17 requirements (31%).

This results show that in general the applications have a minimum of one requirement implemented at any contextual level with the exception of alternative A11. Even though, alternatives A02 and A10 are the only ones that had reached several requirements at the provider enterprise level.

Table 5.2: List of Analysed FOSS alternatives: Contextual environments

Alternative	Licence	Platform	Minimally Functional (MF) (n=64)	Fully Functional (FF) (n=44)	Provider Enterprise (n=16)	Total (n=124)
A01	GPL	Cross-platform	30.9	10	1	41.9
A02	GPL	Windows OS	49.8	18	8.5	76.3
A03	GPL	Windows OS	37.5	14	3	54.5
A04	GPL	Cross-platform	43.2	14	1	58.2
A05	GPL	Cross-platform	48.8	20	3.5	72.3
A06	GPL	Cross-platform	32.8	15	2	49.8
A07	LGPL	Windows OS	39.3	17	2	58.3
A08	EPL	Cross-platform	30.3	11	2	43.3
A09	GPL	Cross-platform	43.3	17	1	61.3
A10	GPL	Cross-platform	52.3	24	11.5	87.8
A11	EPL	Cross-platform	44.3	14	0	58.3
A12	GPL	Linux	53.3	21	5	79.3
Average			42	16	4	61.6

Software analized : CHITS, Cottege Med, Elexi, FreeMED, GNUmed, MedClipse, MirrorMed, OpenEMR, OpenMRS, OSCAR, PatientOS and Tolven.

5.1.2 Functional Analysis

The next step of the analysis was focused on the level of accomplishment of the systems according to requirements defined in the ISO/TS 18308. The data collected was organized according to the families of requirements and analysed alternatives. The data was aggregated to provide an overview of the development level reached by each alternative considering each family of requirements. Table 5.3 shows the summary of the results after all 12 FOSS were tested.

The results show that the central focus of open-source EHR projects have been the implementation of structural (29.5 of 50), procedural (14.4 of 24) and medico-legal (11.2 of 20) requirements. Meanwhile communication, evolution, consumer/cultural issues and privacy and security have presented a limited or null coverage, and ethical issues have not been considered at all. Again, alternatives A02, A10 and A12 show a harmonically distributed development for each group or requirements.

Table 5.3: List of Analysed FOSS alternatives: Functional requirements

	Structure (n=50)	Process (n=24)	Communication (n=7)	Privacy and security (n=15)	Medico-legal (n=20)	Ethical (n=1)	Consumer/ cultural (n=4)	Evolution (n=3)	Total
A01	23.6	4.3	1	2	9	0	0	2	41.9
A02	35.8	17	4.5	4	12	0	2	1	76.3
A03	31.5	15	1	0	5	0	0	2	54.5
A04	32.2	10	0	4	10	0	0	2	58.2
A05	34.8	15	2.5	5	13	0	0	2	72.3
A06	19.8	14	0	2	12	0	0	2	49.8
A07	26.3	16	0	4	12	0	0	0	58.3
A08	23.3	14	0	0	6	0	0	0	43.3
A09	26.3	15	0	4	13	0	0	3	61.3
A10	37.3	19	5.5	8	15	0	3	0	87.8
A11	30.3	15	0	3	10	0	0	0	58.3
A12	33.3	18	4	7	17	0	0	0	79.3
AVG	29.5	14.4	1.5	3.4	11.2	0	0.4	1.2	61.6

The alternatives A02 (76.3), A05 (72.3), A10 (87.8) and A12 (79.3) present the highest level of accomplishment of the 12 analysed software. However, all of the analysed software have a limited level of development in two key families of requirements, communication and privacy/security. In fact, communication (messaging and records exchange) has an average accomplishment of 1.5 (21.1%). The FOSS presented a relative limited level of development of requirement regarding security and privacy (22.6%).

5.1.3 Selected Alternatives

After the analysis of each of the FOSS EHR systems, alternatives A10 and A12 were selected from the list of the analysed software. The selected software has been utilized for the purpose of implementing the prototype interface. The selection was based on the fact that both electronic health record systems have been built with HL7 support at the application level as well as the data level

which eliminates the need to implement a HL7 module for each application or modified the data repository to accommodate HL7 messages. In addition, both are web oriented application, which is ideal for testing with platform independence. This allows focusing in the functionality of the prototype, which is the scope of this research, rather than the portability of the application. Finally, both alternatives scored high level of accomplishment in each of the contextual classifications. This also implies that no modifications of the selected software will be needed, except for the inclusion of a user interface that allows access to the functionalities provided by the prototype.

Considering that the scope of the implementation is a prototype, which has been used to evaluate functionality and performance, alternatives A10 and A12 offered the best environments for implementing and testing based on in the previous mentioned elements. However, since the prototype has been designed as an independent piece of software, it would be possible to be modified to perform with other EHR systems.

5.2 Implementation of the Prototype

After selecting the electronic health records, the software architecture proposed was implemented using a prototype approach. The purpose of the prototype is to have an implementation of the proposed solution capable of performing the key functionalities described in Chapter 4 and, at the same time, evaluate its viability using a simulated scenario. The implementation and testing of the prototype version would provide a validation of the proposed solution and give an answer to points 4 and 6 of the research approach described in Chapter 1.

5.2.1 Implementation

The prototype was designed to be platform independent and was built using Java language for the main components and PHP scripting language for the web interface, the same language used in the implementation of the selected electronic health records systems. The message request database, which contains the sets of tables that storage the messages request and times logs, was implemented using MySQL server. Both electronic health record databases were also implemented in MySQL, accordantly to the developer specifications. Two computers were used server machines: a Linux based server and a Window based server. The selected EHR systems were installed one in each server. A prototype implementation of the interface was adapted for each EHR system.

5.2.2 Architecture

To recreate the concept of client-server architecture each one of the severs posed a role during the communication process. The electronic health record system implemented in the windows based server posed as the client (the one posting requests) whilst the other selected system installed on Linux was the server (the one accepting the request).

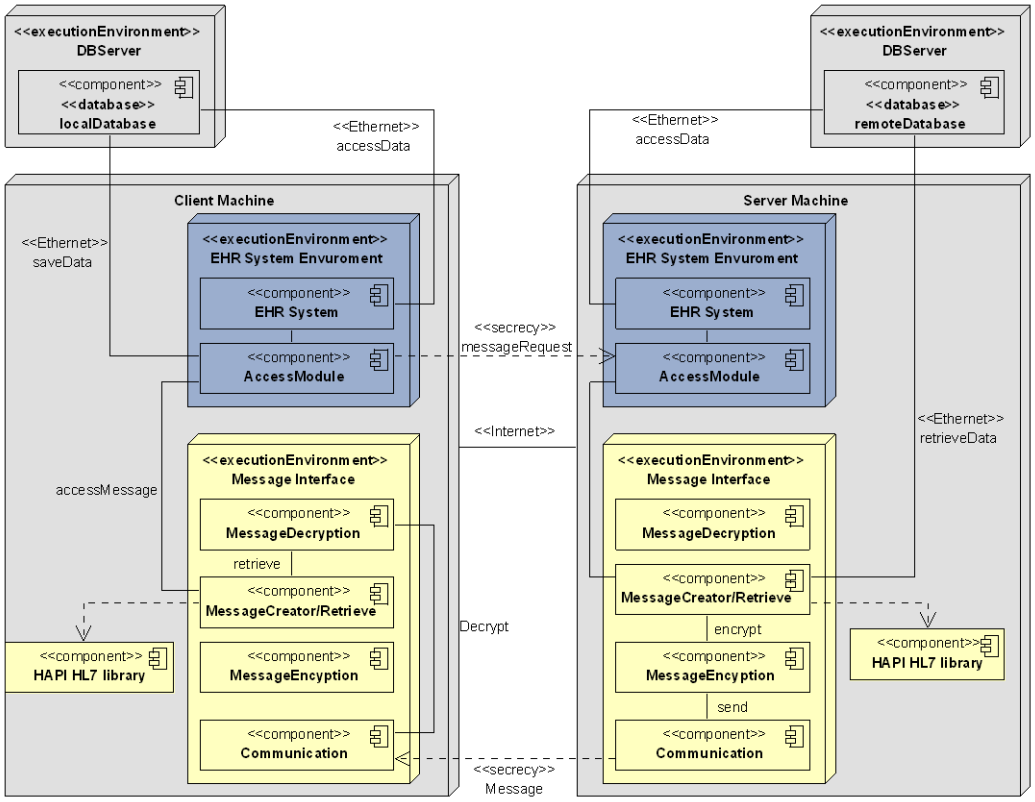


Figure 5.2: Deployment Architecture

Figure 5.2 shows the deployment architecture for the prototype. An access module has been implemented for each module. The message request is placed using a communication channel between both access modules. The server interface receives the request and creates a HL7 message by retrieving the necessary data from the database using HAPI HL7 library. After the message is created the interface will encrypt it using the attribute-based encryption module (`messageEncryption`) and send the encrypted file over the internet back to the requesting client.

At the client side, the message is received by the communication component making it available for access. The user will be able to access the encrypted message through the access module that has been incorporated to the local EHR system. The message can be retrieved and displayed to the user through the access module.

5.3 Testing

The implementation of the prototype, based on the requirements described in section 4.2.1 main functionalities, has shown that a solution for secure data exchange using attribute-based encryption is possible. However, that alone is not sufficient to determine if the proposed architecture would perform adequately in a health environment. For this reason, a set of tests based on a case were conducted. The test results have provided an understanding of the behaviour of the proposed solution and demonstrate its viability of implementation based on the architecture that has been described in section 2 of Chapter 4.

5.3.1 Test Planning

Two types of tests were performed in order to analyse the implemented prototype. A functionality test based on a case study, which is described in section 5.3.1.2 and performance tests, which are described in section 5.3.1.3.

5.3.1.1 Purpose of the tests

The goal of the testing is to evaluate the viability of implementation of the proposed software architecture. The simulated scenario will facilitate the testing of the prototype. The data collected from the simulations and tests will facilitate the functional validation of a proposal as well as analyse the performance of the modelled architecture.

5.3.1.2 Test Design

As it was explained previously, the tests have been based on a case study that simulates the scenario in which a patient care is assessed in a shared care environment. The setting and description of the case study will be described in this section.

5.3.1.2.1 Setting the Case Study

Let us consider that Hospitals 'HA', 'HB' and Clinic 'CL' have previously agreed in a set of principles that allow them the exchange of information. Those principles have been set on contracts that permit the transference of any relevant data regarding health history, which can be required during the treatment of a patient. All institutions have defined independent security approaches and mechanism for protecting the information that is managed on their system, 'HA' and 'HB' being public hospitals and according to the health policy guidelines for a public hospital, 'CL', being a General Practice, following the guideline for security from the General Practice Computing Group. Therefore, there could be differences in access control, security and information release polices. To avoid controversies policy reinforcing method is used during the exchange and release of information. The method proposed is reinforcing security policies by using an attribute-based encryption scheme. In this case, the access policies are used to encrypt the information that has been exchanged, allowing only users with the correct access privileges to decrypt and access the information.

5.3.1.2.2 Case Study for Enforcing of Access Control Using Policies

The scenario described in this section is used as case study in analysis of the proposed solution. Figure 5.3 shows a graphical representation of the relation and flow of information of the actors historically involved in the treatment of patient 'A' described in Figure 5.2.

The paradigm used presents difficulties that arise in providing health care in today's interconnected medical environments. These difficulties require efficient access control mechanisms in order to ensure, for example, in the used paradigm that only doctor 'DC' who has the patient's consent accesses the patient's medical data. Traditional access control models try to cope with these kinds of difficulties giving access to a patient's EHR only to the rightful owner.

> **Case**: 68 years old lady 'A' was admitted to the hospital 'HA' with abdominal pain and doctor 'DC' has been assigned to her case. The patient has indicated having a history of chronic diseases. 'A' has been previously hospitalized at hospital 'HB' for chest pain and followed up treatment with the cardiologist 'C' for Atrial Fibrillation, Hypertension and Recurrent Angina, also radiological information of the patient are maintain in the hospital records. Additionally, she has been diagnosed with diabetes for 20 years and has been visiting clinic 'CL' for her regular medical treatment. She has checked her blood according to the doctor's order at the local pathology 'P' regularly. 'A' has also been seen by the Dietitian 'D', Ophthalmologist 'O', podiatrist 'PO', Exercise Physician 'EX' for her diabetes and diabetes related complications. She visited

gynecologist 'G' for postmenopausal symptoms 2 years back and had an episode of knee pain 3 weeks ago having taken an x'ray at the Radiology 'R'. She is on several medications for different conditions. As an elderly lady with multiple pathologies, the doctor 'DC' has decided to trace back her history from her healthcare providers. The patient has also given consent for the doctor to do that.

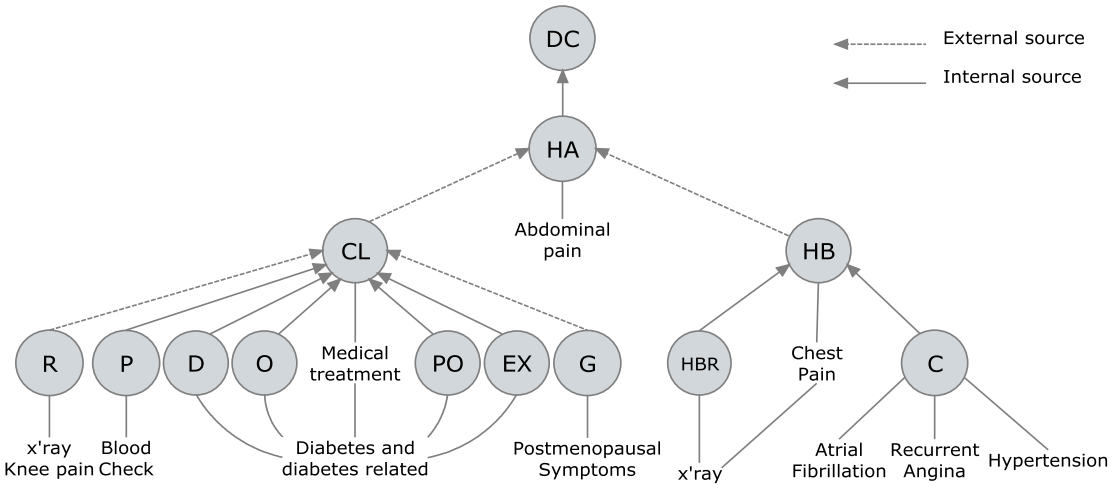


Figure 5.3: Case analysis, interaction and expected flow of information

5.3.1.2.3 Scenarios

5.3.1.2.3.1 Information Exchange

After patient A is admitted to hospital 'HA' and her first encounter with physician 'DC', doctor 'DC' starts collecting patient 'A' historical medical data. The collection starts with the remote request of data from clinic 'CL' and hospital 'HB' health information systems. To guarantee the confidentiality of the information, the data is encrypted using attributes associated to physician 'DC'. Since the transference of data is done by reinforcing access policies only doctor 'DC' will initially be authorized to decrypt the data provided by clinic 'CL' and hospital 'HB'. Considering that patient 'A' will not only be treated by physician 'DC' but

also by a team of physicians and medical staff, the access permissions will eventually be modified in order to provide access to all personnel involved in with patient's 'A' care. This can be done by providing a secret Key to each member of the staff assuming responsibility with patient's 'A' care; each member will be allowed to retrieve the information depending on the described access policies described by the attributes associated to their secret keys. For example, physician treating patient 'A' will have access to all relevant medical history of the patient, on the contrary nurses and administrative staff would be provided with restricted access to the data.

5.3.1.2.3.2 Analysis

This case presents a normal encounter patient-physician in which the historical information of patient A can only access by the primary physician at hospital 'HA', Doctor 'DC'. To simplify the analysis let us assume that the consent policy has been created during the first encounter (steps 1 and 2 in Figure 5.6). As it has been described previously, the policy defines a set of attributes that establishes who would be able to access the medical information of patient A. In this case a set of attributes *({Pat.A},{D.GP, Clinic.CL})* is used to describe the access permission to patient A's information.

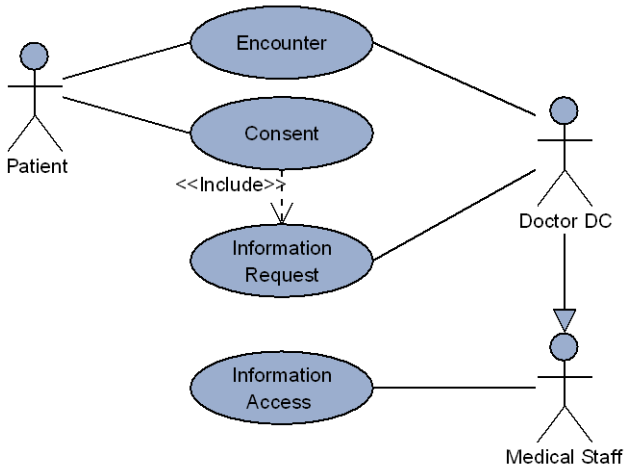


Figure 5.4: Case use Scenario 1

Even though the patient has moved through the health system, the information gathered from the counter, encounters and reports can be shared using electronic communications. An information request made by doctor DC would start the process as is shown in steps 3 and 4 of Figure 5.6. he information contended in the EHRs of hospital 'HB' and clinic 'CL' can be encrypted using the attributes *({Pat.A},{ D.DC, Depto.ME, Hosp.HA })* and send directly to the electronic health record system in the hospital A, which is shown steps 5 and 6 of Figure 5.6. In this case, the access policy for the data is described as $M_{(data)}$= *(Pat.A)* $\vee$ *(D.DC* $\wedge$ *Depto.ME* $\wedge$ *Hosp.HA).* Since patient cannot possess a secret key that includes the attributes *{D.DC, Depto.ME, Hosp.HA }* the access tree has the outcomes described in Figure 5.5.

In this scenario, the transference of information is directly managed between sender ('HB' and 'CL' information systems) and receiver (Doctor 'DC'). Since the information is shared between organizations the attribute

{*D.DC,Depto.ME,H.HA*} is applied to encrypt the relevant medical information associated to patient A, and then sent to the HA's information system.

$$M_{(data)} = (Pat.A) \vee (D.DC \wedge Depto.ME \wedge Hosp.HA)$$

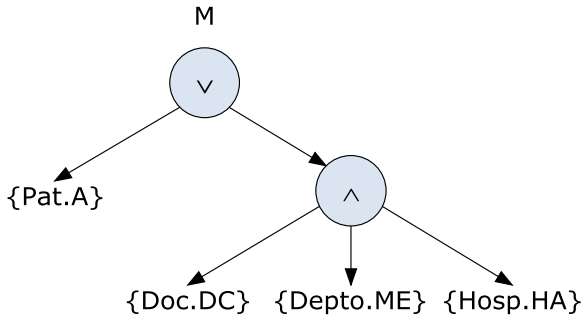


Figure 5.5: Access tree Patient's Data

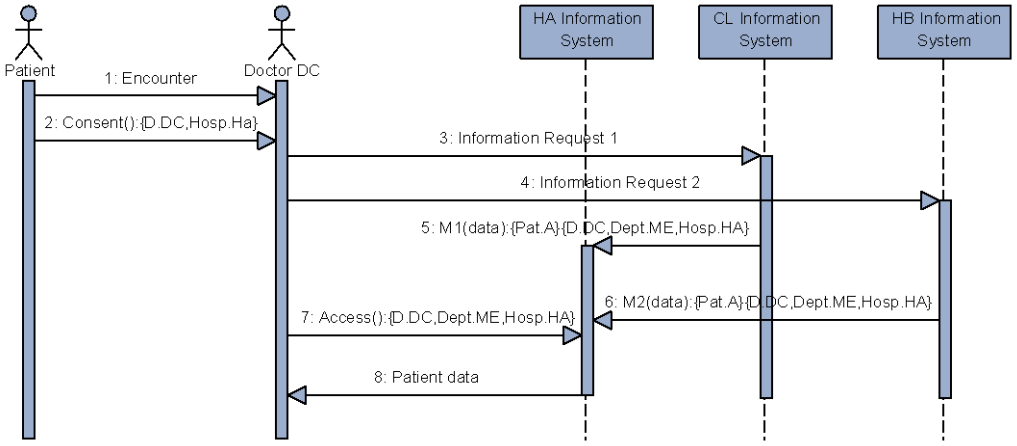


Figure 5.6: Sequence Diagram Scenario 1

The information collected and sent directly to the 'HA' systems, can be accessed by 'DC', as it is show in steps 7 and 8 of Figure 5.6. At this point, the transferred data has been protected using an enforced access policy approach; therefore, the information can only be accessed by Doctor 'DC'. To provide access to other members of the staff access permissions can be modified by associating the new access key to the encrypted data. For example, by allowing Cardiology 'CA-A' to

have access the patient medical history. This delegation of access to specific users is possible because attribute-based encryption supports partial delegation of access permissions. To enforce that only 'CA-A' is able to access the data the information the following attributes will be incorporated to the access permissions ({ *D.DC, Depto.ME*}).

5.3.1.2.4 Access Delegation and Patient Control over Data Access

Now consider the situation presented in role definition. According to the access and security policies of hospital 'HA' only member of the team attending the patient can have access to his EHRs. Since originally the information was requested and collected by doctor 'DC' of the Medicine Department the data could be encrypted using the following attribute set $M_{(data)}$= *(Pat.A)* $\vee$ *(D.DC*$\wedge$ *Depto.ME)*. However, to allow other physician access to patients 'A' data, a new set of attributes need to be incorporated. In this case, physicians could be provided with secret key and assume specific responsibilities, which are described by a specific set of attributes (policies). Additionally, information could be restricted in some specific cases, which can be described by a specific set of attributes (policies). Each specialist will be able to decrypt the data, which is under his responsibility, but will not be able to decrypt the data that has been restricted. This provides a solution for restricting access only to members of the team treating the patient and to patient's control over access permissions. This last point will be discussed in more detail in Chapter 6.

5.3.1.2.4.1 Analysis

Initially only doctor 'DC' has access to the patient information. To allow access to cardiologists 'CA-A' and 'CA-B' a new set attribute can be added to the access

policy of patient 'A', the new set will incorporate attribute sets associated to 'CA-'A'. Since cardiologists 'CA-A' and 'CA-B' works the Cardiology department of hospital 'HA', the new set of attributes would be $M_{(data)}$= *(Pat.A)* ∨ *(H.HA* ∧ *((D.DC*∧*Depto.ME)* ∨*(Depto.CAR*∧ *(D.CA-A*∨ *D.CA-B)))).* No other cardiologist will have the attributes {*D.CA-B, Depto.CAR, H.HA* } {*D.CA-A ,Depto.CAR, H.HA*} associated to their access privileges, therefore no one else but 'CA-A' and 'CA-B' will be allowed to access and manipulate patients 'A' data. The new access tree has the following outcomes:

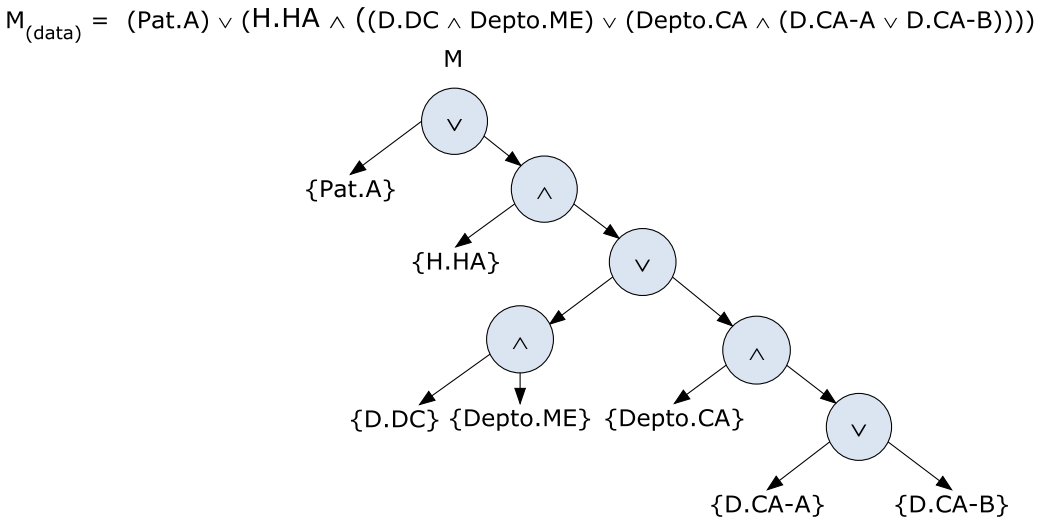


Figure 5.7: Access tree considering access to cardiologists CA-A and CA-B

When patient 'A' provides consent to Doctor 'DC' to collect his historical medical information, she could state that only physician involved in his case would have access to his psychiatric history, denying access to other physicians and personnel of hospital 'HA'. In this case, the access Key of other physicians and personal will not allow them to access to the psychiatric history of patient 'A'. The access to the information is stated according to the consent of the patient and the access

policies. The access then will incorporate the restrictions over information access, making some of the information unable to access for other physicians even when they could have access to the patient's EHR. This will be described and discussed in Chapter 6.

5.3.1.3 Performance Testing and Analysis

Once the initial test conducted to determine the viability of implementing the proposed solution were finished, a set at performance tests were executed. The specification of the performance tests as well as their result will be presented in this section. Two types of tests were performed, general test in which random messages were created and then encrypted under a predefined set of attributes and a specific test in which in which given a defined message this was encrypted using a different set of attributes.

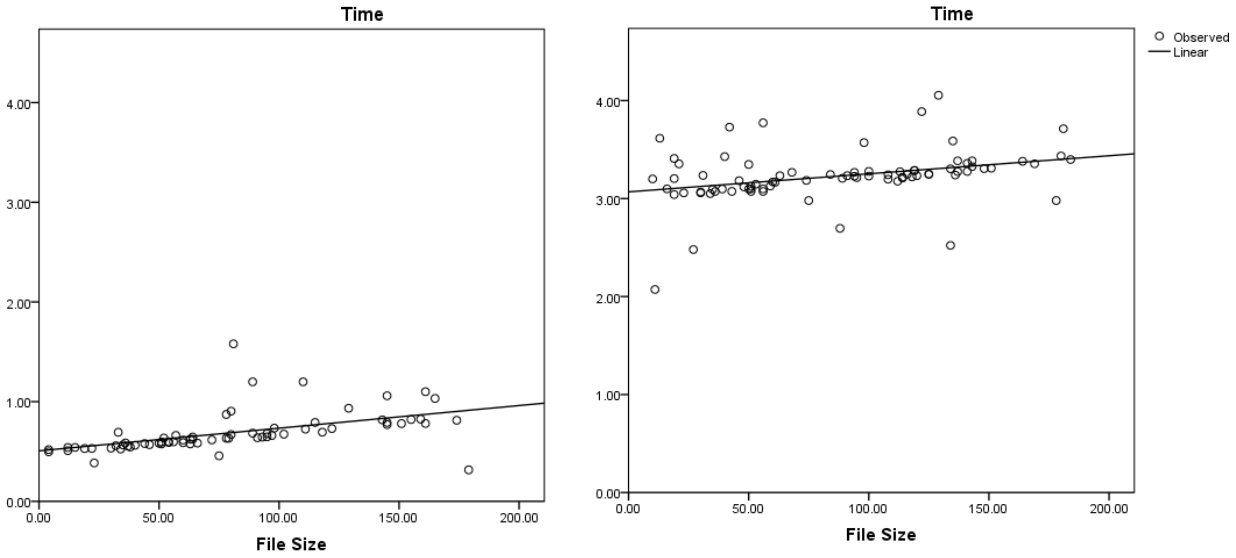
5.3.1.3.1 General Testing and Analysis

The initial set of tests considered the two scenarios described previously and execute the application against a set of predefined message requests. In this section, both the description of the experiments and the results are analysed and discussed.

5.3.1.3.2 Time for File Generation and Encryption

To perform the testing of the interface, the two previously described cases were implemented against a dataset of 300 message requests. The messages requested were executed remotely, alternative A10 served as the requesting application meanwhile alternative A12 as a remote data repository. Each one of the message requests was associated to a specific patient's record within the electronic

repository and randomly to one of the 25 possible messages implemented for the prototype. Each message was created using the existing data of a patient and the encryption was performed using one of the two access trees previously described. The analysis considers the total time required to create and encrypt the message. As it was explained in Chapter 4, the encryption algorithm requires the message *m* and a set of attributes (polices) *Ap*. Therefore, it is assumed that the total time required for the process will depend of the length of the file and the number of attributes used as access structure.



(a) Sample of time required by four attribute encryption

(b) Sample of time required by seven attribute encryption

Figure 5.8: Processing time

Figure 5.8 shows the set of data obtained from the simulation. Two different sets of data are displayer under different time ranges. The first set of data shows a time with a range of 1.26 that goes from 0.32 to 1.58 seconds. The second set of data is display with a range of 1.98 that goes from 2.7 to 4.05 seconds. The time deference between both data sets is explained mainly by the number of attributes

used during the encryption process. In fact, the original size of the file has a limited incidence in the total processing time in comparison of the number of attributes used in the encryption. In the simulation, the data processed under 1.58 seconds was encrypted using a four attribute tree. On the contrary, the second set of data was encrypted using a seven attribute tree.

Let us consider both cases in more detail. Total time required for message creation and data encryption using a four attribute has an average time of 0.68 seconds. On the other hand, the time required to create and encrypt the message seven attributes have an average of 3.22. The flatness of the respective fitting regression lines show that the size (length) of the file would have a relatively reduced effect in the total processing time. In the same way, the time required to process and creates the message has an average time of 0.076 seconds and with a standard deviation of 0.11. Which implies that the total amount of time required to process a message request will be mainly affected by the number of attributes (polices) included during the encryption of the file. This will be analysed in more detail in section 5.3.1.4.

5.3.1.3.3 Size of the File

The size of the encrypted file is proportional to size of the original file. Furthermore, as it is expected, the size of the encrypted file will be also affected by the number of attributes used to encrypt the data. In the Figure 5.9 the set of observations below the line correspond to the size of the files that have been encrypted using 4 attributes. Meanwhile, the data set shown over the line correspond to the size of the files encrypted using a 7 attribute set.

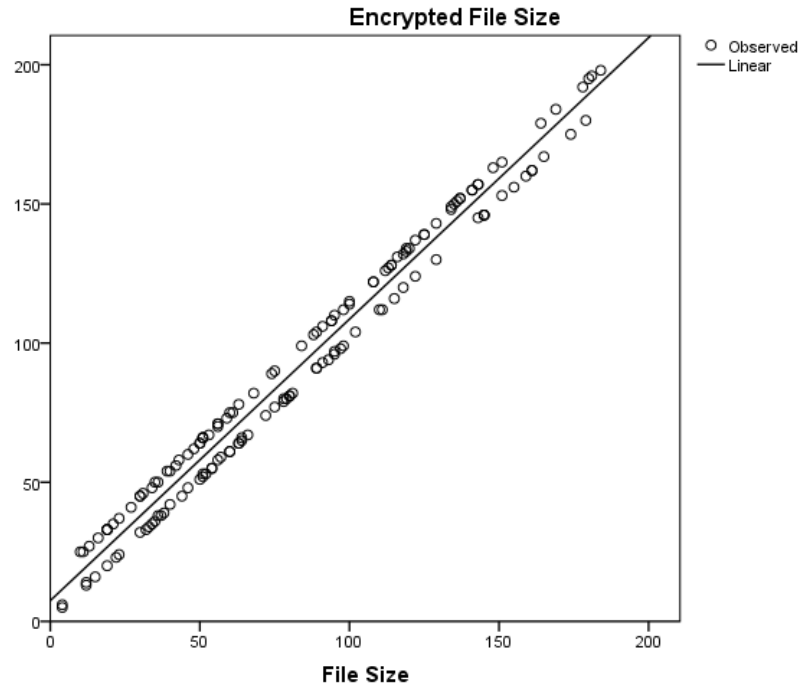


Figure 5.9: File size

5.3.1.4 Specific Testing and Analysis

The second set of test was conducted considering a single message tested against several set of attributes during the encryption process. The target of this test is the analysis of performance. The description of the tests as well as their results are presented and analysed in this section.

5.3.1.4.1 Encryption Time

A simulation experiment was performed to analyse the performance of the interface for encrypting data using a different set of attributes. The experiment considered a message encrypted using a different set of attributes. This setting facilitates the analysis of performance when comparing data encryption using a different number of attributes to encrypt a given file.

The performance of the interface in terms of a number of attributes used during the encryption process can be observed Figure 5.10. As it is expected, the number of attributes (nodes) used to encrypt the data would have a direct effect in the overall processing time. The growth of the curve varies accordantly with the numbers of nodes (attributes) used. Between 1 and 6 tributes the average time is 1.16 seconds with a range between 0.55 and 1.9 seconds. When more than 8 attributes are used the time was increased over 5 seconds. In fact, the processing time in the range of 8 and 33 attributes showed a decreasing growth with an average of 6.55 seconds of processing time and a range that goes from 5.23 seconds to 8.08 seconds. In the range of 34 to 57 attributes, the data shows an increasing growth with an average of 8.48 second and a range between 6.83 and 10.41 seconds. The final set of data also shows an increase in processing time of almost 7 seconds of average difference from the previous data set. In fact, the average time required to process the file is 14.77 seconds with a range between 13.8 and 15.8 seconds.

This corresponds to a nonlinear behaviour associated to time processing. It also indicates that a major number of attributes will require an increasing processing time which is an important antecedent for a full implementation of the proposed solution. This defers from the testing data obtained by Bethencourt in (Bethencourt, et al., 2007) in where the time of encryption optimised is lineal. This difference can be explained by data which is not included in Bethencourt such has time required to place the request, generate the HL7 message and deliver the message.

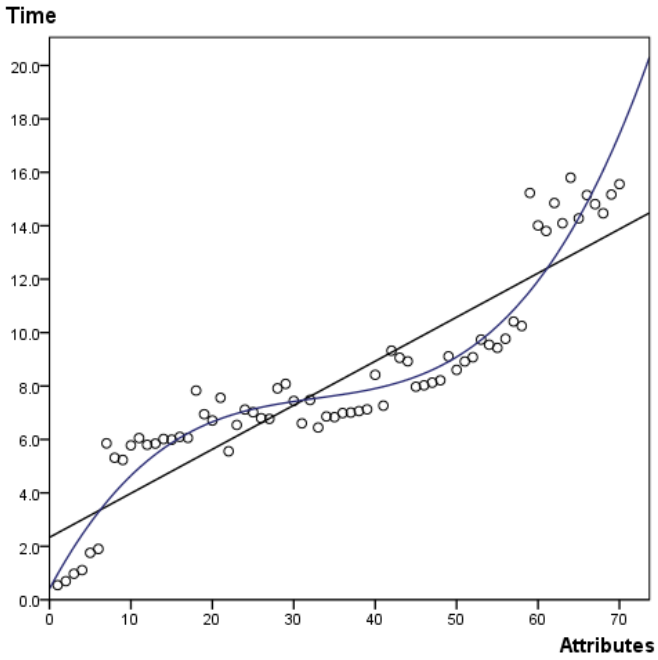


Figure 5.10: Interface performance accordantly to the number of attributes

5.3.1.4.2 File Size

Assuming the same approach as the previous section, in here the variation of the size of the file will be analysed. The size of the encrypted file follows a nonlinear increased depending on the number of attributes used to encrypt the data (see Figure 5.11). Between 1 and 6 attributes the size of the file presents an average increase of 6.3% over the size of the original file. Similar to the time analysis the data shows an initial increase in the file size and then a decreasing growth after the attribute number seven has been included. In fact, between 7 and 33 attributes the average increase of the file size is 9.6% with a range between the 7% and the 12%. After the attribute 34 is included the data set shows an increasing growth which is stopped at attribute 58. In this range, the average increase of the files is 13.98% with a range that goes between 12% and 16%. Finally, a new increase in

file size is shown after attribute 59 is included. The average increase at this point is 22.78% with a range between 22 and 23%.

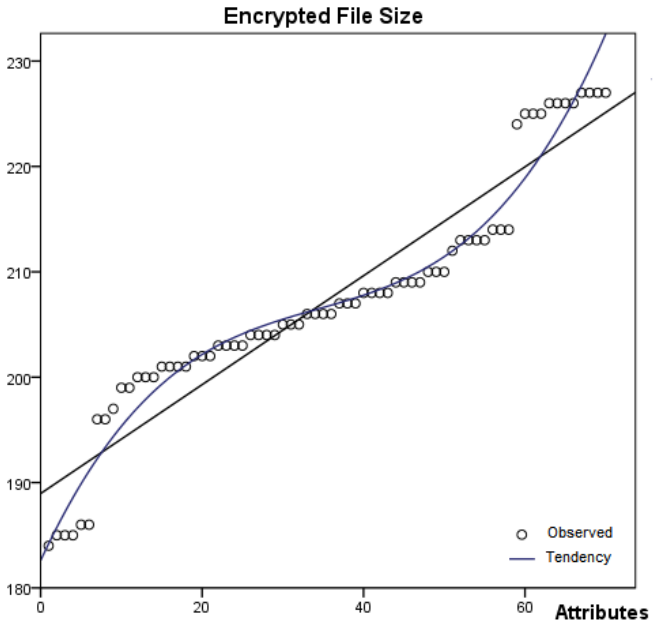


Figure 5.11: Variation of the file size

5.4 Chapter Summary

In this Chapter, the implementation and testing of a prototype system interface was presented and described. First, the process of selection of an open source electronic health record system that is used to implement the proposed solution was presented. The selected system not only provides the software infrastructure required to test the proposed solution but also a data repository that is used to generate a set of standardized messages. The messages generated from the data repositories are later used during the analysis of performance of the prototype.

Section 5.3.1.2.2 provides a case study that is used for empirically testing the proposed solution. The set of scenarios has been developed in order to evaluate

the performance of a prototype based on the proposed solution. Finally, section 5.3.1.3 provides an analysis of performance of the proposed architecture. The analysis is based on a set of random experiments using existing data from the selected electronic health record systems.

The implementation of the prototype, the functionality and performance tests and analysis of the results has shown that a software interface based on the architecture presented in Chapter 4 is a solution to protect patient information in a shared care environment. From the functionally perspective, the prototype has demonstrated to be capable of processing an information request, creating a standard HL7 message, encrypting the information accordantly to a set of predefined policies (attributes) and replay an encrypted message. In the same way, the application has proved to be able to detect an authorized user and provide access to the encrypted data or deny access if the user does not possess the necessary credential to decrypt the file containing the information.

From the point of view of performance, the application has performed within expected parameters. Time and file size will be affected by the number of attributes use during the encryption and the amount of data collected and included in the HL7 message. As it was presented before, the differences in execution time are mainly explained by the number of attributes rather than the extension of the original file.

The next Chapter a real case study will be presented and used to empirically analyse the proposed solution. This case will provide a scenario in which the proposed solution will be analysed considering a real situation.

Chapter 6

Case Study Discussion

The exercise of analysing the flow of information in a shared care environment provides an understanding of the ethical and legal implication of sharing medical information among the medical staff. As it was discussed in Chapter 2, in a shared care environment the protection of a patient's confidentiality is a responsibility shared within the team of specialists providing care to a patient. However, when multiple health care units are involved in the treatment of a patient, the management of confidentiality becomes more complex. Even when specific normative is in place, the implementation of different approaches, the consideration of existing regulations and current technologies to access information make difficult to provide a clear mechanism for the protection of information.

To analyse this situation a real case study is presented, described and discussed in this Chapter. The proposed solution will be contrasted and empirically analysed

with this case in order to provide a technological solution to the issues that will be exposed.

6.1 KJ v Wentworth Area Health Service

6.1.1 Overview

The medico-legal implications of using multidisciplinary approach in providing health services as well as sharing medical information have been discussed in Chapter 2. In the case of a shared care environment, the ethical and legal responsibility of protecting the confidentiality of the patient is extended to all members involved in the care of an individual. In Australia this responsibility is initially regulated by The National Privacy Principles (NPPs) contained in the Privacy & Personal Information Protection Act 1998 (PPIPA, 2009). The NPPs provide a regulatory framework for the management of personal information in the public and private sectors. Even though the NPPs are not specifically defined for the protection of privacy in the health care, they provide a guidance for the management of information contended within medical records.

The Health Records and Information Privacy Act 2002 of New South Wales was fully operational by September 2004. This normative regulates the collection and handling of patients' health information by New South Wales public and private health sectors. The Act can be applied to health providers or to other organizations that collects, maintain or use health information for primary and secondary purposes (HHP, 2005).

Even though the case that will be studied in this chapter occurred before the NSW Health Records and Information Privacy Act 2002 was fully operational, the

consideration of the perspective given by both the National Privacy & Personal Information Protection Act and the NSW Health Records Act provide a more compelling understanding of how the proposed solution may perform in real situation.

6.1.2 Setting the Case Study

The requirement of obtaining informed consent for maintaining and disclosing medical related information is embodied within the public policies, medical standards and current legislation. Informed consent has both an ethical and a legal dimension. Ethically, it is recognized the right that individuals have to decide which course of action health professionals may follow in order to provide care services or the way in which the medical information collected when providing health services will be used. Legally, health professionals have the responsibility to storage and process the personal data in a fashion in which the confidentiality of the information is guarantee at any given time (Clark & Findlay, 2005). In Australia, this has been enforced not only by the directives of regulatory policies but also by the law. In general, informed consent may fall into two categories:

1. Consent for treatment, which involves the informed consent in the application of a course of action in a treatment in which a patient is involved, including medical benefits or others relevant issues.
2. Consent for use of personal information, which include the disclosure of sensitive information which has been obtained during the provision of medical care. In this case, and according to the type of consent provided by the patient, the disclosure of the information could be for primary or secondary purposes.

In the case that will be described the effected argued that her sensitive information was collected, stored and released without the proper consent to members of a multidisciplinary health team.

6.1.3 The Case Study

6.1.3.1 Background

In 2004, the NSW Administrative Decision Tribunal informed its decision in the case of KJ versus The Wentworth Area Health Service. This decision was ruled in concordance with the events occurred in the period in which KJ was been treated for cancer in the Wentworth Area Health Service.

KJ was referred by her practitioner to the Nepean Cancer Care Centre (NCCC), a unit of the Nepean Hospital in the Wentworth Area Health Service. In there, she was treated for cancer between the years 2000 and 2003. During this period she also consulted the units of psychology and psychiatry. In both cases notes were placed in her general medical records. The general medical file was available to all members of the medical team treating her. Furthermore, there was also evidence that access to the general medical record was also granted to two physicians external to the Nepean Hospital (NSWADT, 2004).

6.1.3.2 Issues

6.1.3.3 Collected Information

In the year 2003 KJ complained to the Wentworth Area Health Service. In her presentation KJ argued that she was not informed of any record been created nor that the psychological information has been placed on her general medical file

where it could be accessed by medical staff of the hospital. She was also not informed that her medical records would be sent to physician outside the hospital, including not only members of the medical staff treating her but also other members of the organization. She argued that those actions were in violation of the principle 10 of the Privacy & Personal Information Protection Act 1998, which indicates the obligation that organizations have to inform individuals the purpose for which information has been collected and to whom the information will be provided to (PPIPA, 2009).

6.1.3.4 Disclosure of Personal Information

KJ argued that the placement of the psychological information in her general medical record and further disclosure to two external physicians (her general practitioner and surgeon) was a breach of section 19 of the Privacy & Personal Information Protection Act 1998. In fact, the tribunal ruled that not only the disclosure to the external physicians but also the placement of this sensitive information on her personal file was in violation of the Act, since it is plausible to consider that the exchange of information between units constitute disclosure. In fact, the existence of such records implies that not only physicians but nurses and other medical and administrative staff could eventually have access to KJ's sensitive information.

6.1.3.5 Consent to Disclosure Information

KJ submitted that the patient registration form was not adequate for obtaining informed consent form individuals, especially considering a shared care

environment in which a multidisciplinary team was involved in her treatment. She argued that it was not required to provide access to the psychological information to members of the treating team. And that in any case the disclosure of the psychological information should only occur with the express consent of the patient.

6.1.4 Implication for the Health Records and Information Privacy Act 2002

The concepts of share care and multidisciplinary team are not fully incorporated neither by the National Privacy & Personal Information Protection Act 1998 nor by the NSW Health Records and Information Privacy Act 2002. For this reason, the KJ versus Wentworth Area Health Service case provides an interesting example especially in terms of informed consent and correct disclosure of medical information under a multidisciplinary health team. In fact, under the principle 4 NSW Health Records and Information Privacy Act, the disclosure of health information to a multidisciplinary team would be permitted; nevertheless organizations would still be compelled to provide information regarding the use and disclosure of the information to patients (HRIPNSW, 2002).

For that reason, it has been suggested that health organization should develop management tools which allow, on one hand, a better provision of information to specific patients and provide, on the other hand, education about the use of information in a multidisciplinary team (Connolly, 2004). From a security point of view, the implementation of security mechanisms that allow the protection of privacy but at the same time ensuring the flow of information during the treatment of a patient in a shared environment is also needed. In the following section this

case will be used to analyse the proposed solution and determine how it may perform in a real situation.

6.2 Analysis of the Case

Figure 6.1 provides an overview of the flow of information in the KJ versus Wentworth Area Health Service case. In here, the reference to the general practitioner (GP) to the Nepean Cancer Care Centre (NCCC) is represented by the segmented arrow. In the same way, the red segmented line represents the argued incorrect handle of KJ's psychological information which is made available not only to the hospital medical stuff but also was delivered to KJ's general practitioner (GP) and her surgeon (S).

In the figure it can also be observed including KJ's psychological information within the general medical file makes this information available to other health care units (HCU) of the hospital. Without the existence of an appropriated and secure health information system, KJ's general medical records could have been released to anyone with access to the information including other physicians , nurses or medical personnel.

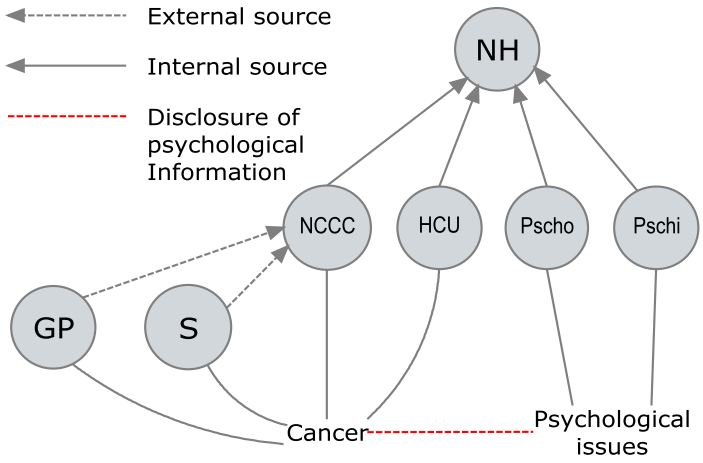


Figure 6.1: Case analysis, interaction and expected flow of information KJ v Wentworth Area Health Service

6.2.1 Enforcing Access Policies

Let us assume that in the KJ versus Wentworth Area Health Service case KJ has provided her informed consent for the collection and handle of her medical records in both cancer related data and psychological information. Let us also assume that regulatory policies for collection, management and disclosure have been implemented as well as information exchange agreements have been signed among the health units of the Wentworth Area Health Service. Finally, let us assume a health information system which contains the electronic health records of KJ is actually in use.

Under those conditions, medical and psychological information should be maintained within her electronic health records. The collected information will be used for the purpose for which KJ has provided consent. This assumption provides a solution of the initial issue of the KJ versus Wentworth Area Health Service case which is out of the scope of this research. It is also understood that

the instrument used to obtain the informed consent of KJ has been adequately designed in order to guarantee the correct interpretation by the patient, which solve the third issue discussed in the KJ versus Wentworth Area Health Service case and which also is out of the scope of this research.

Finally, access to the information will be managed considering the consent provided by KJ. Therefore, access to the information will be provided accordantly to KJ consent and the access policies put in place by the Wentworth Area Health Service in order to guaranty the patient's confidentiality. This is the main issue which concerns this research.

6.2.1.1 Sharing the Information within the Health Team

In order to simplify the analysis, the health information that has been collected from KJ will be divided into cancer and psychological related data. Following KJ's argument regarding appropriate consent, cancer related information would be available to be accessed by the medical staff of the NCCC, KJ's general practitioner and her surgeon. At the same time, her psychological information will be only available by the psychology and psychiatry departments of the Nepean Hospital. Other members of the medical staff would have limited or null access to her electronic health records. Nonetheless, psychological information could be disclosed to other medical staff, such as members of the NCCC treating KJ, her medical practitioner or her surgeon, only upon providing the required consent.

It is assumed that KJ's medical information has been stored in the Nepean Hospital's local electronic health record system, and that the secure access to the

information will be provided by an attribute-based encryption infrastructure. As it was discussed in Chapter 4, attribute-based encryption provides a flexible tool to manage access policies to the information in scenarios such as the previously described. In fact, the shared information can be encrypted using a multi-level access hierarchy accordantly what is required.

6.2.1.2 Access Tree

Let us assume that all the information contained by KJ's electronic health record can be described by $R_{KJ} = R_{KJ(c)} \wedge R_{KJ(p)}$ in which $R_{KJ(c)}$ represents KJ's cancer related information and $R_{KJ(c)}$ corresponds to KJ's psychological information.

As it was discussed previously, the medical personnel allowed to have access to KJ's cancer related information would be NCCC medical staff involve in KJ's case (P), KJ's general practitioner and KJ;s surgeon. Therefore, this information could be encrypted using the attributes *({Pat.KJ},{Depto.NCCC,Hosp.NH},{D.P}, {D.GP },{D.S})*. In this case, the access policy for the data is described by $R_{(kg(c))}$= *(Pat.KJ)* $\wedge$ *((D.GP)*$\vee$ *(D.S)* $\vee$ *(D.P* $\wedge$ *(Depto.NCCC* $\wedge$ *Hosp.NH))*. Since the patient cannot have a secret key that includes *({Depto.NCCC,Hosp.NH},{D.P}, {D.GP },{D.S})* the access tree has only the outcomes described in Figure 6.2.

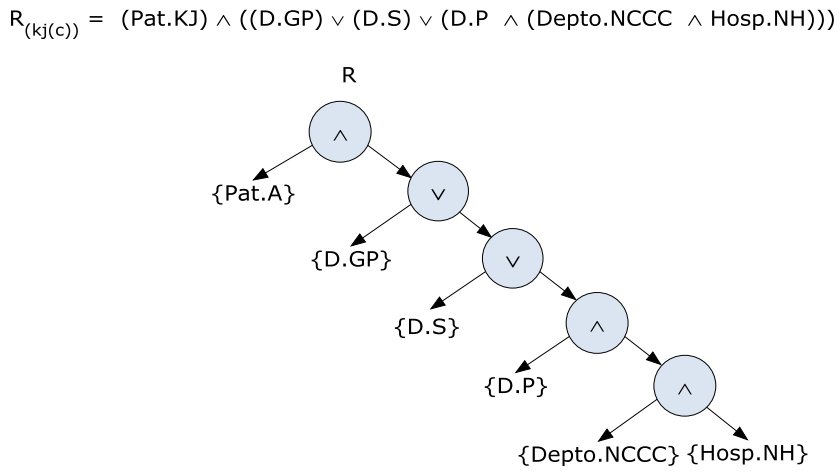


Figure 6.2: Access tree considering access to KJ's cancer related information

In the case of the psychological information, it can be encrypted using the attributes *({Pat.KJ},{Depto.Psycho, Depto.Psychi, Hosp.NH }*. Therefore, the access policy for the data is described as $R_{(kg(p))}$= *(Pat.KJ) ∧ ((Hosp.NH ∧ ((Depto.Psycho)∨ (Depto.Psychi)))*. Since the patient cannot possess a secret key that includes *{Depto.Psycho, Depto.Psychi, Hosp.NH }* the access tree has only the outcomes described in Figure 6.3.

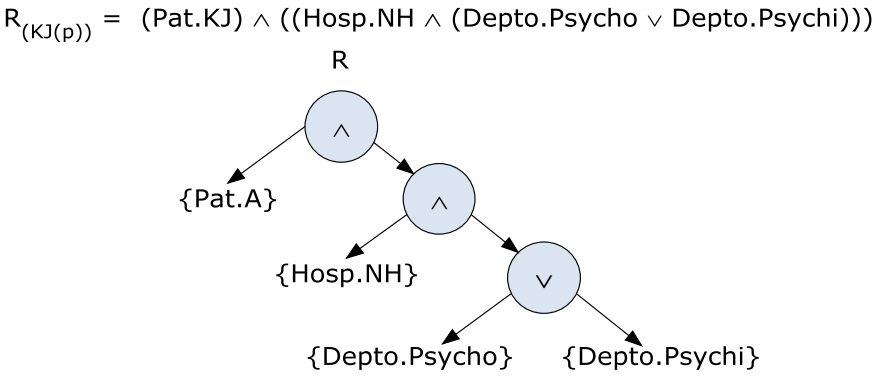


Figure 6.3: Access tree considering access to KJ's psychological related information

As it has been described, attribute-based encryption provides a suitable solution for the issue of disclosure of sensitive information in the case of KJ versus

Wentworth Area Health Service. This solution is flexible enough to guarantee that only authorized user will be able to access specific contents of KJ's electronic health records.

For example, Let us assume that nurses of NCCC have been granted access to KJ's medical records, in this case the access tree will include new attributes to represent this situation as is *({Pat.KJ},{Depto.NCCC,Hosp.NH},{nurse}, {D.P},{D.GP },{D.S}).* In this case, the access policy for the data is described by $R_{(kg(c))}$= *(Pat.KJ) ∧ ((D.GP)∨ (D.S) ∨ ((DP ∨ nurse) ∧ (Depto.NCCC ∧ Hosp.NH)))*

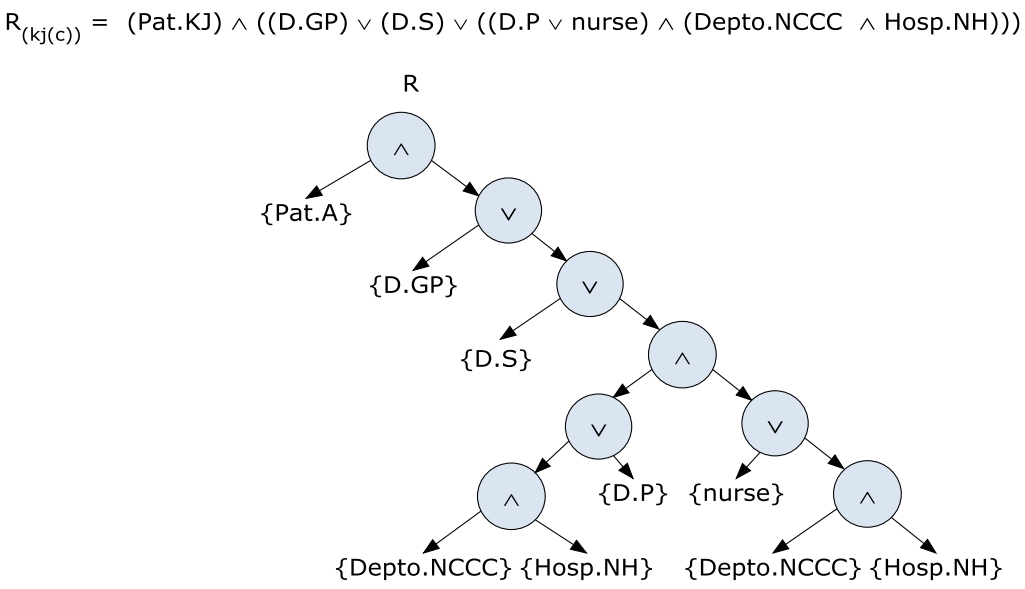


Figure 6.4: Access tree considering access to KJ's cancer related information including nurses

In the same way, if access to the physiological information is granted to KJ's general practitioner the access police will include the attributes *({Pat.KJ},{D,GP}{Depto.Psycho, Depto.Psychi, Hosp.NH }.* Therefore, the access

policy for the data is described as $R_{(kg(p))}$= *(Pat.KJ)* ∧ *(D.GP*∨ *(Hosp.NH* ∧ *((Depto.Psycho)*∨*(Depto.Psychi))).*

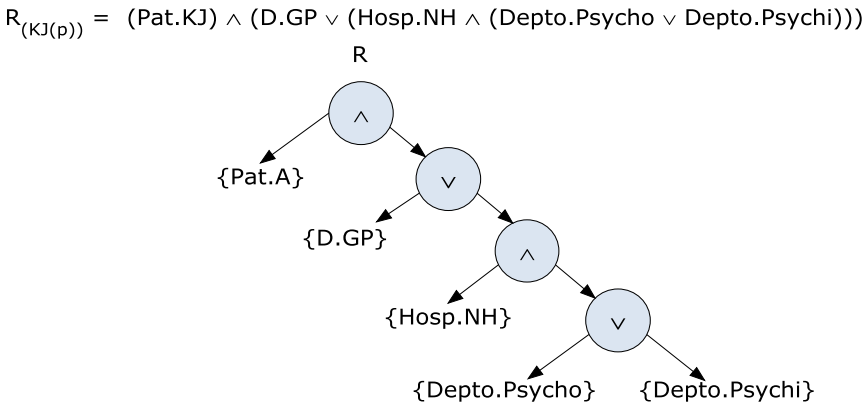


Figure 6.5: Access tree considering access to KJ's psychological related information including KJ's General Practitioner

6.3 Chapter Summary

The KJ versus Wentworth Area Health Service case has provided a situation in which the actual technology does not provide a clear solution. Specially, considering a shared care environment in which a multidisciplinary team of experts responsible of providing health care to a patient. Team work in health care as become a generally accepted practice which the actual legislation has not been able to completely cope. For these reason providing a solution for data sharing in a multidisciplinary environment become a relevant task.

In the KJ versus Wentworth Area Health Service case,the ability of restricting access to specific information is essential to provide a suitable technological

solution . As it has been shown in this Chapter, attribute-based encryption facilitates such possibility by allowing the encryption of the data according to a set of attributes (policies) within different access levels. In fact, attribute-based encryption permits the implementation of flexible access policies that not only guarantee the protection of patient privacy but also allows the flow of information within the health care team treating the patient.

Chapter 7

Conclusion

This research has been oriented to the analysis of security issues associated with the exchange and release of electronic health records in interconnected healthcare environments. More specifically, the present work has been focused on providing an answer to the research question introduced in Chapter 1: "*how could the secure exchange and release of electronic health records be supported by incorporating security services in a shared care environment?*"

This chapter provides a summary of the contents presented and discussed through this thesis. As a starting point, a summary of the main aspects are discussed and key issues regarding the principal topic of the research as well as the proposed solution are presented. It will be also discussed how the proposed approach provides a fitting solution for protecting the confidentiality of the exchange medical data. Finally, further research directions in the topic of security and privacy are presented and discussed based on the findings of this research.

7.1 Summary and Research Results

Electronic health record systems have become a crucial part of modern and interoperable health information systems. One of the key functionalities of EHR systems is their ability to provide reliable information to support the delivery of health care services. Nevertheless, the high sensitivity of the data and the level of accessibility maintained by EHRs raise concerns over the secure access and release of information, especially in shared care environments. Protection of patients' confidentiality in a shared care environment is the main point of interest that was introduced in the research question and discussed from different perspectives through this thesis. The approach followed to provide an answer to the research question has considered several stages that will now be discussed.

1. **Conduct a literature review of the topics associated with the studied domain.**

The first step of the research was the study of the topics associated to the studied domain. For this reason, concepts such as health information systems and electronic health record system were researched. The study of health information systems and their impact in healthcare and future tendencies, allows us to understand the magnitude in which these technologies may affect individuals and health organizations. The review of these concepts has covered the definition, purposes and dimensions of health information system and electronic health record systems. The discussion also included aspects regarding communication, interoperability, security, privacy and confidentiality of patients' medical data.

The protection of patients' confidentiality has been the central point of discussion through the thesis. The preservation of confidentiality over medical data has become a concern not only for patients but also for physicians and other stakeholders of the healthcare industry, especially considering the enormous amount of sensitive data stored and accessed by health information systems. Security issues associated to interoperable electronic health records systems in a shared care environment have been one of the topics of discussion of this research. For this reason, the legal, ethical and personal perspectives regarding the access and release of medical records as well as an analysis of information and security requirements for data exchange have been presented and discussed through Chapter 2.

Shared care has been introduced as a model of service that is driving the healthcare industry. This new paradigm is characterized for a gradual change of the traditional approach of provision of health services, which is characterized by the continuous incorporation of new information and communication technologies, the specialization of health services and an increasing mobility of patients. Conceptually, shared care is the modality in which the care of a patient is managed by several actors within the health care system. In fact, the administration of care is provided by a multidisciplinary team which include the participation of professional within an organization or the incorporation of external specialists and healthcare units. From the point of view of information management, shared care involves the capability in which information can be fiscally and electronically accessed and exchanged among all participants in the attention of a specific case.

How it has been discussed in Chapter 3, in a shared care environment, information regarding a subject of care should be available for all actors involved in his/her treatment. But at the same time, the shared data should be protected against any unauthorized access and release. For this reason, access to information should be granted under the principles of relevance and "need-to-know". The principle of relevance indicates that the amount of information available to be accessed should be the required by a user to perform an action. The principle of "need-to-know" implies, on one hand, that only authorized personal should have access to the information and, on the other hand, that the level of access that a user has over the electronic health records will depend on the permission provided to the user over the data. These principles are disused in more detail in section 2.2.

An important element for consideration is the capability that health information systems have for exchanging information through the health system. Health information standards are the key elements to allow such functionalities. A discussion of the technical aspects regarding communication and interoperability of electronic health records systems has been presented in section 2.4.1.

Finally, traditional as well as other techniques for authentication and access control used by modern health information systems, such as passwords, PIN and biometric technology, have been researched and discussed. A comparative analysis of security approaches, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) and extended Access control models (the three Level Access Security Model, Contextual Role-Based Access Control Model and Situation Role-Based Access

Control Model), has concluded that, even when all technological approaches can be applied to provide different levels of security over sensitive medical data, there still exist limitations to be overcome, especially considering shared care environments. At the application level, the main security issue presented in approaches based on MAC and DAC are inflexibility of the policies, complexity in determining the ownership of the information, difficulty for implementing in large shared care environments and restrictions considering delegation and hierarchical access permissions to the data, which is fundamental to provide different levels of access to the medical personnel responsible for providing care to a patient. Implementation based on RBAC models present security issues associated to the ambiguities that exist in the definition of roles and access privileges among organizations, the non-existence of a common and/or standardized framework for defining roles and access privileges and lack the ability of fine-grained access to information. Extensions to RBAC have allowed the fine-grained definition of access rights to data but at the same time increased the complexity of the models. The discussed approaches have failed to provide suitable solutions for exchange of date in scenarios that involve more than one health care provider.

2. To define and provide a proposal for secure exchange of electronic health record.

The research question pointed through the secure exchange and release of electronic health records supported by the incorporation of security mechanisms. As a result, a conceptual approach for access control policies using an attribute-based encryption scheme is developed and presented in Chapter 4. Attribute-based encryption allows the encryption and decryption of data based on polices, which

are represented as attributes associated to the information. Polices are used to reinforce restrictions over the encrypted data. In fact, attribute-based encryption allows the encryption and decryption of data based on policies, which are represented as attributes associated to the information. The approach allows an independent but secure method to protect the privacy and confidentiality of a patient's information transmitted over insecure channels. The model is flexible in providing access to multiple users based on security policies, which are represented as attributes that describe the access permissions over encrypted data. The use of an attribute-based encryption scheme allows:

- Control over access permissions of transmitted data: only user with the private access key that satisfy the encryption protocol will be able to decrypt the exchange information.
- Delegation of access permission: Access to information can be delegated or granted to other users by providing an access key which satisfies the encryption protocols.
- Protection of the patient's data: the transmitted information is encrypted in a fashion in which only users with the appropriate key will be able to decrypt the information. In addition, data can only be accessed when a user possesses the appropriate access permissions, and information is provided considering the principles of need-to-know and relevance.
- Hierarchical access to rumpled data: User can access the complete information or part of it, depending on the attribute set associated to the private key.

The conceptual definition, general requirements, flow of information, the state machine and other artefacts for the implementation of the proposed approach are discussed in detail in Chapter 4.

3. **Analyse a set of Open-Source EHR systems in order to select suitable software that will be used during the analysis of the case study.**

To proceed with the implementation of prototype two opens-source health information systems were selected. The selection of the software was based on an overview of the actual level of development of the Open EHR systems according to definitions and requirements provided by international standards. The goal of the analysis was the examination of the systems to determine how their functionalities and architectures conciliate with international standards. To reach that goal several open EHRs under the public licence schemes were investigated and assessed. From the analysis, two open source software were selected and then used during the implementation of the prototype. The selected applications not only provided the system infrastructure required for implementing the proposed solution but also the data structures and information repositories needed to generate standardized messages. The evaluation and selection of the open electronic health records are presented in section 5.1.

4. **Modify the selected software by incorporating a prototype version of the proposed security solution.**

A prototype version of the proposed conceptual specification was implemented with the purpose of analysing how it may perform in a simulated situation. The prototype was developed to be a platform independent solution and implemented using Java language. The software was designed as a communication interface

which considered three modules: HL7 message generation, security and communication. The implementation was done using open source libraries for the message creation module as well as the security module. The interface was incorporated to the two open-source electronic health record systems selected with that purpose. The description of the implementation of a prototype version is discussed in Chapter 5.

5. **Define case studies in which the solution will be analysed and tested.**

In order to analyse the behaviour the prototype a case study was introduced. The case study considered a complex environment and a single case from which several scenarios have been derived to discuss different topics through the thesis. The case study is introduced and described in Chapter 5. The testing of the prototype based on the proposed scenarios, has demonstrated the viability of the solution.

A real case was introduced in chapter 6 with the purpose of empirically analysing the proposed solution. The KJ versus Wentworth Area Health Service case has provided a valuable scenario in which the proposed specification can be analysed. In fact, how it has been discussed, implementing attribute-based encryption would allow overcoming the issue of correct disclosure of personal information in a multidisciplinary team that has been introduced by this case.

6. **Run simulations and test the prototype based on the case study. The data collected by these simulations and tests will facilitate the validation of a proposal for secure exchange and release of electronic health records.**

Finally, an analysis of performance of the proposed architecture was provided. The analysis has been based on a set of random experiments using existing data stored in the selected electronic health record systems. As it was expected, the main element that affects the total processing time is the security module. In fact, the number of attributes used to encrypt the data will reflect in the time required to generate an encrypted message.

In conclusion, implementation and testing of the prototype had shown that attribute-based encryption offers several security advantages over traditional methods and also can be used for different purposes. In fact, it provides a flexible access control mechanism that can be implemented under dissimilar circumstances.

7.2 Future Research Directions

The author presented a solution for secure exchange and release of electronic health records. The proposed architecture considers a security module which incorporates an attributes-based encryption scheme. A prototype version of the architecture was implemented and tested. The testing was limited to functionality and performance of the implementation. Future work will be to build a fully functional version of the software and proceed with the quality assurance process. The final result should provide a suitable, flexible and scalable solution for complex health care environments.

Another point to be considered for further research is the alternative applications of attribute-based encryption. The solution proposed in this thesis uses polices represented as attributes that determine the access permissions over an encrypted

data. However, as it was discussed on section 4.2.4.1 the error-tolerance of attribute-based encryption schemes allow the implementation of fuzzy encryption schemes for biometric authentication technology. Fuzzy attribute-based encryption biometric authentication technology offers several security advantages over traditional methods and also can be used for different purposes. These advantages are discussed in section 4.2.4.1. Future work in this area would be to explore and provide a viable scheme for fuzzy attribute-based encryption using biometric technology.

Bibliography

Agrawal, R., & Johnson, C. (2007). Securing electronic health records without impeding the flow of information. *International Journal of Medical Informatics, 76* (5-6), 471-479.

Ahn, C., Nah, Y., Park, S., & Kim, J. (2001). An Integrated Medical Information System Using XML. In W. K. e. al. (Ed.), *Human Society Internet* (pp. 307-322). Berlin Heidelberg: Springer-Verlag.

Alexander, M. J. (1974). *Information System Analysis: Theory and Applications*. Chicago: Science Research Associates.

Alhaqbani, B., & Fidge, C. (2007, September 24). *Access Control Requirements for Processing Electronic Health Records.* Paper presented at the Business Process Management Workshops BPM 2007, International Workshops, Brisbane, Australia.

Ammenwertha, E., Brender, J., Nykänen, P., Prokosch, H.-U., Rigby, M., & Talmon, J. (2004). Visions and strategies to improve evaluation of health information systems Reflections and lessons based on the HIS-EVAL workshop in Innsbruck. *International Journal of Medical Informatics, 73*(6), 479-491.

Anderson, J. G. (2007). Social, Ethical and Legal Barriers to E-health. *International Journal of Medical Informatics, 76*(5-6), 480-483.

Arlow, J., & Neustadt, I. (2005). *UML 2 and the Unified Process: Practical Object-Oriented Analysis and Design* (2 ed.). Massachusetts: Addison-Wesley.

Atkins, W. (2000). A bill of health for biometrics? *Biometric Technology Today, 8*(9), 8-11.

Au, M., Huang, Q., Liu, J., Susilo, W., Wong, D., & Yang, G. (2008). Traceable and Retrievable Identity-Based Encryption *Applied Cryptography and Network Security* (pp. 94-110). Berlin/Heidelberg: Springer.

Bakker, A. (2004). Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. *International Journal of Medical Informatics, 73*(3), 267-270.

Beeler, G. W. (1998). HL7 Version 3 - an object-oriented methodology for collaborative standards development. *International Journal of Medical Informatics, 48*(2), 151-161.

Berler, A., Pavlopoulos, S., & Koutsouris, D. (2004). *Design of an interoperability framework in a regional healthcare system.* Paper presented at the 26th Annual International Conference of the IEEE EMBS, San Francisco, CA, USA.

Berner, E. (2008). Ethical and Legal Issues in the Use of Health Information Technology to Improve Patient Safety. *HEC Forum, 20*(3), 243-258.

Bethencourt, J., Sahai, A., & Waters, B. (2007). *Ciphertext-Policy Attribute-Based Encryption.* Paper presented at the Security and Privacy, 2007. SP '07. IEEE Symposium on.

Bicer, V., Laleci, G. B., Dogac, A., & Kabak, Y. (2005). Artemis Message Exchange Framework: Semantic Interoperability of Exchanged Messages in the Healthcare Domain. *SIGMOD Record, 34*(3), 71-76.

Bilykh, I., Jahnke, J. H., McCallum, G., & Price, M. (2006, 22-23 June 2006). *Using the Clinical Document Architecture as Open Data Exchange Format for Interfacing EMRs with Clinical Decision Support Systems.* Paper presented at the 19th IEEE International Symposium on Computer-Based Medical Systems.

Blobel, B. (2000). Application of the component paradigm for analysis and design of advanced health system architectures. *International Journal of Medical Informatics, 60*(3), 281-301.

Blobel, B. (2004). Authorisation and access control for electronic health record systems. *International Journal of Medical Informatics, 73*(3), 251-257.

Blobel, B. (2006a). Advanced and secure architectural EHR approaches. *International Journal of Medical Informatics, 75*(3-4), 185-190.

Blobel, B. (2006b). Advanced and Secure Architecture EHR Approaches. *International Journal of Medical Information, 75*(3-4), 185-190.

Blobel, B. (2007). Comparing approaches for advanced e-health security infrastructures. *International Journal of Medical Informatics, 76*(5-6), 442-448.

Blobel, B., Nordberg, R., Davis, J. M., & Pharow, P. (2006). Modelling privilege management and access control. *International Journal of Medical Informatics, 75*(8), 597-623.

Blobel, B., & Roger-France, F. (2001). A systematic approach for analysis and design of secure health information systems. *International Journal of Medical Informatics, 62*(1), 51-78.

Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing *Advances in Cryptology — CRYPTO 2001* (pp. 213-229). Berlin/Heidelberg: Springer.

Brandt, M. (2000). Health Informatics Standards: A User's Guide. *Journal of the American Health Information Management Association, 71*(4), 39-43.

Burstein, F. (2002). System development in information system research. In K. Williamson (Ed.), *Research methods for students, academics and professionals: information management* (2 ed., pp. 147-157). Wagga Wagga: Centre for Information Studies.

Burstein, F., & Gregor, S. (1999). *The Systems Development or Engineering Approach to Research in Information Systems: An Action Research Perspective*. Paper presented at the Proc. 10th Australasian Conference on Information Systems. Retrieved 20 January, 2010, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.3.5361&rep=rep1&type=pdf

CEN-ENV (2000a). *Health informatics - Security for healthcare communication - Part 1: Concepts and terminology. Published Standard CEN ENV 13608-1:2000*: European Committee for Standardization.

CEN-ENV (2000b). *Health informatics - Security for healthcare communication - Part 2: Secure data objects. Published Standard CEN ENV 13608-2:2000*: European Committee for Standardization.

CEN-ENV (2000c). *Health informatics - Security for healthcare communication - Part 3: Secure data channels. Published Standard CEN ENV 13608-3:2000*: European Committee for Standardization.

Chen, Y.-C., Chen, L.-K., Tsai, M.-D., Chiu, H.-C., Chiu, J.-S., & Chong, C.-F. (2008). Fingerprint verification on medical image reporting system. *Computer Methods and Programs in Biomedicine, 89*(3), 282-288.

Cheow, M. F., & Win, K. T. (2007). Personal Health Records and Healthcare Systems. *International Journal of Healthcare and Management, 8*(3-4), 209.

Choe, J., & Yoo, S. K. (2008). Web-based secure access from multiple patient repositories. *International Journal of Medical Informatics, 77*(4), 242-248.

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules. *Journal of Medical Systems, 30*(1), 57-64.

Clark, A. M., & Findlay, I. N. (2005). Attaining adequate consent for the use of electronic patient records: An opt-out strategy to reconcile individuals' rights and public benefit. *Public Health, 119*(11), 1003-1010.

Coiera, E. (2003). *A guide to health informatics* (2nd ed.). London: Arnold.

ComLaw (2006). *Private Sector Information Sheet 1A – National Privacy Principles* from http://www.comlaw.gov.au/.

Connolly, C. (2004, January 2004). Managing patient consent in a multidisciplinary team environment – KJ v Wentworth Area Health

Service and its implications for HRIPA. *Privacy Law and Policy Reporter* Retrieved 20 October, 2010, from http://www.austlii.edu.au/au/journals/PLPR/2004/26.html

Conrick, M. (2006). IT and Information Management. In M. Conrick (Ed.), *Health Informatics: Transforming Healthcare with Technology*. Melbourne: Thomson Social Science Press.

Conrick, M., & Newell, C. (2006). Issues of Ethics and Law. In M. Conrick (Ed.), *Health Informatics: Transforming Healthcare with Technology*. Melbourne: Thomson Social Science Press.

Coonan, K. (2004). Medical informatics standards applicable to Emergency Department Information Systems: Making sense of the Jumble. *Academic Emergency Medicine, 11*(11), 1198-1205.

Danko, A., Kennedy, R., Haskell, R., Androwich, I. M., Button, P., Correia, C. M., et al. (2003). Modeling nursing interventions in the act class of HL7 RIM Version 3. *Journal of Biomedical Informatics, 36*(4-5), 294-303.

Delac, K., & Grgic, M. (2004). *A Survey of Biometric Recognition Methods*. Paper presented at the 46th International Symposium Electronic in Marine. ELMAR 2004.

Dogac, A., Laleci, G. B., Kirbas, S., Kabak, Y., Sinir, S. S., Yildiz, A., et al. (2006). Artemis: Deploying semantically enriched Web services in the healthcare domain. *Journal of Information System, 31* (4-5), 321-339.

Dolin, R., Alchuler, L., Boyer, S., Beebe, C., Behlen, F., Biron, P., et al. (2006). HL7 Clinical Document Architecture, Release 2. *Journal of the American Informatics Association, 13*(1).

Eddy, A. (2000). A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of the Health Insurance Privacy and Accountability Act of 1996. *Annals of health law, 9*, 1-72.

Engelbrecht, R., Ingenerf, J., & Reiner, J. (2006). Relevance of Terminological Standards and Services in Telemedicine. In K. Zielinski, M. Duplaga & Ingram (Eds.), *Information Technology Solutions for Healthcare*. London: Springer-Verlag.

Englebardt, S., & Nelson, R. (2002). *Health Care Informatics: An Interdisciplinary Approach*. St. Louis: Mosby.

Fernandez, E., & Sorgente, T. (2005). *An analysis of modeling flaws in HL7 and JAHIS*. Paper presented at the ACM Symposium on Applied Computing.

Ferraiolo, D., & Kuhn, R. (1992). *Role-Based Access Control.* Paper presented at the 15th National Computer Security Conference, Balmy, Baltimore, USA.

Field, M. G. (1973). The Concept of the "Health System" at the Macrosociological Level. *Social Science and Medicine, 7*(10), 762-785.

Flores Zuniga, A., Win, K., & Susilo, W. (2009). Biometrics for Electronic Health Records. *Journal of Medical Systems*. Retrieved from http://dx.doi.org/10.1007/s10916-009-9313-6

Garson, K., & Adams, C. (2008, March 4-6). *Security and privacy system architecture for an e-hospital environment.* Paper presented at the Proceedings of the 7th symposium on Identity and trust on the Internet, Gaithersburg, Maryland.

Gates, M. A. (2007). Biometrics - Passing on Using Passwords. *Radiology Today, 8*(17), 28-31

Goldschmidt, P. G. (2005). HIT and MIS: implications of health information technology and medical information systems. *Communications of the ACM, 48*(10), 68 - 74.

Grain, H. (2006). Consumer issues in Informatics. In M. Conrick (Ed.), *Health Informatics: Transforming Healthcare with Technology*. Melbourne: Thomson Social Science Press.

Grimson, J. (2001). Delivering the electronic healthcare record for the 21st century. *International Journal of Medical Informatics, 64*(2-3), 111-127.

Gritzalis, D., & Lambrinoudakis, C. (2004). A security architecture for interconnecting health information systems. *International Journal of Medical Informatics, 73*(3), 305-309.

Guo, J., Takada, A., Tanaka, K., Niu, T., He, M., Sato, J., et al. (2005). Enhancement of MML Medical Data Exchange Standard for a localized Chinese Version. *Journal of Medical System, 29*(5), 555-567.

Guo, J., Takada, A., Tanaka, K., Sato, J., Suzuki, M., Suzuki, T., et al. (2004). The development of a MML(Medical Markup Language) Version 3.0 as a medical Document Exchange Format for HL7 message. *Journal of Medical Systems, 28*(6), 523-533.

Hafner, M., Memon, M., & Alam, M. (2008). Modeling and Enforcing Advanced Access Control Policies in Healthcare Systems with Sectet *Models in Software Engineering* (pp. 132-144). Berlin/Heidelberg: Springer.

Hammond, W. (1995). The status of healthcare standards in the United States. *Internationa Journal of Bio-Medica Computing, 39*(1), 87-92.

Hammond, W., & Cimino, J. (2001). Standards in Medical Informatics. In E. Shoertliffe, L. Parreault, G. Wiederhold & L. Fagan (Eds.), *Medical Informatics: Computer Applications in Health Care and Biomedicine* (pp. 212-256). New York: Springer-Verlag

Haux, R. (2006a). Health information systems - past, present, future. *International Journal of Medical Informatics, 75*(3-4), 268-281.

Haux, R. (2006b). Individualization, globalization and health - about sustainable information technologies and the aim of medical informatics. *International Journal of Medical Informatics, 75*(12), 795–808.

HealthConnect (2002). *Consent and Electronic Health Records: A disclosure paper*

Heard, S. (2006). Electronic Health Records. In M. Conrick (Ed.), *Health Informatics: Transforming Healthcare with Technology* (pp. 222-332). Melbourne: Thomson Social Science Press.

Hebda, T., Czar, P., & Mascara, C. (2005). *Handbook of Informatics for Nurses & Healthcare Professionals* (3rd ed.). New Jersey: Pearson Prentice-Hall.

Heckle, R. R., & Lutters, W. G. (2007, July 18-20). *Privacy implications for single sign-on authentication in a hospital environment.* Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania.

Heitmann, K. U. (2003). *HL7 Version 2: XML Encoding Syntax, Release 1*: ANSI/HL7.

Heitmann, K. U., Schweiger, R., & Dudeck, J. (2003). Discharge and referral data exchange using global standards - the SCIPHOX project in Germany. *International Journal of Medical Informatics, 70*(2-3), 195-203.

Henderson, M. (2003). *HL7 Messaging*. Texas: Otech Inc.

HHP (2005). *Handbook to Health Privacy - Health Records and Information Privacy Act 2002 (NSW)*. Sydney: Office of the NSW Privacy Commissioner.

Hinchley, A. (2005). *Understanding Version 3: A premier on the HL7 Version 3 Communication Standard*. Munich: Alexander Mönch Pub.

HL7 (Producer). (2006) HL7 Version 3 Interoperability Standard: Normative Edition. *Version 3 – The Foundation of Healthcare Interoperability*.

Health Records Act - Victoria (2000).

Health Records and Information Privacy Act - New South Wales (2002).

HRPAACT (1997). Health Records (Privacy and Access) Act - Australian Capital Territory.

Health Service (Conciliation and Review) Act - Western Australia (1995).

Huang, E.-W., Hsiao, S.-H., & Liou, D.-M. (2003). Design and implementation of a web-based HL7 message generation and validation system. *International Journal of Medical Informatics, 70*(1), 49-58.

IBG (2008). Biometric Basics: What are the Benefits of Biometric Technology? *International Biometric Group Reports and Research*, from http://www.biometricgroup.com/reports/public/reports_and_research.html

Ibraimi, L., Tang, Q., Hartel, P., & Jonker, W. (2009). Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes *Information Security Practice and Experience* (pp. 1-12). Berlin/Heidelberg: Springer.

ISO/IEC (Producer). (1998, 05-09-2006) ISO/IEC 10746-1: Information Technology-Open Distributed Processing-Reference Model: Overview. Available: http://isotc.iso.org/. Podcast retrieved from http://isotc.iso.org/.

ISO/TC-215 (2004). *Health informatics - Requirements for an electronic health record architecture. Published Standard ISO/TS 18308:2004*: International Organization for Standardization.

ISO/TC-215 (2005). *Health informatics - Electronic health record - Definition, scope, and context. Published Standard ISO/TR 20514:2005*: International Organization for Standardization.

Joshi, J. B. D., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security Models for Web-Based Applcations. *Communications of the ACM, 44*(2), 38-44.

Katirai, H., & Sax, U. (2005). Unlocking the Value of Clinical Information: What You Need to Do Now to Enjoy the Benefits in the Future. In K.-D. A. e. al. (Ed.), (pp. 330 – 338). Berlin Heidelberg Springer-Verlag.

Keen, P. G. W. (1987). MIS research: Current status, trends and needs. In R. A. Buckingham, R. A. Hirschheim, F. F. Land & C. J. C.J. Tully (Eds.), *Information systems education: Recommendations and implementation* (pp. 1-13). Cambridge, England: Cambridge University Press.

Kim, D.-K., Ray, I., France, R., & Li, N. (2004, March 29 - April 2). *Modeling Role-Based Access Control Using Parameterized UML Models.* Paper presented at the 7th International Conference Fundamental Approaches to Software Engineering, FASE 2004, Barcelona, Spain.

Langer, S. (2002). OpenRIMS: An Open Architecture Radiology Informatics Management System. *Journal of Digital Imaging, 15*(2), 91-97.

Lee, G., Kim, W., Kim, D.-k., & Yeh, H. (2004, July 15-17). *Effective Web-Related Resource Security Using Distributed Role Hierarchy* Paper presented at the Advances inWeb-Age Information Management 5th International Conference,WAIM 2004 Dalian, China.

Liaw, S.-T., Sulaiman, N., Pearce, C., Sims, J., Hill, K., Grain, H., et al. (2003). Falls Prevention within the Australian General Practice Data Model: Methodology, Information Model, and Terminology Issues. *Journal of the American Medical Informatics Association, 10*(5), 425-432.

Liu, S.-l., Guo, B.-a., & Zhang, Q.-s. (2009). An identity-based encryption scheme with compact ciphertexts. *Journal of Shanghai Jiaotong University (Science), 14*(1), 86-89.

Lopez, D. M., & Blobel, B. G. M. E. (2009). A development framework for semantically interoperable health information systems. *International Journal of Medical Informatics, 78*(2), 83-103.

Lusignan, S. d., Chan, T., Theadom, A., & Dhoul, N. (2007). The roles of policy and professionalism in the protection of processed clinical data: A literature review. *International Journal of Medical Informatics, 76*(4), 261-268.

Lyman, J., Boyd, J., Dalton, J., & Egybazy, C. (2003, Oct. 5-8). *Applying the HL7 reference information model to a clinical data warehouse.* Paper presented at the IEEE International Conference on Systems, Man and Cybernetics, New York.

Marcheschi, P., Mazzarisi, A., Dalmiani, S., & Benassi, A. (2004, Sept. 19-22). *HL7 clinical document architecture to share cardiological images and*

structured data in next generation infrastructure. Paper presented at the Computers in Cardiology, Chicago, Illinois.

Marohn, D. (2006). Biometrics in healthcare. *Biometric Technology Today, 14*(9), 9-11.

McDonald, C. J., Overhage, J. M., Dexter, P., Takesue, B., & Suico, J. G. (1998). What is done, what is needed and what is realistic to expect from medical informatics standards. *International Journal of Medical Informatics, 48*(1-3), 5–12.

Morrison, M. (2000). *XML Unleashed*. New York: Prentice-Hall.

Motta, G. H. M. B., & Furuie, S. S. (2003). A contextual role-based access control authorization model for electronic patient record. *Information Technology in Biomedicine, IEEE Transactions on, 7*(3), 202-207.

Müller, M. L., ÜCkert, F., Bürkle, T., & Prokosch, H.-U. (2005). Cross-institutional data exchange using the clinical document architecture (CDA). *International Journal of Medical Informatics, 74*(2-4), 245-256.

NSWADT (2004, 28 February 2007). KJ v Wentworth Area Health Service. *Office of the NSW Privacy Commissioner* Retrieved 30 September, 2010, from http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_07_cnadt84

Nunamaker, J. F., Chen, M., & Purdin, T. (1991). Systems development in information systems research. *Journal of Management Information Systems, 7*(3), 89-106.

Ohno-Machadoa, L., Silveira, P. S. P., & Vinterbo, S. (2004). Protecting patient privacy by quantifiable control of disclosures in disseminated databases. *International Journal of Medical Informatics, 73*(7-8), 599-606.

Parker, C., Wafula, E., & Swatman, P. (1994). *Information systems research methods: The technology transfer problem.* Paper presented at the 5th Australian Conference on Information System, Caulfield, Vic.,Monash University, Department of Information Systems.

Peleg, M., Beimel, D., Dori, D., & Denekamp, Y. (2008). Situation-Based Access Control: Privacy management via modeling of patient data access scenarios. *Journal of Biomedical Informatics, 41*(6), 1028-1040.

Pierce, F. S. (2003). Biometric Identification. *Health Management Technology, 24*(5), 38.

Pons, A. P., & Polak, P. (2008). Understanding user perspectives on biometric technology. *Commun. ACM, 51*(9), 115-118.

Privacy & Personal Information Protection Act 1998 Act No. 119 of 1988 as amended C.F.R. (2009).

Rash, M. C. (2005, April 4). Privacy concerns hinder electronic medical records. *The Business Journal of the Greater Triad Area*.

Reynolds, P. (2004). The keys to identity: as healthcare organizations strive for greater security, some are using a very personal approach in the form of biometrics.(Security/Authentication)(Cover Story). *Health Management Technology, 25*(12), 12(14).

Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., et al. (2007). Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association, 14*(1), 1-9.

Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption *Advances in Cryptology – EUROCRYPT 2005* (pp. 457-473). Berlin/Heidelberg: Springer

Sahai, A., & Waters, B. (2008). Fuzzy Identities and Attribute-Based Encryption *Security with Noisy Data* (pp. 113-125). London: Springer

Sakamoto, N., & Nakaya, u. (2005.). 2005. In S. S. e. al. (Ed.), *HSI 2005* (pp. 165 - 178). Berlin Heidelberg: Springer-Verlag.

Sandhu, Coynek, E. J., Feinsteink, H. L., & Youmank, C. E. (1996). Role-Based Access Control Models. *IEEE Computer, 29*(2), 38-47.

Sandhu, Ferraiolot, D., & Kuhnt, R. (2000, July 26-27). *The NIST Model for Role-Based Access Control: Towards A Unified Standard.* Paper presented at the 5th ACM Workshop on Role Based Access Control, Berlin, Germany.

Sandhu, R. S., & Samarati, P. (1994). Access control: principles and practice. *IEEE Communications Magazine, 32*(9), 40-48.

Shamir, A. (1985). Identity-Based Cryptosystems and Signature Schemes *Advances in Cryptology* (pp. 47-53). Berlin/Heidelberg: Springer.

Shin, Y. N., Lee, Y. J., Shin, W., & Choi, J. (2008, March 25-28). *Designing Fingerprint-Recognition-Based Access Control for Electronic Medical Records Systems.* Paper presented at the INAW 2008 - 2nd International Conference on Advanced Information Networking and Applications - Workshops, Okinawa, Japan.

Shine, K. (1996). Impact of Information Technology on Medicine. *Journal of Technology and Society, 18*(2), 117-126.

Stair, R., & Reynolds, G. (2009). *Principles of Information Systems: A Managerial Approach* (9th ed.). Boston: Thomson/Course Technology.

Stallings, W., & Brown, L. (2008). *Computer security : principles and practice*. Upper Saddle River, NJ: Pearson international.

Takeda, H., Matsumura, Y., Kuwata, S., Nakano, H., Sakamoto, N., & Yamamoyo, R. (2000). Architecture for networking electronic patient records systems. *International Journal of Medical Informatics, 69*(2), 161-167.

Tanenbaum, A. S. (2003). *Computer Network* (4th ed.). New Jersey: Prentice Hall.

Tnag, P., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association 13*(2), 121-126.

Um, K. S., Kwak, Y. S., Cho, H., & Kim, I. K. (2005). Development of an HL7 interface engine, based on tree structure and streaming algorithm, for large-size messages which include image data. *Computer Methods and Programs in Biomedicine, 80*(2), 126-140.

van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *International Journal of Medical Informatics, 78*(3), 141-160.