Information security strategy in Telemedicine and e-Health systems:

A case study of England's Shared Electronic Health Record System

A Thesis submitted for the degree of Doctor of Philosophy

By

Yara Mahmoud Mohammad

School of Information Systems, Computing and Mathematics

Brunel University

October 2010

Author's Declaration

I hereby declare that I am the sole author of this thesis.
I authorise Brunel University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

Signature

Date:

Abstract

Shared electronic health record (EHR) systems constitute an important Telemedicine and e-Health application. Successful implementation of shared health records calls for a satisfactory level of security. This is invariably achieved through applying and enforcing strict, and often quite complicated, rules and procedures in the access process. For this reason, information security strategy for EHR systems is needed to be in place. This research reviewed the definition of different terms that related to electronically stored and shared health records and delineated related information security terms leading to a definition of an information security strategy. This research also made a contribution to understanding information security strategy as a significant need in EHR systems. A major case study of the National Programme for IT (NPfIT) in England is used to be the container of other two sub-case studies in two different Acute Trusts. Different research methods used: participant observation and networking, semi-structured interviews, and documentary analysis. This research aimed to provide a comprehensive understanding to the information security strategy of England's EHR system by presenting its different information security issues such as consent mechanisms, access control, sharing level, and related legal and regulatory documents. Six factors that influence the building of an information security strategy in EHR systems, were identified in this research, political, social, financial, technical, clinical and legal. Those factors are considered to be driving the strategy directly or indirectly. EHR systems are technical-clinical systems, but having other factors (than technical and clinical) that drive this technical-clinical system is a big concern. This research makes a significant contribution by identifying these factors, and in addition, this research shows not only how these factors can influence building the information security strategy, but also how they can influence each other. The study of the mutual influence among the six factors led to the argument that the most powerful factor is the political factor, as it directly or indirectly influences the remaining five factors. Finally, this research proposes guidelines for building an information security strategy in EHR systems. These guidelines are presented and discussed in the form of a framework. This framework was designed after literature analysis and after completing the whole research journey. It provides a tool to help putting the strategy in line by minimising the influence of various factors that may steer the strategy to undesirable directions.

Dedication

To my Parents:

Mahmoud Mohammad & Khadija Younes

Acknowledgement

I would like to extend my heartfelt gratitude and appreciation to Professor Ray Paul for his invaluable guidance and support throughout the course of this research for my PhD degree. My sincere thanks and appreciation go to Dr Lampros Stergioulas for his supervision and for assisting me and guiding me during my study for my MSc and PhD degrees. I would like to thank Dr Malcolm Clarke, Dr Tanja Bratan, Urvashi Sharma, and all BRiGHT research group members for their support. I also wish to convey my thanks to Professor Trisha Greenhalgh.

My thanks to the Ministry of Health and Ministry of Higher Education in Syria for funding my study during my MSc and PhD degrees.

My deep gratitude goes to my parents, sisters and brothers for their encouragement and inspiration in all my undertakings. I would also like to express my love and gratitude to my friends for their support.

Contents

List of Figures

Glossary of terms

Term	Description
ACF	Access Control Framework
CfH	Connecting for Health
CRS	Care Records Service
DoH	Department of Health
EHR	Electronic health record
EMR	Electronic medical record
EPR	Electronic patient record
ERDIP	Electronic Record Development and Implementation Programme
ETP	Electronic Transmission of Prescriptions
FFIEC	Federal Financial Institutions Examination Council
GP	General Practitioner
HR	Human Resources
IG	Information Governance
IGSoC	Information Governance Statement of Compliance
ISG	Information security governance
ISM	Information security management
ISMS	Information Security Management System
ISO	International Standards Organisation
IT	Information Technology
LAN	Local area network
LPfIT	London Programme for IT
LR	Legitimate Relationship
LRS	Legitimate Relationship Service
LSP	Local Service Provider
N3	National Network for the NHS
NCRS	NHS Care Records Service
NHS	National Health Service
NHS IT	National Health Service Information Technology
NMEPfIT	North, Midlands and East (NME) Programme for IT
NPfIT	National Programme for IT
PACS	Picture Archiving and Communications Systems
PAS	Patient Administrations System
PHR	Personal health record
QMAS	Quality Management and Analysis System
RA	Registration Authority
RA	Regulatory Affairs
SCR	Summary Care Records
SPfIT	Southern Programme for IT
SUS	Secondary Uses Service
UUID	Unique identity number
WAN	Wide area network

Publications arising from the Thesis

The following publications have arisen from the research carried out:

Mohammad, Y. Stergioulas, L. (2010) 'Building an information security strategy for EHR: guidelines for assessing the current situation', *32nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society* "Merging Medical Humanism and Technology", 31 August - 4 September, Buenos Aires, Argentina.

Mohammad, N. **Mohammad, Y.** Auray, J. and Verdier, C. (2008) 'Evaluation of health information systems: reasons for failure', *ICSSHC Congress*, 3-5 September, Lyon, France.

Greenhalgh, T. Stramer, K. Bratan, T. Byrne, E. **Mohammad, Y.** and Russell, J. (2008) ,innovation theory multi-site case study using diffusion of Introduction of shared electronic records', *British Medical Journal*, 337;a1786.

Greenhalgh, T. Stramer, K, Bratan, T. Byrne, E. Russell, J. **Mohammad, Y.** Wood, G. Hinder, S. (2008) *Summary Care Record Early Adopter Programme: An Independent Evaluation by University College London*. University College London, London, UK. (http://www.haps.bham.ac.uk/publichealth/cfhep/002.shtml)

Mohammad, Y. Stergioulas, L. (2007) 'Articulation and implementation of data protection policies in Electronic Health Records (EHR)', The publication reflects proceedings at the *Westminster Health Forum Seminar Leadership, Management and Incentives in the NHS*, February, London, UK.

Mohammad, Y. Stergioulas, L. and Yosuf, M. (2007) 'Data protection in shared health records: requirements and challenges', *Medinfo 2007 Congress*, 20-24 August, Brisbane, Australia.

Chapter One

Problem & Context

1.1 Introduction

There are different applications of Telemedicine and e-Health, and shared electronic health record (EHR) systems are one of these applications. Shared EHRs are accessible and shared in different places with different users. Electronic health records (EHR) systems are still in their infancy and shared patient records is the new form of EHR. With shared health records, the accuracy and accessibility do increase, but potential threats to confidentiality and patient privacy are more controversial (Carter, 2000). "From the patient's perspective, confidentiality is essential to the patient-physician relationship" (Whiddett et al., 2006). For this reason, the consideration of confidentiality and privacy requirements is very important for achieving a satisfactory level of patient data security.

Electronic health records require strictly controlled access. The information accessing process should identify the users and determine their roles. In addition, it should be established if they are entitled to look at the patient's record and which parts of the record they need or are allowed to access.

The concept of information security encompasses some issues like privacy and trust (Purser, 2004). In addition, information security can be viewed from different disciplines and dimensions (Solms, 2001), such as legal, ethical, political, financial, technical and organisational.

Furthermore, information security contains different elements such as integrity, confidentiality, access control, availability, authenticity and utility (Tipton and Krause, 2004 and Steward, 2005). For this reason some security dimensions (Solms, 2001) should be determined in order to start the process of designing a good information security strategy (Wylder, 2004) in an electronic health record system. The limits of the existing information systems must be exceeded and a strategy that supports new technologies and services must be chosen to meet patients' expectation of quality and efficiency in healthcare (Elberg, 2001).

The implementation of shared health records demands a satisfactory level of security. This is invariably achieved through applying and enforcing strict, and often quite complicated, rules and procedures in the access process, which perplex and confuse users. Furthermore, the increasingly sophisticated use of information and communications technologies is constantly threatening to reduce people's privacy (Margulis, 2003). The current challenge is to implement a shared health record system, which is easy and secure to use, and satisfies all stakeholders, such as patients, health professionals, healthcare providers, and other groups in terms of legal or financial requirements.

1.2 Problem definition

This research attempts to investigate the current view and use of some shared electronic health record systems and helps to figure the influencing factors on implementing and developing information security strategy in shared electronic health records. Moreover, this research attempts to provide possible recommendations for developing an information security strategy. This involves analysing the current situation of information security in EHR systems and the current security requirements accommodated in the deployment of data protection policies. It attempts to explore the key steps required to design an appropriate information security strategy (Purser, 2004). The study researches the possibility to develop a framework to obtain desired levels of security starting from user permission schemes, policies around patient rights and stakeholder views. Then, it studies examples and success factors that could be important for implementation of information security strategy of EHR systems in real settings.

In addition, the research aims to find and explore some issues that could exist in the current policy of granting access to EHRs by different users outside healthcare organisations, including legal, ethical and civil rights issues, and it goes beyond this by suggesting methods for solutions. It provides a categorisation system of users' access rights with respect to EHR information sharing and the level of interaction with the EHR system for each user group that is required to satisfy the patient's privacy and confidentiality needs.

This research employs qualitative research approach (i.e. interviews with doctors, nurses, IT staff, managers and patient group representatives), with the primary purpose to determine the experiences and opinions of the interviewees on electronic health records and their concerns regarding data protection and information security issues.

1.3 Aim & Objectives

1.3.1 Aim

To investigate the influence of various factors on building information security strategy for electronic health record systems.

1.3.2 Objectives

***** Understanding the EHR information security strategy

- To attempt characterising the different disciplines that should be taken into account when considering an information security strategy in EHR systems.
- To intend designing a suitable, effective and convenient research method to collect and analyse relevant information.
- To study access rights within and outside healthcare organisations.
- To assess the level of confidence and trust in using shared health records for different EHR user groups.

* Building EHR information security strategy

- To investigate possible ways to develop an information security strategy with well designed policies to achieve a level of security acceptable to the range of users involved.
- To determine privacy and confidentiality concerns and requirements of EHR user groups, and to estimate the degree to which these needs, designs and visions have been accommodated.
- To suggest key elements for building a framework for implementation which offers guidelines on how to implement EHR systems with the desired levels of security and functionality and on how to apply information security strategy on a real EHR system.

1.4 Research design

To achieve the aims of this research, the chosen approach is a case study design; see

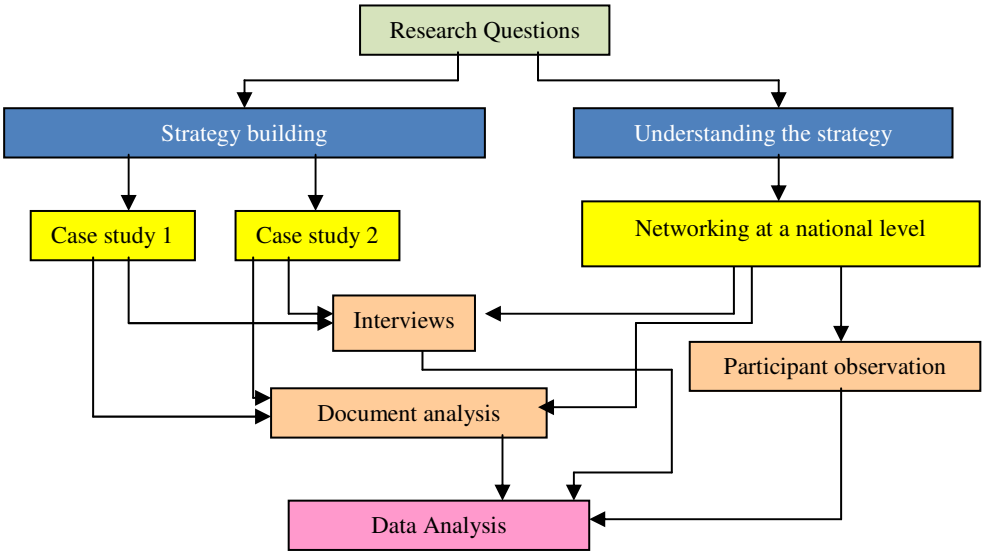

Figure 1.1: Research design

Figure 1.1 (which will be explained in detail in Chapter Three). This case study is being analysed in three different levels (macro, meso and micro). The macro level is the national level, which is based on exploring and analysing the National Programme for IT (NPfIT) in England. On this level, the national strategy for information security of EHR systems will be researched, studied and explained in Chapter Four; the meso level is the organisational level which is being based on choosing two different acute Trusts in London; and the micro level involves different individuals who are users or developers of EHR systems. On the meso and micro levels, different issues are being explored regarding what could influence building an information security strategy of EHR systems as will be discussed in Chapter Five. Then, suggested solutions and guidelines based on analysing the three different levels will be provided in Chapter Six.

1.5 Impact of research

It is aimed that the findings will provide a clear idea about the potential problems and challenges which might exist in the current information security procedures in some EHR systems or might arise in future systems.

1.6 Challenges

A major challenge in this study is to explore the security and privacy requirements from various points of view. Furthermore, the significant difference amongst the various user groups in healthcare necessitates more sophisticated information sharing policies than in any other IT system. The widespread adoption of access-controlled EHRs depends on solutions being found to several challenging technical and policy issues. Another challenge comes from addressing the relevant ethical issues, which more often than not, make a critical judgement difficult with regard to many privacy and confidentiality matters.

1.7 Thesis outline

Chapter one: This chapter begins by providing an introduction to the main issues that this research addresses. The focus of this research is information security in sharing health information in a digital form by using the electronic health records. The chapter provides the aim and the objectives of this research and a description of the originality and the impact of this research.

Chapter two: By providing a brief introduction to the main area of this research, the chapter provides a detailed definition of different terms that are used in this research, and then provides an overview about electronic health records and a background on information security strategy by reviewing normative and relevant literature.

Chapter three: This chapter discusses the research design and explains the research methods used together with the reasons for choosing each method, and the chosen approach for obtaining and analysing information in this research.

Chapter four: This chapter presents all captured information, from different resources, about information security issues in the NPfIT, in an attempt to understand the information security strategy for England's EHR system.

Chapter five: This chapter identifies different factors that influence building information security strategy for an EHR system by discussing these factors and showing different points of view of stakeholders and relevant newsletter articles that been published.

Chapter six: This chapter provides suggested guidelines for building an information security strategy for EHR systems based on the three steps of building strategy, which they are analysing the current situation, determining the requirements and defining the target situation.

Chapter seven: This chapter summarises the main conclusions of this research and evaluates research outcomes. It also discusses the applicability of the findings and the future development of EHR security, and it presents the research limitations and research contributions as well as directions for future work.

Chapter Two

Information Security Strategy of EHR Systems in context

This chapter presents a definition of information security strategy for electronic health record systems, and an overview about electronic health records and information security strategy as found in literature. This chapter starts by defining different terms that related to EHR, information security, and strategy. Following the definitions, an overview about electronic health records is presented, and the different information security issues in EHRs are highlighted. Then, a general description about information security strategy and how to build it is provided.

2.1 Concepts and definitions

In this research, it is needed to define the concepts that are used for designing the research method, collecting and analysing research information. Different terms could be used to indicate same or similar subjects. For this reason, it is important to puzzle out the meaning of used terms in this research and to clarify why these terms are chosen.

Because this research focuses on shared electronic health records and their information security strategy, it is necessary to determine what is meant by "shared electronic health records", "information security" and "strategy".

2.1.1 Shared electronic health records

Different terms could be used to describe health and medical information that been stored and shared in an electronic form such as EHR, EMR, EPR and PHR. Each term indicates different type of records as defined by different resources as follows:

- **Electronic health record (EHR)** includes information regarding patient needs to support continuing, efficient and quality integrated healthcare provided by different healthcare professionals (Hayrinen et. al, 2008). The EHR is a computer-based collection of health information of patients that has been gathered and managed by

an enterprise, typically a clinician or a hospital. There are those who consider EHRs as a combination of EMRs and PHRs, but EHR is used by clinicians, not patients (Clarke and Meiris, 2006).

- **Electronic medical record (EMR)** is the record that includes clinical information which is held in a structured representation, as clinical information is the information which falls, strictly within the medical domain (Rector et. al, 1991), and it is a computerised platform for managing medical information collected by a hospital or clinician practice (Clarke and Meiris, 2006). EMRs don't include non-medical information such as social or mental health information.

- **Electronic patient record (EPR)** implies to the individual healthcare information for principal use in patient care (Takeda et. al, 2000).

- **Personal health record (PHR)** is a person-centred system designed to track and support health activities across one's entire life experience; not limited to single organisation or provider (Clarke and Meiris, 2006). The PHR is "*a set of computer-based tools that allow people to access and manage their lifelong health information and make appropriate parts of it available to those who need it*"(Kaleber et al., 2008).

In this research, the term of EHR is used because it has a wider use for different medical, health and personal information of patients during their lifetime.

2.1.2 Information security

There are different terms to be considered when talking about information security, such as:

- **Information security** is used to protect information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investments and business opportunities (Ladan et al., 2006). Information security involves the use of physical and logical data access controls to ensure the proper use of data and to prevent unauthorized or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets (Peltier, 2001 in Anderson, 2003).

Information security is also "*a well-informed sense of assurance that information risks and controls are in balance*" (Anderson, 2003).

Information security includes measures and controls of systems' protection against denial of service and unauthorised (accidental or intentional) disclosure, modification, or destruction of systems and data. System security considers all hardware and software functions, characteristics and features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the system and for the data and information contained in the system. It includes the totality of security safeguards needed to provide an acceptable protection level for a system and for data handled by a system (Slade, 2006).

- **Data protection** refers to the set of privacy-motivated laws, policies and procedures that aim to minimise intrusion into respondents' privacy caused by the collection, storage and dissemination of personal data (Glossary of Statistical Terms).

- **Confidentiality** is the privacy interests that arise from specific relationships (e.g., doctor/patient, researcher/subject) and corresponding legal and ethical duties (Boulos et al., 2009 and US CDC Public Health Law 101). It refers to the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (Gerber et.al, 2001 and ISO/IEC TR 13335-1, 1996) ensuring that information is accessible only to those authorised to have access (Ladan et al., 2006). Confidentiality is to protect sensitive information from unauthorized disclosure (Vermeulen, et al., 2002) or intelligible interception (Posthumus and Solms, 2004, Gerber et al., 2001 and Boddington and Hill, 1998).

- **Integrity** is the property that data have not been altered or destroyed in an unauthorized manner (Gerber et al., 2001 and ISO/IEC TR 13335-1, 1996) ensuring that information is accurate and complete (Vermeulen, et al., 2002) in storage and transport; that is correctly processed (Gerber et al., 2001 and Boddington and Hill, 1998). Integrity also includes reliability which is the property of consistent intended

behaviour and results (Gerber et al., 2001 and ISO/IEC TR 13335-1, 1996) and safeguarding the accuracy and completeness of information and processing methods (Ladan et al., 2006).

- **Availability** is "*the property of being accessible and usable upon demand by an authorised entity*" (ISO/IEC TR 13335-1, 1996, pp.5) ensuring that information is available to those who are authorised to have it, when and where they should have it (Boddington and Hill, 1998, and Gerber et al., 2001). In this case, data is accessible when required (Vermeulen, et al., 2002) by authorised users who have access to information and associated assets when required (Ladan et al., 2006).

- **Privacy** is technically defined as the condition of being isolated from view, or secret. Privacy can be seen more concerned with social aspects, which is generally known as the ability to control information about oneself. Slade (2006) provided some definitions of privacy, which they are: (1) the right of an individual, acting on its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others. (2) The right of individuals to control or influence what information related to them may be collected and stored, and by whom, and to whom, that information may be disclosed. This term is not a synonym for confidentiality, which is a different concept. Privacy is a reason for security rather than a kind of security (Slade, 2006). Privacy in health sector is the individual's right to control the acquisition, use and disclosure of their identifiable health information (Boulos et al., 2009 and US CDC Public Health Law 101).

- **Auditability** (usually called accountability) (ISO/IEC TR 13335-1, 1996). It is the ability of investigation, which ensures that the actions of an entity may be traced uniquely to the entity (Gerber et al., 2001).

- **Information security management (ISM)** refers to the structured process for the implementation and on-going management of information security in an organisation (Vermeulen and Solms, 2002).

- **Information security governance (ISG)** describes the process of how information security is addressed at an executive level (Posthumus and Solms, 2004)

- **Authenticity** is "*the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information "(*ISO/IEC TR 13335-1, 1996, pp.5). It can also be referred to as the property that ensures the integrity of the identity (Gerber et al., 2001).

Therefore, in this research information security encompasses all the above mentioned security issues.

2.1.3 Strategy

This research is concerned with strategy of information security; however, it is essential to recognise the difference between strategy, policy, and standard, as each of these terms have different meaning and is used for specific purposes.

- **Strategy**: Burke and Jarratt, (2004) explained the definition of a strategy as they believe that strategy has been the subject of extensive research since the 1960s. Chandler (1962) described strategy as the process of determining the organisation's long-term goals and objectives, of adopting a course of action and allocating sufficient resources. This traditional and implicitly rational definition of strategy was later challenged by Mintzberg's (1978) and Mintzberg and Waters's (1985) contention that strategy was more a pattern of action resulting from whatever intended (deliberate) or unintended (emergent) strategies were realized. Mintzberg (1978) assumed that strategy could be something more than an explicit plan of action. According to Burke and Jarratt (2004), strategy can be seen from different angles which recognised "strategy as plan", "strategy as pattern", "strategy as ploy", "strategy as perspective", and "strategy as position". Since Mintzberg's contribution, strategy has become much more than planning. Strategy is what the firm does much more than what a firm says it is going to do to compete in the marketplace. As Mintzberg (1978) concludes, strategy is not just a notion of how to deal with an enemy or a set of competitors or a market, as it is treated in so much of the literature and in its popular usage. It also draws into some of the most fundamental issues

about organizations as instruments for collective perception and action (Burke and Jarratt, 2004).

- **Policy** can be defined as ‘‘a course of action, guiding principle, or procedure considered expedient’’ or ‘‘a certificate of insurance’’ (Solms and Solms, 2004 and The American Heritage Dictionary, 2000). Policy is a broad statement of principle that presents management’s position for a defined control area. Policies are intended to be a long-term guide of more specific rules to address specific situations. Policies are interpreted and supported by standards, baselines, procedures, and guidelines. Policies should be relatively few in number, should be approved and supported by executive management, and should provide overall direction to the organization. Policies are mandatory in nature, and an inability to comply with a policy should require approval of an exception (Tipton and Krause, 2004). Policy is organizational-level rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures. Policies are supported by more detailed guidelines, procedures, and standards (Slade, 2006).

- **Standard** is described by language is the form of that language which is considered acceptable and correct by most educated users of it (Cambridge Dictionary). Standard is a rule that specifies a particular course of action or response to a given situation. Standards are mandatory directives to carry out management’s policies and are used to measure compliance with policies. Standards serve as specifications for the implementation of policies. Standards are designed to promote implementation of high-level organization policy rather than to create new policy in themselves (Tipton and Krause, 2004). Part of the supporting detail of a security policy, a standard is a specific item of hardware or software, configuration, or level of performance that is to be adhered to in operations (Slade, 2006).

- **Information security strategy** is the roadmap for the foreseeable future and details how the organisation intends to progress along the path of maturity. The strategy therefore provides a consistent and coherent framework for improvement and ensures that the organisation remains focused on the most important issues (Purser, 2004). It is a plan to prevent or minimise risks while complying with legal, statutory, contractual, and internally developed requirements (FFIEC, 1998 and Wylder, 2004).

- **Information security policy** is a direction-giving document for information security within an organisation. It is a document that indicates management's commitment to and support of information security, as well as defining the role of information security that has to play in reaching and supporting the organisation's vision and mission (Hone and Eloff1, 2002). Information security policy is a document or set of documents that describes, at a high level, the security controls that will be implemented in an organisation (Andress, 2004). And it may be defined as "*complied documentation of computer security decisions*" (NIS00).

- **Information protection policy** provides guidelines to users on processing, storing, and transmitting sensitive information. The main goal of this policy to ensure that information is appropriately protected from unauthorised modification or disclosure (Andress, 2004)

- Baseline is a platform-specific security rule that is accepted across the industry as providing the most effective approach to a specific security implementation. Baselines are established to ensure that the security features of commonly used systems are configured and administered uniformly so that a consistent level of security can be achieved throughout the organisation (Tipton and Krause, 2004).

- **Procedure** defines specifically how policies, standards, baselines, and guidelines should be implemented in a given situation. Procedures are either technology or process dependent and refer to specific platforms, applications, or processes. They are used to outline steps that must be taken by an organisational element to implement security related to these discrete systems and processes. Procedures are normally developed, implemented, and enforced by the organisation owning the process or system. Procedures support organisation policies, standards, baselines, and guidelines as closely as possible, while addressing specific technical or procedural requirements within the local organisation to which they apply (Tipton and Krause, 2004).

- **Guideline** is a general statement used to recommend or suggest an approach to implementation of policies, standards, and baselines. Guidelines are essentially recommendations to consider when implementing security. While they are not

mandatory in nature, they are to be followed unless there is a documented and approved reason not to (Tipton and Krause, 2004).

To sum up, this research adopts that information security strategy of EHR systems is a roadmap for the foreseeable future and details the progress along the path of maturity and keeps the focus on the most important security issues while complying with legal, statutory, contractual and internally developed requirements for electronically stored and shared information to support continuing, efficient and quality integrated healthcare provided by different healthcare professionals.

In the following section below, the overview of EHR use, its characteristics, and benefits are described. In addition, the section is summarised by addressing issues surrounding information security in EHR systems.

2.2 Electronic Health Records

2.2.1 EHR overview

In the beginning, computer use in health care was for administrative and financial purposes in hospitals in the 1960s. It focused on the clinical input of data to improve clinical decisions and reduce medical errors (Berner and Simborg, 2005). With increasing pressure to enhance medical productivity, professionals tried to find more reliable systems that provide intuitive access to the information which they need when they see their patients (Shortliffe and Fagan, 2000). The ideal way to achieve this aim is to collect all information related to a patient in electronic files (Fritsche et al., 2001).

The electronic patient record system offers an improved access to patient-specific information and provides a major benefit for the quality of health care and for the quality of life of clinicians in practise (Shortliffe and Fagan, 2000). The new communication technologies offer clinicians creative ways to interact with their patients and to provide higher quality care (Shortliffe et al., 2000). The Internet's implications extend well beyond its impact on connecting up distributed health records. One can expect that as the Internet evolves and supports broadband communications, it will become the technology of choice for linking medical experts with other clinicians and patients at a distance (Shortliffe, 1998). The Internet

enables data sharing between distant computers, and medical observers believe that future implementations of electronic health record systems will be based on Internet technology (Kohane et al., 1996). Indeed today, distribution of biomedical information through the Internet is increasingly commonplace and accepted (Lowe et al., 1996). Because an electronic record provides a natural database for individually customised health messages, online records also open up new avenues for health education (Eysenbach, 2000).

The Internet offers an attractive infrastructure for the efficient communication of health information on a local or a global scale. However, Internet technologies were designed to optimise information sharing and interoperability, not security. In the area of healthcare, the potential benefits of ubiquitous data communications need to be balanced against the risks to personal privacy and the risks of data corruption and service interruption (Baker and Masys, 1999). Successful implementation of shared health records have to meet users' needs for acceptable levels of security and privacy, and also to address some important legal issues. The Internet gives the opportunity to access medical information worldwide which speeds the transformation of the patient-clinician relationship and also to share decision making between patient and clinicians (Winker et al., 2000). For Internet users who want to have access to medical information, personal privacy was ranked as their most important concern (Winker et al., 2000). Whatever electronic access to patient information is discussed, security issues are among the first ones raised because of concerns about confidentiality (Cimino et al., 2002)

A yet unanswered question is what health records will look like, once they have been effectively implemented on computer systems and the new possibilities to leverage their potential and enhance healthcare services become increasingly apparent. It is unlikely that the computer-based health record will bear much resemblance to the old fashioned paper-folder record that still inhabits many of healthcare environments. One can have a taster of the changes that are likely to occur to EHRs, by considering the potential role of wide-area networking and the Internet (Shortliffe et al., 2000).

2.2.2 EHR characterisations

Information sharing is generally accepted as the key to substantial improvements in productivity and better quality of care (Katehakis et al., 2001). For this reason shared

electronic health record systems should have some common characteristics and meet a number of common requirements, which could provide the ingredients for setting common international standards on implementation of electronic health record systems. Fritsche et al. (2001) noted that collection of comprehensive and valid scientific medical data through EHR should be:

1- Easy to install and maintain with less cost.
2- Time-saving for the medical staff who use it in their daily work.
3- Able to store all medical information in retrievable format to allow compatibility with other systems.
4- Able to provide validation of medical data by repeated use of data in patient's care.

2.2.3 EHR benefits

Nowadays computer systems can store an enormous quantity of data in a small physical space (Coiera, 2003). With electronic health records, it is easy to produce duplicate copies of data for purposes, such as data sharing, or to create back-up copies for security reasons. On the other hand, paper records are neither easily nor routinely duplicated, and can be exposed to physical damage or destroyed by disasters such as fire or flooding, or they could be lost in transit (e.g. in the mail) when moving from city to city (Coiera, 2003 and NHS CfH, 2006a).

Other advantages of computer-based health records are that such systems can incorporate information management tools to provide services such as clinical reminders and alerts, linkages with knowledge sources for healthcare decision support, and analysis of collected data (Shortliffe et al., 2000). Baldwin et al (2003) believe that sending medical diagnostic information in an electronic form will benefit telemedicine applications "*however, we believe that the change in use of the consultation from diagnosis to management, with diagnostic information sent in advance, has been the most significant factor affecting the consultation time.*"

One of the most important and desirable characteristics of EHR is the capability offered to users to modify records and update information. In the daily use of health records (paper or electronic), there is a significant probability of entering incorrect

information, but it is relatively easy to correct the incorrect entries only in the case of computer-based health records (Fritsche et al., 2001).

2.3 Information security issues in EHR systems

According to Slade (2006), the three basic aspects of security are considered to be confidentiality, integrity, and availability. Those aspects implicate specific considerations when talking about shared EHRs, such as access control, consent mechanisms and data accuracy. "*There is a need to investigate certain pertinent issues regarding healthcare data quality and integrity"* (Guah and Currie, 2004).

According to Papazafeiropoulou and Gandecha (2007), two problems are associated with sharing EHRs which they are " *patients may not be able to predict who might need to see their data. In addition, health professionals may find it time consuming to maintain a cross-referenced database for each patient*." Shortliffe and Fagan (2000) argued that there are at least four major issues that have consistently constrained the efforts to build effective EHR systems, which they are:

1- Standards are needed in the area of clinical terminology;
2- Concerns about data privacy, confidentiality, and security;
3- Challenge of data entry by physicians;
4- And difficulties related to integration of record systems with other information and data in healthcare settings.

2.3.1 Consent mechanisms

It is very important to understand the different models of consent. Patients' consent can be obtained by different ways. By all means, informed consent is the term of approaching a legal and ethical consent. Here are the definitions of some consent mechanisms:

- **Informed consent** means "informed, competent and voluntary consent" (Kluge, 2004). It is said to obtain when the patient has been given all information that the objective reasonable person in the patient's position would want to know before making a choice. In addition, the patient must have understood the information at a subjective level, must also have understood the likely consequences of any choice

that could be made, and must have made the choice in an authentic fashion (Kluge, 2004), Gert, 2002 and Hyun, 2002). "*The electronic patient record should be treated never as a mere thing but always as a person-analogue in information and decision space*" (Kluge, 2004).

- **Implied consent** is where agreement may reasonably be informed form the action or inaction of the individual and there is good reason to believe that the patient has knowledge relevant to this agreement (Win, 2004).

- **Express consent** is the consent given explicitly, either orally or in writing. Express consent is equivocal and does not require any influence on the part of provider seeking consent (Win, 2004).

- **General consent with specific denials** refers to an instance in which a patient attaches specific exclusion conditions to the general approval of access to the record for future accesses (Win, 2004 and Coiera and Clarke, 2004).

- **General denial with specific consent** refers to an instance in which a patient issues a blanket block on all future accesses, but allows the inclusion of future use under specified conditions (Win, 2004 and Coiera and Clarke, 2004).

Informed consent implies that patients are fully informed of the implication of their medical status, and give voluntary agreement to divulge or permit access to or the collection of their information (Win, 2004). Effective notification and truly informed consent requires that individuals know and understand the contents of the record (Win and Fulcher, 2007 and Carter, 1998).

It is unethical to use implied consent when the patient is not fully aware of information disclosure. Health data shouldn't be processed in the absence of explicit consent unless they are needed for medical purposes or undertaken by a professional who, in the circumstances, owes a duty of confidentiality (Win, 2004). The preceding assumes a competent patient. Not all patients fall into that category. Some are incompetent, and even there are many sub-categories, such as children, the congenitally incompetent, incompetent patients who previously were competent, etc.

An ethical security structure should include tests for competence in its protocols and it should engage appropriate substitute consent (Kluge, 2004).

2.3.2 Access control

Individuals that use an EHR are authorised to use the components of an EHR according to identity, role, work-assignment, present condition and/or location in accordance to an individual's scope of practice within a legal jurisdiction (Dickinson et al., 2004).

According to Bakker (2004), in a request to an information system that probably holds data for a certain patient, the following items should be specified:

- The identity of the patient.
- The date and time when the data are requested.
- The identity and qualifications of the health professional who is asking for the data.
- The role of the health care professional.

2.3.3 Data accuracy

Agrawal and Johnson (2007) suggested that mechanisms are needed to enable patients to check the accuracy of their data and make corrections in case errors are found. Staroselsky et al (2006) stated that engaging patients in the review and electronic submission of health maintenance information can contribute to a more complete EHR. However, it does not eliminate the need for direct routine data exchange among providers. All available information resources should be incorporated into a system that will provide accurate data to the right clinicians at the right time so they can make appropriate choices that improve the quality of patient's care (Staroselsky et al, 2006).

2.4 Information security strategy

It is very common in any business to have a strategy; meanwhile, a strategy itself is a plan that needs to be designed in a timeline. Purser set a timeline for producing

information security strategy, this timeline can be adopted to build the information security strategy for shared EHR Systems as well.

The steps of building an information security strategy according to (Purser, 2004) are:

1. Analysis of the current situation
2. Business strategy requirements
3. Legal and regulatory requirements
4. Requirements due to external trends
5. Definition of the target situation
6. Definition/ prioritisation of strategic initiatives
7. Distribution of draft strategy
8. Agreement/Publication of final strategy

To make these steps clearer, they can be reduced to focus on the major stages only of creating an information security strategy, which they are:

1. Analysis of the current situation.
2. Determination of the requirements.
3. Definition of the target situation.

Those three steps can be simplified as when there is a need to plan for any project, first, the planners should know what they have, then what they need, and finally what they want. To abridge the steps in three words (have, need, want) as it shows in Figure 2.1.

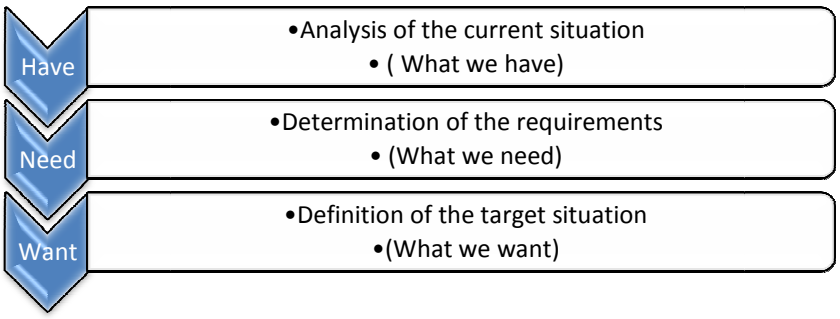

Figure 2.1: The three steps to build a strategy

According to the handbook of the Federal Financial Institutions Examination Council (FFIEC) (2006), they described that the security strategy should include:

- Appropriate consideration of prevention, detection, and response mechanisms,
- Implementation of the "least permissions" and "least privileges" concepts,
- Layered controls that establish multiple control points between threats and organization assets, and
- Policies that guide officers and employees in implementing the security program.

According to Posthumus and Solms (2004), they draw the internal and external requirements that contribute to an effective information security strategy as it shows in Figure 2.2:

External requirements and guidelines:

- Information security standards and best practices.
- Legal and regulatory issues.

Internal requirements:

- Business issues.
- IT infrastructure issues.

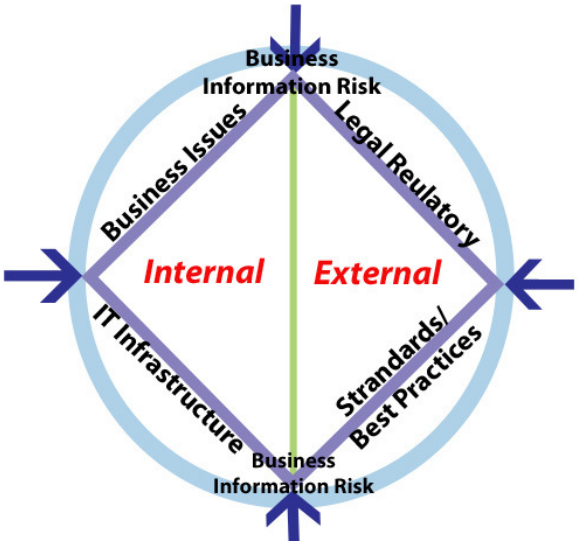

Figure 2.2: The internal and external requirements that contribute to an effective information security strategy (Posthumus and Solms, 2004)

Swindle and Conner (2004) stated that information security is a complex issue. For this reason, information security must become a central management and governance responsibility (Posthumus and Solms ,2004).

Implementing and developing an information security strategy is a dynamic procedure as it requires corresponding with different changes inside or outside the system. Figure 2.3 shows the strategic planning cycle.

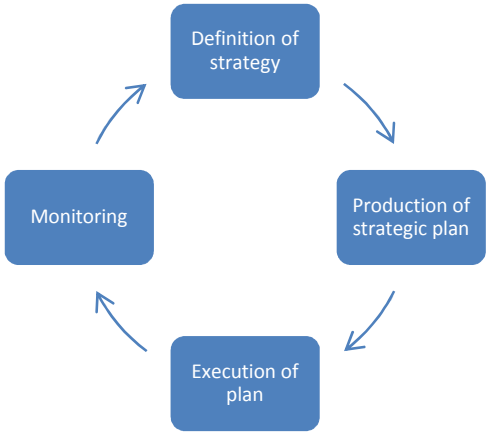

Figure 2.3 The strategic planning cycle (Purser, 2004)

Summary

This chapter has showed that there are different types of electronic records that include health and medical information. These records are categorised and defined according to the type of information and the contents of these records. EHR has a wider use comparing to other electronic records that contain different medical, health and personal information of patients in their lifelong time. This is why this kind of record is selected in this research after comparing it to other records, such as EMR, EPR and PHR. The term of information security is chosen in this research because it has a comprehensive meaning that includes all security issues such as data protection, confidentiality, integrity, availability, etc. Furthermore, the third focus in this chapter is on the meaning of strategy, and how to emerge information security concept in a strategy in EHR systems. This chapter provided the main tools for understanding the combination of EHR systems and their information security issues, and how a strategy can be designed especially for information security.

Chapter Three

Research Methodology

In this chapter, the rationale for the employed methodology in this research is explained, starting with methodology design and then describing the research methods that have been used with explanation why these research methods were chosen. The overall research approach is outlined, followed by detailed description of the data collection and data analysis resources.

3.1 Methodology design

This research attempts to define the different factors that influence building information security strategy of EHR systems. It also pursues the possibility of providing guidelines for developing and implementing an information security strategy for shared EHR systems. The research was designed to achieve the above aims. Information security strategy is a subject that concerns human behaviour and it also imports different cultural and circumstantial beliefs. Therefore, it needs to be guarded by specific rules. These concerns led the researcher to employ a qualitative research approach for the purpose of this research.

This research involves different stakeholders as well as different types of shared health records, and it considers diverse range of policies, legal Acts and released documents. Therefore, a hybrid research method was designed to collect the required research information to achieve the aim of this study. Where, hybrid model is defined later in the chapter.

It is essential to look at EHR systems from different angles and points of view from a wider prospective. At the same time a detailed view of different EHR systems should be considered.

A major case study with ethnographic research method of the National Programme for IT (NPfIT) in England is carried out, containing other two sub-case studies in

two different Acute Trusts. This approach helps to obtain wide and partial views of EHR systems.

Information about the NPfIT was updated regularly by attending National Health Service (NHS) Connecting for Health (CfH) events, which helped observing the changes of the national plans and some local plans in EHR systems in England. An investigation was done on how different user groups of EHR systems are dealing with information security issues in their workplace. For this reason, a choice of two different hospitals was made to interview different professionals in different working areas such as Medical staff, IT staff and Information Governance staff, who provided their own views about the current systems they are using and they explained their concerns and hopes of having a desired secure EHR system. In addition to that, it was important to look at different released documents that are concerned with information security in dealing with shared electronic health information. The employed methods to collect research information are explained in detail later in this chapter.

Overall, a case study design was employed for this study (Yin, 1993). This approach allowed for "*an in-depth view of human actions and interpretations surrounding the development and use of computer-based information systems*" (Walsham, 1995). This helps in characterising the organizations' experiences in terms of processes of incremental or radical organizational change (Orlikowski, 1993).

According to Markus (1983), case studies could be made by

- Interviews with designers and users of the systems
- Documentary evidence about the systems and the organizations such as

  - corporate annual reports,
  - organizational charts,
  - design documents,
  - and internal correspondence about the systems.

- Last, a prediction based on research data analysis.

These qualitative methods including observational methods are used to study how a strategy around information security can be developed and the use of EHR in the work place. This provides the identification of different themes to peruse the research.

This research covers different EHR systems, and examines and analyses users' requirements. It includes at least the three levels of EHR users:

- End users – e.g. healthcare professionals
- Providers – e.g. software and network providers
- Mediatory – e.g. NHS CfH

3.2 Data collection methods

To be able to collect data for this research, a set of different research methods were applied. These methods are explained below:

3.2.1 Participant observation - Networking

An ethnographic method was used in this research by ongoing observation, both structured and unstructured (Crespin et al., 2005). "*In ethnography, these data sources are supplemented by data collected through participant observation. Ethnographies usually require the researcher to spend a long period of time in the "field" and emphasize detailed, observational evidence*" (Myers, 1999). The ethnographic research method was used by Orlikowski (1991) who collected his research data via participant observation, interviews, documents, and informal social contact with the participants (Myers, 1999).

Participation in Connecting for Health (CfH) events, along with sharing knowledge and providing ideas and suggestions in various NHS CfH workshops and conferences, helped identifying key issues and finding solutions. Attendance of these events also provides up-to-date information and data of the NHS Care Records Service (NCRS).

In addition, joining some specific networks and being a member of them such as the Health Informatics Community of the NHS allows sharing knowledge and data

online as well as in live meetings. This online community includes some NHS CfH Special Interest Groups such as the Health Records and Clinical Coders group and the Health Informatics Workforce Development group. Some of the regular meetings were organised to discuss some specific issues related to health informatics in the NHS in general and to NHS Care Records Service (CRS) in particular. There were many opportunities in taking part in other NHS CfH forums and networking activities, such as London Clinical Network Forum and Data Quality Forum, who organise regular meetings, workshops and conferences to raise and discuss up-to-date issues related to the NHS Care Records Service in the London Cluster.

Around 25 events were attended during three years. Appendix (F) lists the attended NHS CfH events. The first attended event was in October 2006 and the last was in November 2009. Those events were organised by NHS CfH to provide potential involvement opportunities to NHS professionals regarding the NPfIT in England. Some of these attended events focused on the NHS Care Records Service (CRS) in general and some other were about information sharing and information security issues in NHS Care Records Service such as consent, confidentiality, data quality, legitimate relationships and management of information security for the CRS. Most of these events were allocated for 100 attendees; only few were allocated for 200 or 400 attendees. Most of the events were attended by around 70% of available places. Most of these events were featuring live product demonstrations, exhibition area interactive workshops and questions and answers (Q&A) panel discussions.

The researcher interviewed different NHS staff and software providers informally during the attended events. Notes were taken by the researcher in these events, in addition to the presentations and different documents were shared after attending the events.

3.2.2 Semi-structured interviews

Semi-structured interviews were conducted with professionals who are working on EHR systems, mainly at the two hospital sites. They were asked to provide a description of the system they are currently using, specify particular problems they face in using the EHR system, and give some predictions about expected problems in the future. In addition, interviews with government NHS CfH management staff

provides important information needed to design an information security strategy from the decision maker's viewpoint. Furthermore, meeting with representatives of patient groups and patient associations provided generic information about patients' views.

Interviews with research participants took place at their normal place of work, unless otherwise agreed. The research involves no risks for participants, with the only inconvenience being the time expenditure for interviews. Participants were able to share their views and needs regarding information security in the electronic health records, which may enhance their understanding of this aspect of their work. The average number of interviews per participant is one interview of an approximate duration of 30-45 minutes (average duration: 40 minutes).

This research planned to interview:

- IT managers/ technical support staff.
- Software providers.
- Doctors.
- Nurses.
- Government NHS CfH management staff.
- Representatives of patient groups and patient associations.

Some of the above listed interviewees were interviewed in the two hospitals case studies, and some other interviewees such as patients' representatives, some software providers, nurses and other healthcare professionals were met and interviewed informally in different NHS CfH events.

The two case studies were done in two public hospitals in London. Those two hospitals were chosen because of their close locations to the chief investigator. Another reason for choosing them is that both of them are big Acute Trusts that have different departments and they use different EHR systems. Hospital A is an Acute Trust that employs around 2,400 member of staff; Hospital B is another Acute Trust that employs around 4,200 member of staff such as doctors, nurses, therapists and other health professionals as well as administrative and support staff. The interviews

were audio taped and prescribed. Five professionals were interviewed from hospital A and three professionals from hospital B as listed below:

Hospital A:

1- Clinical Director, Surgery.
2- Clinical Director, Ambulatory, Diagnostic and Therapies.
3- Head of Information inc. Coding and Patient Administrations System PAS.
4- Director of Training Programme, Lead Clinician, Chronic Pain Service.
5- Information Governance Administrator.

Hospital B:

1- Caldecott Guardian and Clinical Lead for Health Informatics.
2- Clinical Director, Medicine and Rehabilitation.
3- Director of Information and Communication Technologies.

To design a coherent set of questions to be asked in the interviews, different aspects should be taken into account, such as the role of the interviewee and what information is required for this research. Three groups of questions that should be explored with interviewees:

Q1-

1- What is the current EHR policy on security?
2- What do people/ stakeholders want? (Analysis of needs)
3- What is the security taxonomy that should be considered?

Q2-

1- To what degree EHR security can be accommodated?
2- How secure should the system be?

Q3-

1- How to design and implement secure EHR systems?

It was also useful to get an idea about the authorisation access levels of electronic health records and to know how patients' privacy can be protected; and to what

degree this should be protected and how this can be made reality. Some other example questions to be asked in the interviews include:

- Are patients currently able to control the access of others to their personal health records and to what degree?
- How can patients be informed about people who have access to their personal health records?
- How to offer differentiated authorisation levels for the various types of users?
- How should access to the records system be designed in order to provide de-identified records for research purposes?
- How should medical information be structured in the health record? Should it be according to the type of illness, the name of the specialist, or the GP? Which doctors or nurses will be able to access the full medical history of the patient, even if this is not related to his/ her specialisation?

For IT managers/ technical support staff

- How usable a smart card system could be for everyday practice? Can they propose any alternative?
- What concerns do they have about system security and data confidentiality?
- Is the available infrastructure sufficient for the implementation of the designed system?
  - If not, what additional infrastructure would they like to use/ see in place?
- Is the current EHR system well designed and technically sounds?
  - If no, how do they think the system should look like?
- Is the system compatible with other web applications? Does/should the system allow patients and doctors to have access to health records from other countries?
  - If yes, how should confidential data transmission is conducted?

For software providers

- How do they provide a secure health records system which satisfies doctors and patients?
- Do they consider all aspects of user rights in protecting patient privacy?
- Are they designing a flexible system which could be upgraded upon users' request?

Appendix (C) shows the final semi-structured interviews schedule as used in the interviews in the two hospitals case studies with considering the listed questions above for different users' groups.

3.2.3 Document analysis

Some documents were released by different organisations, such as Department of Health, NHS CfH, Ministry of Justice and International Organisation for Standardisation to define EHR systems deployment policies which are related to confidentiality and security concerns. These documents were analysed critically to show related parts that are important to protect the user's right for confidential and secure medical data. In addition, documents were supplied by the two hospitals (with permission) which were used to determine some current information security policies and a strategy for the coming years.

These documents are published from different organisations as mentioned before and they have different nature of contents. They include relevant International Standards that are listed in Appendix (E) and relevant British legislation Acts that are listed in Appendix (D). Furthermore, some documents that are published by Department of Health and NHS CfH such as some reports, leaflets, brochures and letters are listed in Appendix (G). In addition, other documents were analysed that are published by different independent or governmental organisations are listed in Appendix (I).

In this research, I had the chance to use some data from the Summary Care Records early adopters' evaluation report (Greenhalgh et al., 2008) with access to some interviews as I was a member of the evaluation team. The first year of "Early Adopters of the Summary Care Records (SCR)" evaluation used mainly qualitative methods, consisting of 1500 hours of ethnographic observation within NHS CfH and the "Early Adopter" sites (which are 5 PCTs that participated in the early phase of SCR implementation); 250 interviews with NHS staff; some 2500 pages of correspondence and documentary evidence; interviews and focus groups with 170 NHS patients and carers; and incorporation of relevant surveys and statistics produced by others.

3.3 Data Analysis

The data collected in the interviews were analysed in the following 7 steps, adapted from Creswell (2003), with additions from Miles and Humberman (1994):

Step 1: Transcribing the interviews.

Step 2: Reading the transcribed interviews to have an overall picture of the information.

Step 3: Making initial analysis by organising the material into 'chunks', before bringing meaning to those 'chunks'.

Step 4: Combining the features to form major themes or categories, and identifying connections between them.

Step 5: Determining a visualisation method to assist interpretation.

Step 6: Deciding on how the description and themes will be represented in the qualitative narrative, e.g. narrative passage, perhaps aided by figures.

Step 7: Interpreting the data and drawing conclusions.

3.4 Ethical considerations

This research had to go through the NHS ethical approval via the Central Office of Research Ethics Committees (COREC). A list of documents was required to apply to get the NHS ethical approval:

1. NHS research ethics committee application form, which is a 31 pages form.
2. Covering letter on headed paper.
3. Research protocol.
4. Summary C.V. for Chief Investigator.
5. Summary C.V. for supervisor.
6. Research participant information sheet.
7. Research participant consent form.
8. Statement of indemnity arrangements.

9. Letter from sponsor.
10. Letter from funder.
11. Two referees' or other scientific critique report.
12. Diagram (flowchart) of protocol in non-technical language.
13. Interview schedules or topic guides for participants.
14. Supporting letters from the two hospitals.

In addition, ethical approval from Brunel University was sought and granted. After submitting the above listed documents, a panel of twelve healthcare professionals interviewed the chief investigator before granting the ethical approval. Following the ethical approval, two different applications were submitted to the two hospitals to sign the research honorary contracts. The process to obtain the ethical approval took more than six months of the research time.

This research involves a qualitative research approach (i.e. interviews with doctors, nurses, IT staff, managers and patient group representatives). Participants were able to share their views and needs regarding information security in the EHR system they use. For this reason, all participants had the right to keep their information secure as it is explained below:

- Before any participant becomes a subject of research, he/she shall be notified of:

- The aims, methods, anticipated benefits and potential hazards of the research.
- His/her right to stop participation in the research and his/her right to terminate at any time his/her participation.
- The confidential nature of his/her replies.

Appendix (A) shows the Staff Information Sheet that been handed to the interviewees before taking part.

- No individual shall become a subject of research unless he/she is given the notice referred to in the preceding paragraph and provides a freely given consent that he/she agrees to participate.

The consent form is based on the outline as set out in the COREC "Guidelines for Researchers" document, and also includes a tick box for agreeing for the interviews

to be audio-recorded. Interviewees receive a copy of both the information sheet and the consent form for their own records. The used consent form is shown in Appendix (B).

- The identification of individuals from whom information is obtained in the course of the project shall be kept strictly confidential. Furthermore, all mentioned names in the interviews were coded. At the conclusion of the research, any information that reveals the identity of individuals who were subjects of research shall be destroyed unless the individual concerned has consented in writing to its inclusion beforehand.

- All data were processed in accordance with Data Protection Act (1998). No clinical data were held on any of the participants. Personal information such as names and contact details were stored on a secure database. All files relating to the interviews, electronic and hard-copy, were stored either on the secure server or in locked cupboard in the Chief Investigator's University office. Names of all participants and the organisations they work for were replaced with codes on all documents, and not to be mentioned in publications.

Summary

Overall, a major case study of the National Programme for IT (NPfIT) in England is used to be the container of other two sub-case studies in two different Acute Trusts. This approach allows for an in-depth view of human actions and interpretations surrounding the development and use of computer-based information systems. Such an approach helps in characterising the organizations' experiences in terms of processes of incremental or radical organizational change. A hybrid research method is used based on different research methods: participant observation and networking, semi-structured interviews, and documentary analysis.

Chapter Four

Understanding the NPfIT strategy for Information Security of Care Record Service

There is no one written strategy document that clarifies how information will be secured during and after implementing shared electronic health records in the National Programme for IT in England. This chapter focuses on providing an understanding of the NPfIT information security strategy as a key requirement in this research to achieve the research aim by identifying the different factors that could influence this strategy. Different information regarding information security in EHR in England was shared and published by NHS, and different visions and mechanisms were proposed to be in place when the NPfIT is being implemented. This chapter presents all captured information during this research that was given, published and presented by NHS CfH professionals from different and various sources, in an attempt to understand the NPfIT strategy for information security of the CRS in England.

4.1 An overview of Shared Electronic Health Records in England

The ERDIP programme was launched in April 2000 with four Demonstrator Communities (Cornwall, South Staffordshire, County Durham and Tees), chosen to pioneer the use of online health records and demonstrate how electronic records can be used to share patient information across health and social service communities (ERDIP, 2003). The Electronic Record Development and Implementation Programme (ERDIP) was established to provide the opportunity for in-service development and demonstration of best practice and progress towards shared Electronic Health Records (EHRs) (ERDIP, 2003).

Then the National Programme for Information Technology (NPfIT) was launched by Ministers in June 2002. Following the announcement of the Programme, the Department of Health (DoH) established a unit to procure and deliver the IT systems,

headed since October 2002 by its first Director General for National Health Service Information Technology (NHS IT). In April 2005 this unit became an agency of the Department of Health called NHS CfH (NAO, 2006).

The National Programme for Information Technology (NPfIT) in the National Health Service (NHS) in England is a ten year programme which presents an unprecedented opportunity to use Information Technology (IT) to reform the way the NHS in England uses information, and hence to improve services and the quality of patient care. The core of the programme is the NHS Care Records Service (CRS), which is planned to make relevant parts of patient's clinical record available to whoever needs it to care for the patient. The programme also includes many other elements, including X-ray accessibility by computer, electronic transmission of prescriptions, and electronic booking of first outpatient appointments (NAO, 2006).

The new IT infrastructure will link many different computer systems across the NHS in England and deliver (NHS CfH, 2005):

- The NHS Care Records Service (NHS CRS)
- Choose and Book, an electronic booking service
- a system for the Electronic Transmission of Prescriptions (ETP)
- a new national broadband IT network for the NHS (N3)
- Picture Archiving and Communications Systems (PACS)
- IT supporting GP payments, including the Quality Management and Analysis System (QMAS)
- Contact- a central email and directory service for the NHS.

The NHS CRS is supposed to enable each person's detailed records to be securely shared between different parts of the local NHS, such as the GP surgery and hospital. Patients will also be able to have a summary of their important health information, known as their Summary Care Record available to authorised NHS staff treating them anywhere in the NHS in England. Patients will be able to register to access their Summary Care Record using secure HealthSpace website (NHS CfH, 2008).

The NPfIT programme was divided into five clusters as shown in Figure 4.1:

- North West, West Midlands (population 12.3 million, NHS staff 276,000)
- North East (population 7.5 million, NHS staff 170,000)
- East of England, East Midlands (population 9.5 million, NHS staff 174,000)
- Southern (population 13 million, NHS staff 249,000)
- And London (population 7.2 million, NHS staff 165,000).

For each cluster, a different Local Service Provider (LSP) was contracted to be responsible for delivering services at a local level. This structure was intended to avoid the risk of committing to one supplier which might not then deliver; by having a number of different suppliers implementing similar systems in parallel, a degree of competition would be present which would not be if a single national contract had been tendered. However, in July 2007 Accenture withdrew from the project, and in May 2008 Fujitsu had their contract terminated, meaning that half the original contractors had dropped out of the project. As of May 2008, two IT providers were LSPs for the main body of the programme.

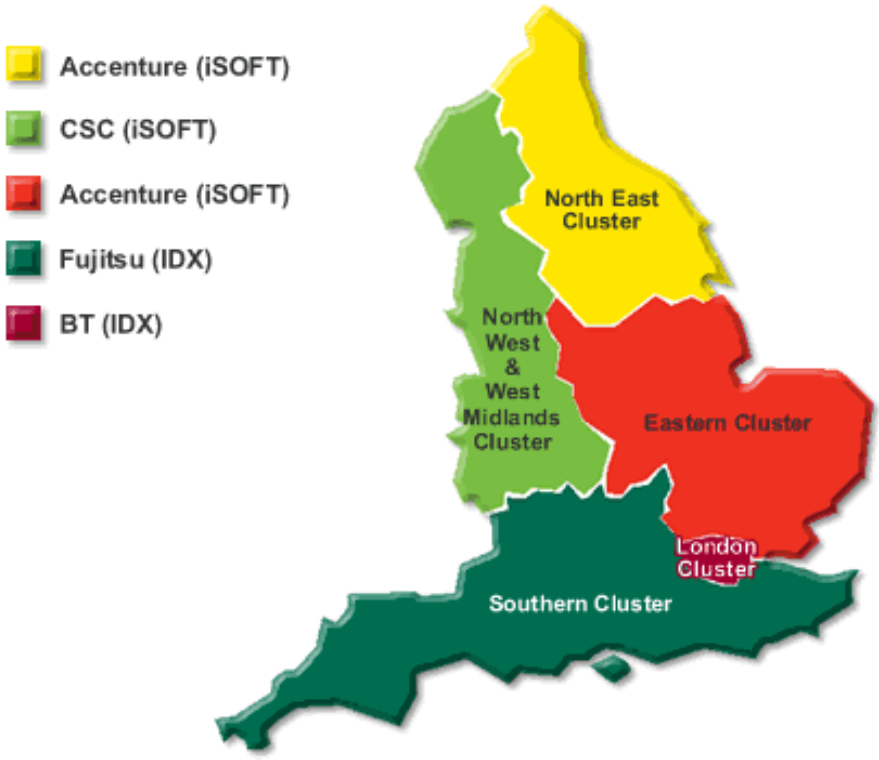

Figure 4.1: The five clusters of the NPfIT

Then, the National Programme for IT operates in England and the country is split into three Programmes for IT, each of which is hosted by the strategic health authorities and has a Local Service Provider (LSP) as shown in Figure 4.2:

- London Programme for IT (LPfIT): BT
- North, Midlands and East (NME) Programme for IT (NMEPfIT): Computer Sciences Corporation (CSC)
- Southern Programme for IT (SPfIT): Fujitsu

Figure 4.2: The three Programmes for IT of the NPfIT

In one of NHS CfH conferences in November 2007 they presented the strategy roadmap of the NPfIT from 2000 to 2012 as it shows in Figure 4.3 and they titled it "*We have a clear direction for the overall journey.*" This vision includes NHS CfH plan about "reform" journey, centre's "leadership" journey, and "service" journey. It also presents some expected key outcomes, such as:

- In the early stage of the NPfIT (around 2002): Key illnesses, throughput, and capacity.
- In a later stage (2006): Health priorities, waiting times, and financial stability.
- In the semi-final stage (2010): Quality, safety, responsiveness, and joint up care.
- In the final stage (2012): Health & well being and equity.

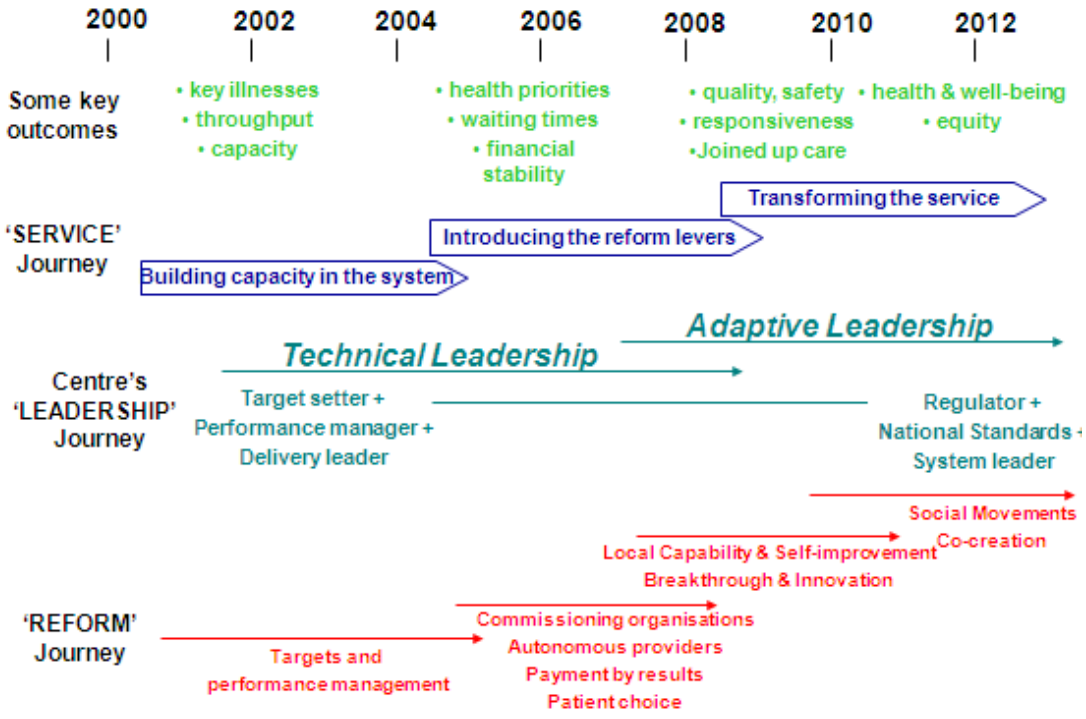

Figure 4.3: The direction of the overall journey of the NPfIT (Thick, 2007)

4.2 Care record service (CRS) design

NHS CRS is designed, according to NHS CfH, to enable each person's detailed records to be securely shared between different parts of the local NHS, such as the GP surgery and hospital. The access process design as proposed by NHS CfH is shown in Figure 4.4.

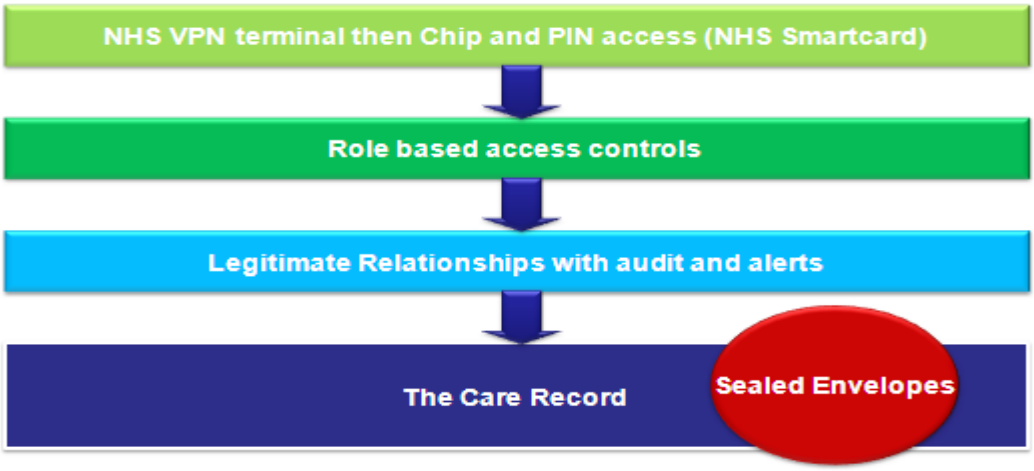

Figure 4.4: The access process (Eccles, 2007)

NHS health carers will be able to access patients' health records by using their NHS smart cards with chip and pin access mechanism through NHS VPN terminal.

Access will be granted according to role-based access controls with legitimate relationships between health carers and patients. With this process, an audit and alert procedures will be running to access the care records of patients.

To limit access to sensitive data, NHS CfH proposed a mechanism to ensure confidentiality of patients' information within the NHS Care Record Service which they called it "sealed envelopes", it is going to be explained in more details later. NHS CfH plan to obtain a secure shared electronic health records system was presented in different NHS CfH events such as (meetings, conferences and workshops) that are listed in Appendix (F), and in different (documents, leaflets, CDs and brochures) that listed in Appendix (D).

4.2.1 NHS smartcard

A smartcard is a creditcard-sized plastic card (see Figure 4.5), containing an electronic chip for security. It is printed with the health carer name, photograph and unique identity number (UUID).

Each trust and PCT is responsible for setting up a Registration Authority (RA) to issue NHS smartcards and manage the registration process.

The registration process was set to ensure:

- Identity is confirmed beyond reasonable doubt to a government recommended standard (e-GIF level 3) (Cabinet Office, 2010).
- Allocated access control according to job role and duties.
- Passcode is set by individual, which must not be shared.

Figure 4.5: NHS smartcard

4.2.2 National Network for the NHS (N3)

British Telecommunication (BT) was awarded the N3 contract on February 19th 2004 and acts as a network integrator. The service replaces NHSnet.

Primary Care Trusts (PCTs) and practices can get branch practices connected to the network and use N3 Virtual Privet Network (VPN) services to provide a secure network between GP practice and its branch surgeries.

4.2.3 Access Control

Access to NHS CRS data (held by the Personal Spine Information Service) is controlled by the Access Control Framework which registers and authenticates all users.

It will provide a single log-in and a record of each healthcare professional accessing a patient's NHS Care Record. All information will be provided on a need-to-know basis and based on a user's role and 'legitimate relationship' with the patient.

It will store details of those relationships between healthcare professionals and patients, as well as patient preferences on information sharing (e.g. whether certain sensitive information is restricted from routine sharing).

4.2.4 Legitimate Relationship

Legitimate Relationship is the concept of only allowing NHS health carers to access patient clinical data with the view to providing healthcare. A 'Legitimate Relationship' (LR) reflects the fact that a member of staff from a service organisation may be involved in the care and treatment of a particular patient, or has some other direct relationship with the patient that justifies access to that patient's records.

The Legitimate Relationship Service (LRS) provides a mechanism for setting up and maintaining legitimate relationships between NHS personnel and patients. The LRS is a centrally managed service residing on the BT N3 network and applications which are part of the NHS Care Records Service (NCRS) must utilise it in order to comply with NHS CfH Access Control Framework (ACF) guidance. An NCRS user is unable to access a patient's clinical record without a Legitimate Relationship.

A Legitimate Relationship will normally be created transparently for a user as part of the usual workflow within NCRS applications, for example, when a GP refers a patient to a hospital clinic, the recipient application will automatically create a Legitimate Relationship (in this case it is a Referral LR that is created) for the Workgroup associated with the clinic team.

4.2.5 Alerts

Alerts are used to alert a privacy officer in a healthcare organisation in situation where there is questionable appropriateness of user access.

4.2.5 Audit trails

Records made when a patient's record is accessed, which are available to patients on request and to privacy officers for investigative purposes.

4.2.6 Sealed Envelopes

Sealed Envelopes is a mechanism was proposed by NHS CfH to ensure different access control levels when the detailed health record system is in place. This access mechanism assumes that patients, and/or their authorised representative(s), in consultation with their clinician(s), will be able to (NHS CfH, 2006b):

- Identify one or more sets of sensitive information, see Figure 4.6 for different sets of EHR systems, which should be sealed from everyone other than the author and people in the same Workgroup as the sealer;
- For each set of sealed information, decide whether people other than the author and those in the same Workgroup as the sealer could ever gain access:
    - If "sealed", the information could be made available to users outside the Workgroup with the patient's permission, or through override in exceptional circumstances (e.g. public interest); or
    - If "sealed and locked", users from outside the Workgroup would be unaware that the sealed information existed;
- change their minds at any time and change or remove one or more of the restrictions.

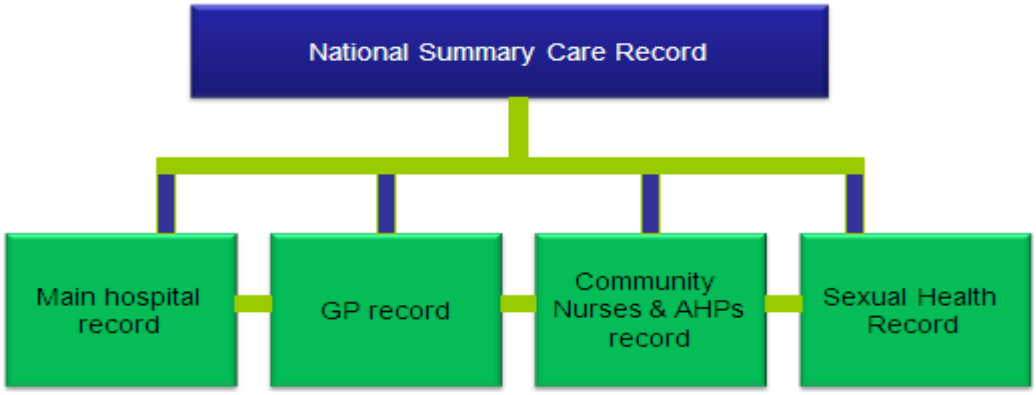

Figure 4.6: Sharing between different EHR systems (Eccles, 2007)

4.2.7 The consent model

In the SCR, the approach for individuals to participate is on an opt-out basis. That means that the patient's record would be uploaded to the spine unless the patient actively did something to indicate otherwise.

The advantage of the opt-out approach is that a greater coverage of the health system will be achieved and more people will end up on the system. In addition, more comprehensive data will be available for health care. The disadvantage is that the patient doesn't make an active choice to make his/her health record available on the system (HealthConnect program Office, 2002).

When the programme was implemented, patients were given three options to store and share their EHR information; these options are:

- **Store and share**: This option is available to clinicians via SCR which is visible to an authorized user, with legitimate relationship to that patient. For patients, their SCRs are visible to them via HealthSpace.

- **Store but don’t share**: For clinicians, SCR will exist but will not be automatically visible to any authorized user. The patient may give a clinician permission to override the share status and view the record. The status can only be overridden with a court order or statute. For patients, SCRs are visible to them via HealthSpace.

- **Don’t store and don’t share**: This occurs when the patient decides to opt out. For clinicians, via SCR, a blank summary is created, stating that the patient didn’t want to have a SCR. Even if the consent status is changed to share, no data is available to be viewed. For patients, via HealthSpace, no clinical data is available. A note confirming this choice is visible.

These options were changed after the first year independent evaluation for early adopters of the SCR in (2008) to be only two choices:

- **Store but don’t share**: In this case, consent is requested in order to view, patients need to give their consent at every time a clinician needs to access to the patient’s record.

- **Don't store and don't share**: This is when patient decides to opt out of the national system.

The Care Record Service (CRS) in England is designed to have different sharing levels. Each sharing level is supposed to have different consent mechanisms.

When records are being shared within the clinical department, different information from different sets is being shared. For instance, three sets of information are shared (see Figure 4.7):

- The clinical notes investigations, results, and treatment.
- Administrative record and demographics information.
- Administrative record, appointments and letters.

The consent to access and share this information in this case is implicit because the three sets of information exist in the same record system.

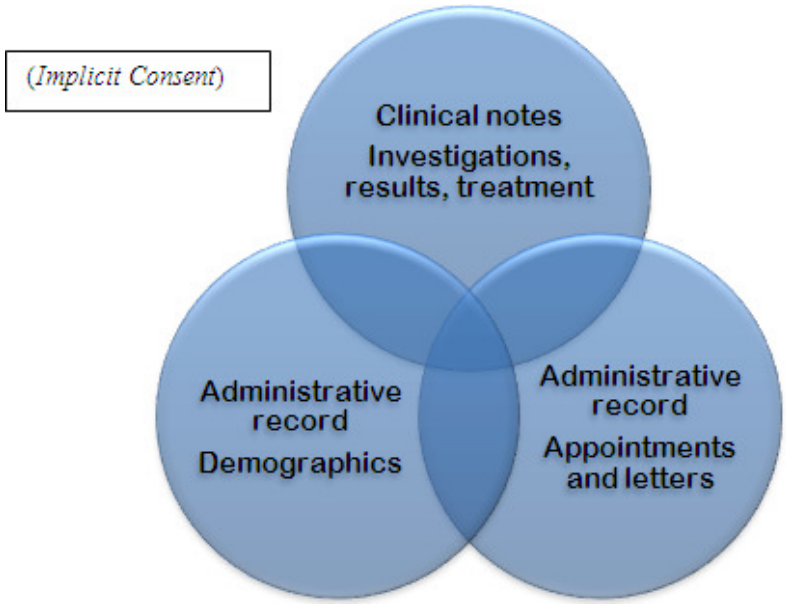

Figure 4.7: Sharing records within the clinical department (Ahmed and Smith, 2007)

When the records are being shared within an Acute Trust, which is a secondary care organisation, usually three different record sets are being shared (see Figure 4.8) mainly:

- Investigations and results with labs/other departments
- Treatments with pharmacy and other departments
- Anonymous activity reporting to Trust management

The consent to access and share this information in this case is implicit even if the three sets of records exist in separate record systems and could be integrated in one clinical notes system.

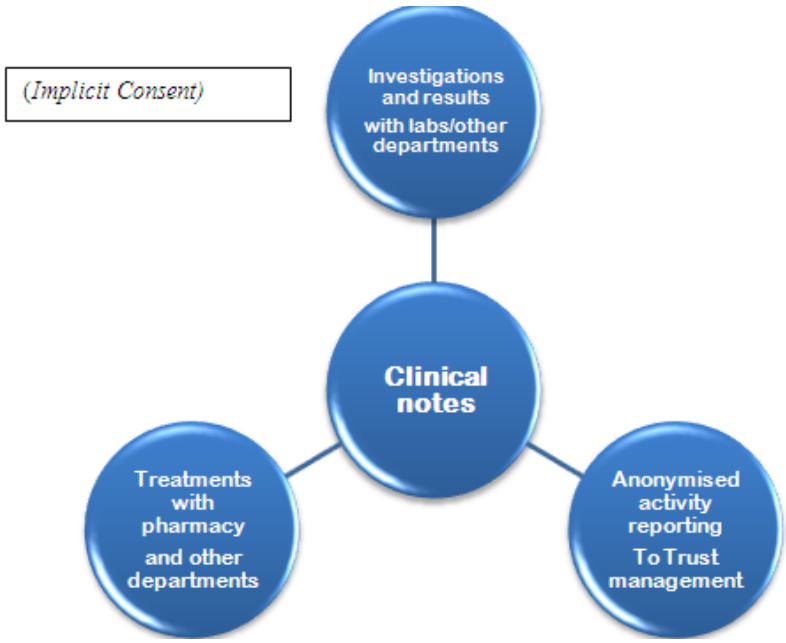

Figure 4.8: Sharing records within an Acute Trust (Ahmed and Smith, 2007)

The consent to access and share information is explicit, when clinical records are being shared outside the provider organisation (see Figure 4.9), as when sharing is between:

- General Practice.
- Statutory grounds (consent is not essential).
- Other healthcare providers.
- Referrals to secondary/tertiary care.

Clinical records are anonymised and the consent to access and share the information is implicit when clinical records are accessed and shared with other organisations and for different uses (see Figure 4.10), such as:

- Epidemiology
- Commissioners
- Secondary Uses Service (SUS)

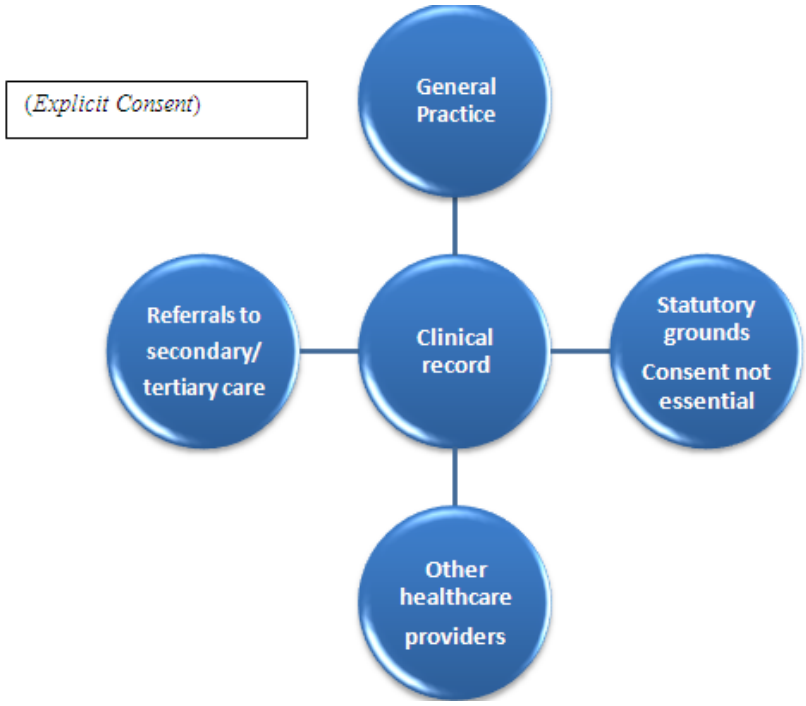

Figure 4.9: Sharing records outside the provider organisation (Ahmed and Smith, 2007)

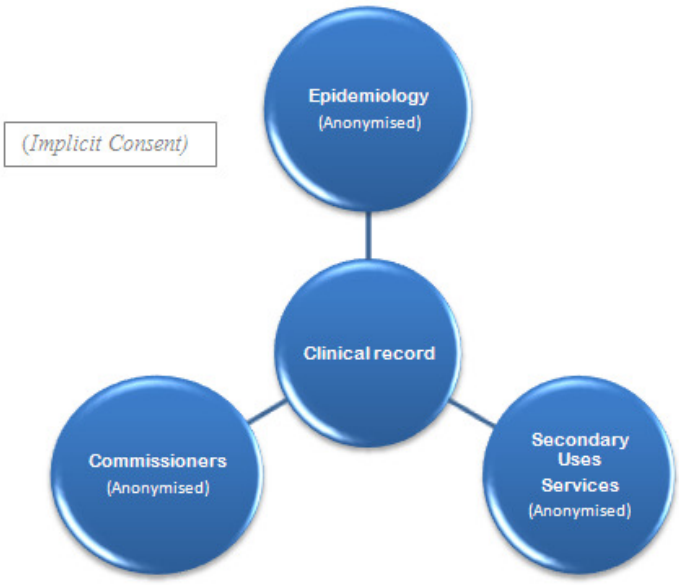

Figure 4.10: Sharing records outside the provider organisation (Ahmed and Smith, 2007)

4.3 Relevant documents

4.3.1 Information Governance

NHS CfH website (http://www.connectingforhealth.nhs.uk/) provides information about what Information Governance is and what it includes.

It defines the Information Governance (IG) mission, which is to ensure necessary safeguards for, and appropriate use of, patient and personal information. IG includes key areas ,which are:

- information policy for health and social care,
- IG standards for NPfIT systems
- and development of guidance for NHS and partner organisations.

The Information Governance Statement of Compliance (IGSoC) is "*the agreement between NHS CfH and Approved Service Recipients that sets out the terms and conditions for use of NHS Connecting for Health services, including the N3 network, in order to preserve the integrity of those services whether this use is directly or indirectly"* (NHS CfH, 2007).

The IGSoC includes (NHS CfH, 2007):

- The requirement that no patient identifiable data or other sensitive data be stored or processed offshore, where the location is deemed non-compliant with the NHS CFH Offshore Policy
- The right to audit by NHS CfH or nominated third parties
- Change control notification procedures and approvals processes
- The requirement for organisations to achieve, or be working towards, ISO27001 (see later in section 4.3.3)
- The requirements for reporting security events and incidents.

A published document, called "IG Toolkit" (DoH, 2007) should be considered, which includes Information Governance standards and guidance for the NHS and partner organisations.

NHS IG defines confidentiality in terms of:

- standards of practice for confidentiality, and
- patient consent to information sharing.

IG assures that health records are confidential as they should be shared only on a need-to-know basis. NHS CfH introduced national standards so that all of its systems can protect the confidentiality of patient information and provide access to relevant information to those who need it. For this reason IG considered two key patient confidentiality issues:

-Patient choices: which is mainly information on some of the choices available to patients to control access to confidential information; and

-Information Governance alerts: where are triggered when specialist staff need to be informed of questionable access, and there is someone viewing a confidential patient record and he is not entitled to do so.

IG Toolkit listed different documents that guard information sharing in EHR systems. These documents are:

4.3.2 The Care Record Guarantee

This document describes how patient information is protected and used. The NHS (National Health Service) Care Record Service (CRS) in England set the Care Record Guarantee to form an important part of the public information campaign about NHS Care Records and to cover people's access to their own records, controls on others' access, how access will be monitored and policed, options people have to further limit access, access in an emergency, and what happens when someone cannot make decisions for themselves. However, this document is still general and it looks at how access rights should be. It does not explain the details of how to keep these records confidential and secure in case of intended abuse. Hence, a well-defined security strategy that is acceptable to all key stakeholders is lacking.

4.3.3 Standards and guidance

NHS CfH has a range of standards to ensure that information is processed securely and with proper regard for its confidentiality, integrity and availability.

NHS CfH recommends the ISO 27000 series to be used in practice. These standards have been specifically retained by the International Standards Organisation (ISO) for information security issues. A list of ISO standards that concerns information security and data protection is shown in Appendix (E). The ISO 27000 series includes a range of individual standards, each one targets various information security controls (NHS CfH, 2010). The aim of the ISO 27001 standard is to "*provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System*" within the context of the organisation's overall business risks. This standard was published in October 2005, essentially replacing and enhancing the content of the old BS7799-2 standard. The ISO 27001 standard defines its process approach as "*The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management*". It employs the PDCA, Plan-Do-Check-Act model to structure the processes (NHS CfH, 2010).

It is a strategic decision to adopt the ISO 27000 series of standards. It is recommended that working towards and, in turn, being certified to the ISO 27001 standard will help manage and protect valuable information resources. Organisations, including health organisations, must prove they are compliant or working towards compliance to show that information security is being considered seriously and that effective steps to information security are in place. This also gives confidence to interested parties.

An Information Security Management System (ISMS) is a basic requirement for compliance with the ISO/IEC 27001 standard. This must be in place in order to provide an appropriate level of governance for the services provided by an organisation. It is recommended that all organisations using NHS CfH digital services and/or have an N3 connection have a corporate document that describes their organisation’s ISMS as a part of their data accreditation process (NHS CfH, 2010).

ISO 27001 is applicable to all types of organisations consuming NHS CfH digital services and who have an N3 connection (e.g. Acute Trusts, Foundation Trusts, County/City Councils, GPs, Commercial Enterprises, Government Agencies, not-for profit organisations). It defines requirements for the implementation of security controls customised to the needs of individual organisations or parts therefore. The standard considers the protection of critical information, such as in the health sector (NHS CfH, 2010).

The standard should be supported by the entire organisation through education, training, communication and awareness of comprehensive security policies and procedures, and should be controlled by professionals who are responsible for Information Governance within the organisation, either the health organisation or the technology and networking provider organisation. ISO 27001 is also highly effective for organisations which manage information on behalf of others, such as IT outsourcing companies. It can be used to assure customers that their information is being protected (NHS CfH, 2010).

4.3.4 Legal Acts

A list of relevant legal acts is shown in Appendix (D) that concerns sharing medical information and accessing health records.

Data Protection Act (1998) defines health information as “personal data”, and health records are considered to be under “accessible records”. In this Act, in Schedule 3, Section 4(3), for processing of sensitive personal data, that the data subject (the patient) has to give his/her explicit consent to the processing of his/her personal data, and access process must be carried out in the course of its legitimate activities by anybody. However, in the same section, Article 8 says that if it is necessary for medical purposes, access process is allowed by a health professional without explicit consent.

On the other hand, Freedom of Information Act (2000) exempts sharing some information, such as health and safety information and personal information. While the Access to Health Records Act (1990) includes provisions about:

- Right of access to health records.
- Cases where right of access may be wholly excluded.
- Cases where right to access may be partially excluded.
- Correction of inaccurate health records.
- Duty of health service bodies to take advice.

The Access to Medical Reports Act 1988 allows individuals to see medical reports. However, in certain circumstances the patient may be prohibited from viewing all or part of the report if:

- In the opinion of the doctor, viewing the report may cause serious harm to the patient.
- Access to the report would disclose third-party information.

Summary:

The NPfIT doesn't have a single document for information security strategy, but there are different information security artefacts (documents, presentations, etc.) that are being presented in different occasions such as access control, sealed envelopes, consent mechanisms and different standards and legal acts that govern information security and information sharing protocols in general and in the health sector in particular. This chapter has attempted to put together and to make some sense out of the different information security artefacts that have been published, discussed, or proposed in the NPfIT. The different information security issues were highlighted to understand the NPfIT information security strategy and make it available for later discussion and analysis to determine the different influential factors.

Chapter Five

The influencing factors on designing an information security strategy for EHR systems

In the previous chapter, the current status of information security strategy in the NPfIT was demonstrated. To place the strategy in a more coherent frame, NHS visions and plans were gathered from different resources. In this chapter, the factors that influence the implementation and development of an information security strategy for electronic health record systems are identified and discussed. This discussion shows how these factors were determined by including points of view of NHS professionals who were interviewed, and opinions that focused on the NPfIT in newsletters such as E-Health Insider (http://www.e-health-insider.com/).

The identification of the various influential factors was done by analysing the research data by classifying name categories, asking stimulating questions, making comparisons, and extracting innovative, integrated, realistic themes from a mass of unorganised raw data. Data resources were interviews, documents, news articles, and workshops and conferences discussions and presentations. These sets of information were thematically analysed by combining and cataloguing related patterns into sub-themes. These sub-themes were derived from patterns, such as (meanings, conversation topics, feelings etc.); while non-relevant fragmented ideas were filtered out of the themes. The influencing factors were defined, by combining the sub-themes in different categories, to be:

1- Political
2- Financial
3- Technical
4- Social
5- Legal
6- Clinical

Each factor influences the building of information security strategy in EHR systems is explained in this chapter (See Figure 5.1). Later, it is argued that the political factor is the most powerful factor of all the six factors.

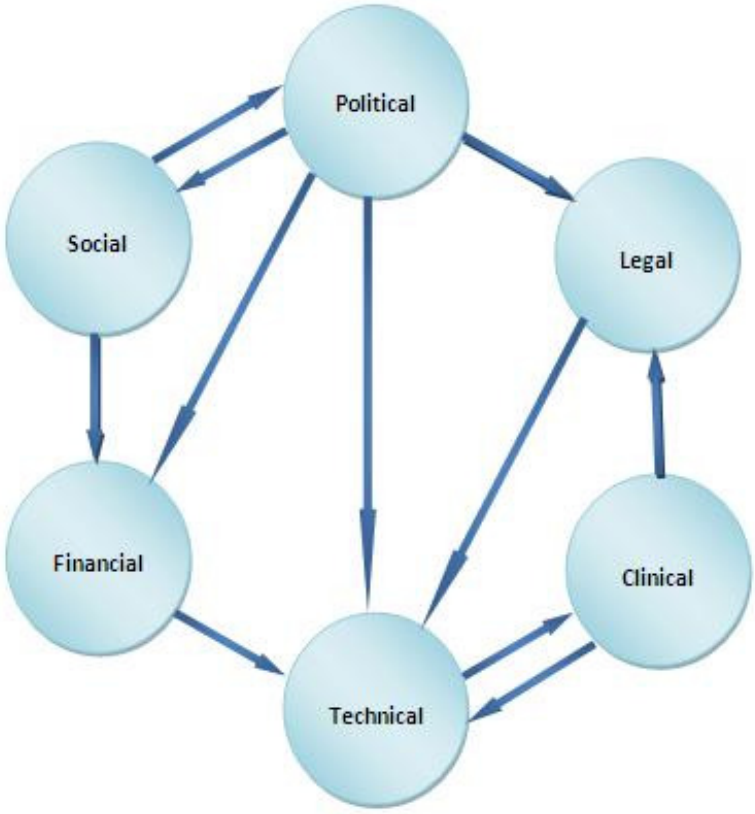

Figure 5.1: The influencing factors

5.1 Political

The political factor is vital for any plan that has been made by the NPfIT. In fact, the project itself was proposed by political bodies following the General Election of 1997 when the Prime Minister proposed "*The challenge for the NHS is to harness the information revolution and use it to benefit patients*" (NHS, 1998). Any organisational changes in this project were led by Department of Health. The funding for this project is drawn from public taxation and the priority in spending money was set according to political views. Furthermore, relevant legislations were set in British law, based on political will.

Very recently in September 2010, following the General Election of 2010, the Health Minister has announced that the National Programme for IT in the NHS is centralised and national approach is *"no longer required*" and trusts will instead be

able to operate "*a more locally-led plural system of procurement*" (EHI, 2010l). The Minister added "*Improving IT is essential to delivering a patient-centred NHS. But the nationally imposed system is neither necessary nor appropriate to deliver this*" (EHI, 2010l). The change of the Government has a very significant impact on how the national EHR system is going to be, or not to be.

An interviewed clinical lead in NHS CfH explained how the consent model has been decided and how the political factor is steering the project

> "*The decision of opt out model was first made by the National Clinical Advisory Board. When the NPfIT started that was the first governance board. Then the Care Record Development Board was chaired by AA. Because of so much discussion and unhappiness about the opt out in some parts of the world and some parts of England, they revealed the decision and they asked the ethics sub-groups chaired by BB. and they confirmed the position of opt out. Then the minister asked AA. to look at the decision in June. And November 2006 they reconfirmed the opt out position and asked for the independent evaluation.*"

Some clinicians are dubious about the political influence, but they think that for an individual clinician, not with national access to the EHR systems, which are available in hospitals, the system is brilliant. The Director of Training Programme, Lead Clinician and Chronic Pain Service in Hospital A said

> "*Personally I've said that I don't want my records on it, because of political aspersion, and because I don't trust the Government. I don't think it's essentially seen as a totally secure system and I think the Government will use the information for its own purposes. It should be perhaps quite separate from the individual's healthcare; you know which is what they are sliding up for.*"

He added, according to his thirty seven years medical experience, that the number of times he needed instant access to a patient's complete health record could be probably counted on one hand

"*Probably it wouldn't even fill one hand. It's not something which is needed from the point of view of medical care. It's a political device. That's my fixed and perhaps deluded view*"

Some interviewees believe that national EHR system, which in their view has been brought forward by the Government without any discussion with people about what its ramifications are and it is being sold as something which, without being piloted or tested, would be of benefit to individuals in the health service. As there was no explanation of the fact that it may put people at serious risk of having their privacy invaded by the Government. As a clinician believe "*the more you stretch it, the more you get holes in it*" (See Figure 5.2).

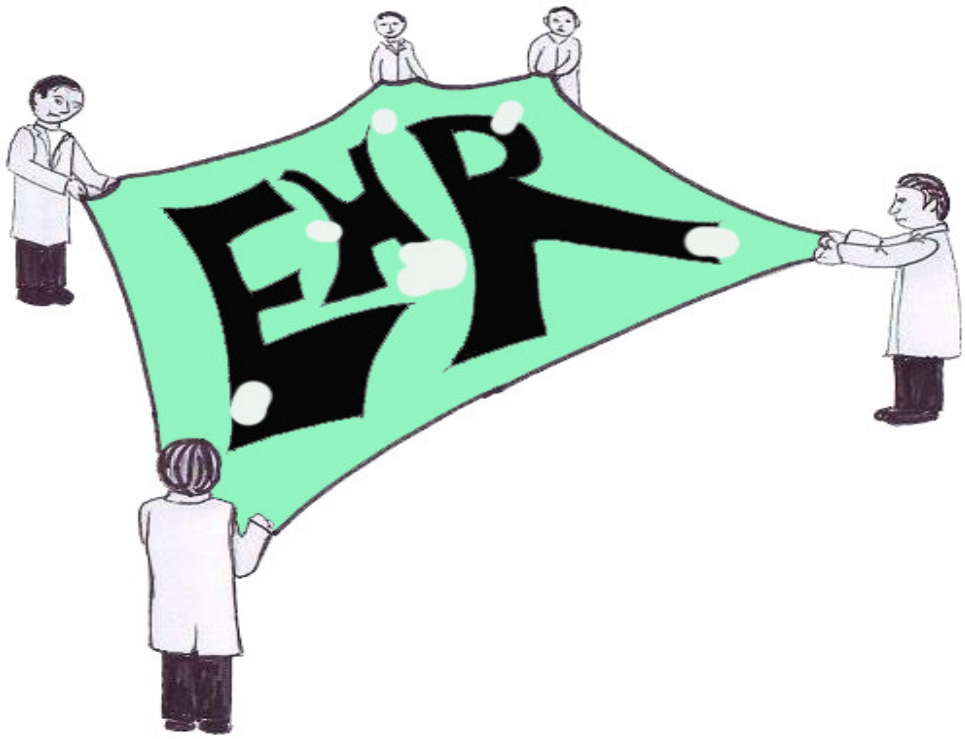

Figure 5.2: The more you stretch it, the more you get holes in it

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A expressed his concern about using a shared EHR system for patients' benefit, by saying:

"*It should only be used for their benefit. And there is a serious lack of definition between what is the patient's benefit in terms of his health on*

> *that day and his health as a member of an amorphous mass people. That is increasingly controlled by a democratic western government.*"

There are different views on who should lead the decision making to set information security policy. Most of the views of the interviewees showed that it should be a combination at different levels. It is believed that national policy should be created locally with broad national guidelines. Some clinicians believe that decision making should come from the Department of Health "*because ultimately the Department of Health is responsible for the whole thing*".

Some clinicians believe the decision was too IT oriented "*decision making has not been from the clinical side, but from the IT side*".

On the other hand, a clinician had an opposing view about decision making in information security policy

> "S*omebody in IT or in charge of IT will know more about the national picture of the national agenda and how we would get from A to B. And this information needs to be passed down and they need to be able to tell them up what our problems are.*"

5.2 Financial

The NPfIT project is funded by the NHS and the NHS gets the money from public taxation. At the end, the funder is the public. The Information Governance Administrator in Hospital A said

> "*It is the biggest IT project, and the NHS are trying to do it, it is a bit of a worry. And that's gone up hugely from the original estimates. So hopefully there will be something that is coming out of it in the end.*"

The financial factor mostly affects the infrastructure of the system, in term of hardware, software, system design and space. Most interviewees had the view that the available infrastructure is not enough to obtain a satisfactory level of information security when accessing health records in practise. The head of Information inc. Coding and Patient Administrations System (PAS) in hospital A said "*locally it has been put together in a piecemeal fashion; not all systems are connected to each*

other". It is thought not good in term of integrated health records as the CfH solution is built Top-down rather than bottom-up; in theory, it should be integrated by taking only the good local systems and integrate them in a national system.

The Clinical Director, Ambulatory, Diagnostic and Therapies in Hospital A said

> "*There has to be balance between too much individualising and you have so many systems they cannot talk to each other. And the biological [biometric] access is not in place. In terms of speed of connection, it is still very slow; I suppose there should be a huge server that bears care records and everybody can go in and fish out what they need*."

The Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B said

> "*We don't have enough in terms of hardware. If there is one PC in a ward someone may have been looking on your shoulder, which of course may breach confidentiality. If you are writing down patient's notes in a public area as only one PC available; we just don't have the hardware infrastructure."*(See Figure 5.2).

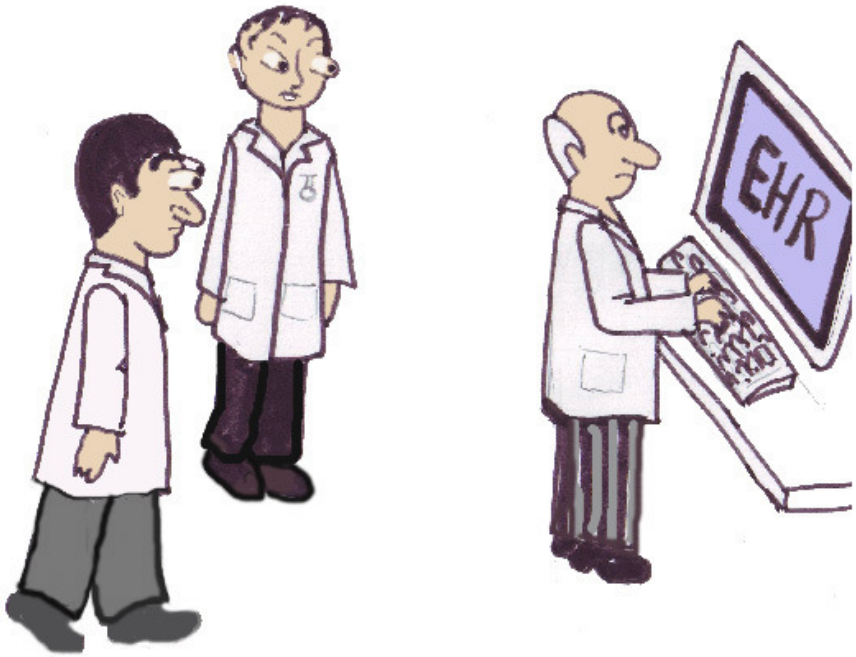

Figure 5.3: Indirect intrusion on patient privacy

> Another problem was the lack of compatibility between old and new systems. It costs a lot of money to transfer data between them as the Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B said:
>
> "*The problem is all manufacturers of the legacy systems are protected in their data format. As they say, we can do that [transferring data] but it will cost you £50.000. I wonder what it should be so expensive to swap data from one format to another. So getting machines to talk to each other is a real problem.*"

The other problem that has been noticed by health carers in the national system is to do with the sustainability of EHR systems. A lot of clinicians have spent a lot of years trying to get their individual systems working and they have bought in packages. After a while because of the companies which help them are not big enough and good enough to sustain them. So technically, they tend to become unwieldy instead of integration, bits are added on. In this case, clinicians get more interfaces and eventually the systems just die out because they are too slow and they can't be maintained. This causes some problems on the scale of the national project as it wouldn't be sustainable and will actually either completely collapse or break up into lots of separate little bits, as people tag on separate solutions for their own needs.

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A said

> "*You know DD. Bank can change their IT systems whenever they like, but I don't think the health service is going to be capable. Well, we would need a lot more hardware for a start. We need a lot more resources for training people. We probably need to spend six percent or more on new hardware or training programmes. Just to make it more!*"

5.3 Technical

The technical factor could be seen from different aspects such as training, usability, data quality, availability and technical support. Each aspect has different influence of information security of EHR systems.

5.3.1 Training

Training on systems that don't yet exist doesn't make sense. Even training should be provided in a continuous manner. No gap should exist between training on a system and using the EHR system. The importance of training comes from the need to merge new technologies efficiently into the working place.

> "*You can put everything in place but it comes down to people doing what they're supposed to do. So it is very important that people are trained.*"

> "*The assumption that a lot of us know how to use the system, Windows based system and to get the information so the training was supervision how to log on and how to use the basic features.*"

> "*No, I don't think you could ever have sufficient training. I think you probably won't get fully trained until you've got it in your office, because the potential functionality of it is so enormous*."

In healthcare organisations everybody signs the information security policy; however, it is not guaranteed that they read it. For this reason face to face training is quite important. The Information Governance Administrator in Hospital A said:

> "*Information governance training has been sadly lacking. At the moment we give information governance training at the common start date. We do all through it on an on-demand basis, so we are happy to go out and talk to departments, team meetings and things, but there is a gap really. when I go and talk to people and give them the training and talk to them about information governance and related legislation, data protection and the code of confidentiality, they're all, they are aware of it but you*

do get a 'oh I say' you know reaction and 'oh I didn't know that, I didn't know I was supposed to do that', so I think it needs strengthening."

Another way of training is via e-learning modules such as the tool that has been launched to support national standards for hospital record keeping. The online tool allows users to complete training on two modules; one covering the principles of good record keeping and one covering the standards for hospital admission clerking, inpatient handover and hospital discharge (EHI ,2010k).

5.3.2 Usability

Some clinicians find the EHR system good in term of usability, but there are other people who would find it very difficult. It could be a big transition for doctors who are used to sit with a patient and a piece of paper in front of them. They need to change their consultative practices and they have to get used to using a keyboard and a computer for real-time data entry. For this reason a lot of people are inhibited by technology. For instance, many clinicians forget about the available functions in the EHR software in their office. They are not used to sit tracking results, tracking patients, taking actions or reviewing work. They have to wait for piles of notes, while everything is available by a few clicks and the whole patient record is available to them.

Some professional believes that the proposed national system is not what they really need. Some clinicians find it not easy to have to log in with passwords. While others find the incompatibility between different systems is a problem in every day practice.

"*What they are offering at the moment is not what we need in the integrated system.*"

"*In electronic care records, it makes it more difficult by having a key to login.*"

"*I would like to have systems that do communicate with each other not put me in complete isolation, but the system should have enough flexibility to individualise that system.*"

The Information Governance Administrator in Hospital A said

> "*Electronic systems are supposed to speed things up and make things easier but the doctors are saying it doesn't, because they have got to go and sit at the terminal and do it. I suppose you would have to have similar sort of security to have, that you do with your online banking really. I mean online banking, they keep making the security tighter and tighter on that don't they and I have one of these pin sentry things, card reader that you use to log on, whereas it used to be, you had a unique word or unique number and you had to do all that, so I guess that's the sort of thing they could do.*"

5.3.3 Data quality

Operationally, some departments are still using manual systems because the quality of the data run in electronic systems is not good enough, or the systems is not developed enough to enable them to use the system efficiently and effectively.

A big part of data quality programme is change management. It is about ensuring that the right operational staff out there in their job description that they need to be using the system and they need to make sure that quality and security of the data is good and they trained in it

> "*Because at the moment the job description doesn't necessarily reflect this and there is not enough staff to use it.*"

The head of Information inc. Coding and Patient Administrations System (PAS) in hospital A said

> "*If or when we end up migrating to NPfIT system we have to make sure that our data is very clean; system managers are directly involved in data quality of their systems.*"

The Director of Training Programme, Lead Clinician, Chronic Pain Service in Hospital A said

"*Data quality is a very, very variable thing in clinical practice. What I'm much more concerned about clinically is that the correct... the data should be complete.*"

5.3.4 Availability

It is believed, if the system works, it will be ideal because having information on a central database server means that a patient gets taken ill somewhere further away, they can access the important information about him/her and they can give him/her good treatment there and then. On the other hand, some healthcare professionals showed their concern about the ability of accessing data when the patient is unconscious such as the Information Governance Administrator in Hospital A who said:

"*If you were unconscious and you can't say, get me to a terminal and I'll log on. I suppose unless there's any ID on the patient, I suppose. Especially if they've come from an accident where they did have, the lady had her handbag; it might not be with her anymore. DNA database is a good idea because you can't assume that people will have ID on them; that was good enough to be able to exactly know who they are.*"

The head of Information inc. Coding and Patient Administrations System (PAS) in hospital A said "*Availability and access would be a concern for me. When the information on the spine whether it will be available when they need it in the right time."*

The Clinical Director, Ambulatory, Diagnostic and Therapies in Hospital A explained an experience with data loss in the hospital while the backup files were on the same broken down server

"*A person with experience in pathology has worked with the system since implemented, there are a lot of breakdowns, people are not got to use the system, things were not supposed to happen like the system was supposed to be mirrored but the mirroring was in the same server, for instance, and when the server went down, the mirroring went down."*

This incident caused a period over a year and a half with the system being down and not being stable for that period of time.

Similar views were voiced by the Clinical Director, Medicine and Rehabilitation in Hospital B who believes that the breakdown procedures are not enough

> "*The reliability of IT, at the moment, cannot be guaranteed. We can lose patients' data. When this happens, we have downtime procedures, but they are not totally reliable. It is not a very friendly system, it takes about 25 minutes for each patient and the other paper system would be done in about 10 minutes.*"

Health carers have concerns about reliability, but they believe if security could be guaranteed, the GPs in particular and patients' representatives would be considered and could be reassured, then obviously there are a lot of potential advantages. If they have a paperless system, and the system breaks down, then they are in a real mess.

Some healthcare professionals suggested that people could wear an electronic version of bracelets around their neck, if they have particular health problems like the microchip animals. And they believe it is fiction now, but they think it can be a possible solution for future.

5.3.5 Technical support

Clinicians don't believe that they get the sufficient and reliable technical support and they believe that clinicians are the less informed and involved in what they really need as was seen in both hospitals.

The Clinical Director, Ambulatory, Diagnostic and Therapies in Hospital A said

> "*The technical support is not exactly wonderful and it is not individualised to the person. It is like giving a blanket, this is what available you take it or leave it. You cannot say I have a special need, and say ok, your need will be addressed.*"

The Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B said

"*One of the real problems with NHS IT system that everyone says what we will do is 'we will put a prototype and we will work with you to develop the final product'. It is like when you say 'you buy a car and then we will work with you to develop the wheels'.*" (See Figure 5.3).

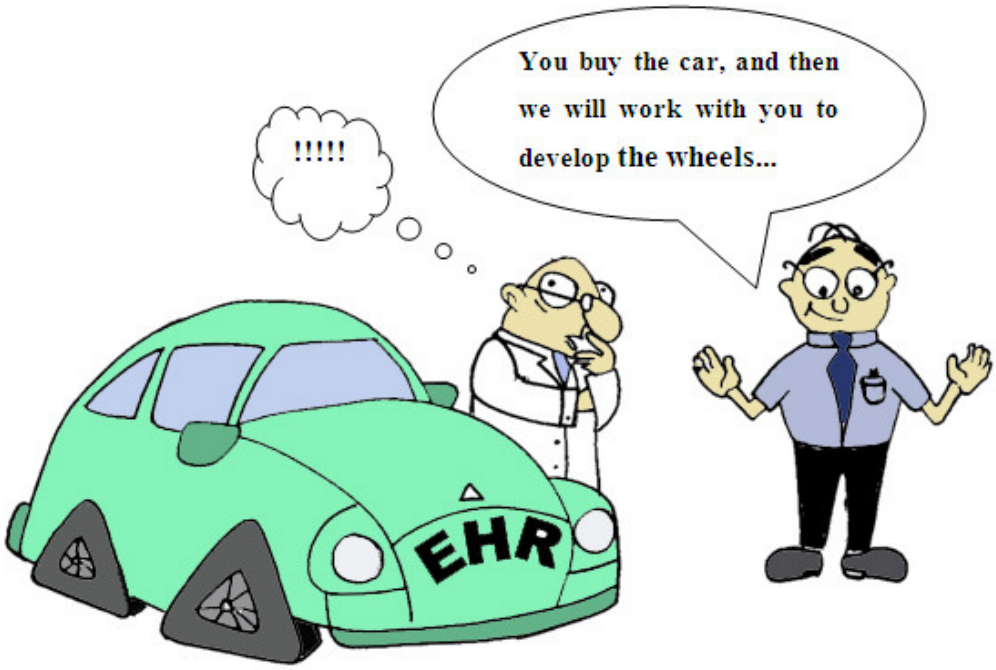

Figure 5.4: The expectation misfit

On the other hand, the Director of Information and Communication Technologies in hospital B who expressed just the opposite idea of clinical involvement in the process of system development:

"I had a project manager who had spoken to a number of clinicians and worked out the information that was needed. He has clinical background, and from that we gave our importance to development. We ended with a product and we shared it with colleagues and it makes a lot of sense of what we have done."

Some other clinicians had some negative views about technical staff in healthcare organisations by saying:

"*One of my on-going worries about the whole NHS IT and specifically as I have seen in this hospital here is in the IT department, as if you could*

get a job in IT at twice salary why would you work in the NHS? Because you cannot get a job twice salary somewhere else!"

5.4 Social

In this research context, social factor concerns users' awareness and empowerment of patients and medical staff and their involvement in designing and developing the information security strategy of EHR systems.

There are focus groups that are involved; it is difficult to show the effect of these groups on security issues. For example, the head of "Information inc. Coding and Patient Administrations System (PAS)" in hospital A pointed out that patients are not involved in the local security policy and said:

"*Focus groups should be part of the local and national policy. In terms of information security, patients' focus groups don't have the experience and they don't take part in the local policy.*"

While the Clinical Director, Surgery in hospital A thinks that patients and clinicians should be effectively involved:

"*I suppose patients have the complete right to say no we don't want to do this and we don't want to do that. And it doesn't sound too good to take away people's rights, but in science the public is not the best informed. And likewise, the doctors are not the best informed; especially with information technology and security. There are some people that not be allowed anywhere near computer and security systems.*"

Clinicians feel isolated and ignored when it comes to information technology projects such as the NPfIT which cause disappointment and dissatisfaction. The Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B expressed his views about clinical involvement by saying:

"*Everything had been decided first, no point in getting clinical involvement. Because the programmers would just say this is just what we can do. The big problem with any innovation is to get clinical*

> *involvement; and for involvement you need ownership; and for ownership you need consultation.*"

Clinicians also look at the big NHS IT project as it always starts with the happy users because what they got is not what they want because who are designing the system are computer professionals not health professionals.

The Clinical Director, Medicine and Rehabilitation in Hospital B also expressed his concerns towards patients' involvement:

> "*The patients' representatives are very concerned that confidentiality will not be protected and patients will not necessarily have rights in there, it was actually put on the IT system. Even if they may accepted it is on a paper system previously taking notes. This is the kind of concern that not yet resolved.*"

In terms of involving various stakeholders, the involvement is low, as the EHR system seems to be very much run on an IT base. Even if the project organisers tend to involved stakeholders and get people working on the different modalities at the clinical level, in practise, people tend to look at it more as an administrative tool, rather than a clinical tool. Even if in healthcare all workable and sustainable solutions come from the clinical staff themselves. It's very hard to force systems on people and get them to change their working practices. And if they are provided with a finished product they wouldn't do it.

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A said "*No. I don't think any clinician or any patient group is involved and I've heard lots of other clinicians make the same criticism.*"

On the opposite side, the Information Governance Administrator in Hospital A said

> "*There are special interest groups, that sort of thing. And these consultants were going to all these various meetings and it was really, it was good because they were getting a lot of knowledge about what was happening. But then, everything just went so quiet, there was nothing happening, so the group was disbanded."*

Based on the accounts of interviewees in hospital A, there was probably about half a dozen consultants in hospital A on that group who were keen but it was just disbanded because there was not anything happening. There were no more workshops or events that were holding centrally in the NPfIT. So there was no reason for them to continue. The special interest groups were chosen because they were people that were keen. They had the London Clinical Advisory Group, but that has just been put on hold. Then they re-instated it and sent an e-mail saying that they are not going to carry on with those events.

Some public efforts played a role in raising public awareness in 2006 using national newspaper by advising readers how to opt out of the NHS Summary Care Record (SCR) on the national Spine database (EHI, 2006a). As a response, the Department of Health has rejected patients' requests to stop their information being uploaded to the NHS data spine (EHI, 2006b).

Many incidents happened that made people worried about their confidential information being lost or put in the wrong place. For example, when a mailing house used by NHS CfH has led to patients receiving information packs addressed to other patients (EHI, 2010j). Another incident, when a hospital worker was suspended after medical records belonging to patients at a secure hospital were found on a USB stick in a supermarket car park (EHI, 2010d).

5.5 Legal

In the previous chapter, it was reviewed the legal acts that govern information security and privacy in sharing medical information and other privet information, as well as the international and national standards that are applied on shared EHR systems. These acts and standards are required by law to be applied to grant secure use of new technologies and sharing information in healthcare.

The Clinical Director, Surgery in hospital A said:

> "*To safeguard ourselves, we have a full explanation for the procedure and the complications signed and dated and signed by the patient and the doctor. It is like a contract between the doctor and the patient for the operation. So there is no reason not to do it when it is digitally.*"

The Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B said

> "*The problem is you have no way in stopping any hospital employee looking at his neighbour's haemoglobin on the record system. We have an information security policy, but there is actually nothing to stopping doing so.*"

Usually in hospitals everyone is aware of the three pages in the policy, but the hospitals has a new policy coming up every two years, for this reason people are not aware about the changes. Some clinicians don't think security is an issue, but accuracy is an issue for them. And they are pretty sure that no one in the hospital will breach the policy.

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A said

> "*Access controls, they are the same access to electronic records as they have to paper notes, i.e. any clinician can look at them. Anybody basically with a password and a username can get into the system. But if you haven't got those you can't get at them.*"

It is known inevitably in health records, there are flaws in security and there is nothing secure about paper notes, which might be left on a desk in outpatient's or on a shelf in a ward and anybody can go and look at them. There is always the question if it is going to be a patient or a patient's relative or somebody passing through the wards. Clinicians don't make a great deal of fuss. There are Caldecott rules about how records should be stored and how to look after them. This makes some clinicians think that electronic systems are much more secure than paper records, but in theory if a security breach occurs in the EHR system, it could be massive.

The Director of Training Programme, Lead Clinician, Chronic Pain Service in Hospital A said: "*Now one of the problems is that I don't think there's a clear definition about who's going to have access to what levels of information on this database.*" It is thought that not anybody should have access to patient's health record except the patient and a doctor or health professional that was given

permission to access it by the patient. Some people are very concerned that this is already being looked at as the property of the NHS and not the property of the individual. There's no clear demarcation between a personal health record and the demographic and administrative data that goes with it.

The Director of Training Programme, Lead Clinician, Chronic Pain Service in Hospital A said: "*You need to know what you need to know. You don't need to know what you don't need to know and that's sound to me to be quite a complicated thing.*"

The Information Governance Administrator in Hospital A said:

> "*It is like with everything really, it's much better if we are all working to the same standard rather than all doing our own thing, that is what tends to happen now. Everybody does their own thing and everyone is duplicating the work. They could just be one standard, everybody could work to make life so much easier.*"

The Information Governance Administrator in Hospital A said:

> "*Sometimes, it is very difficult. I mean part of our information governance toolkit, one of the requirements in there is how do monitor compliance that, when people have got the smart cards, are using them according to our security policy around that, very difficult, because there's people out there, they have got the card and how do we know that they are not saying to somebody, here's my card, shove it in the computer.*"

In hospital A they have a Regulatory Affairs (RA) Manager and he is supposed to be looking at and putting in processes to check the information governance policy, it is their responsibility because it sits within the Human Resources (HR) Department. They have got the registration authority manager there and they do all the issuing of cards. There are a lot of improvements to the RA system. They are doing a lot more electronically, they are doing away with a lot of paper forms and there is going to be more capability in checking and monitoring. It could be done in a GP's surgery when

there is a small number of staff and the Practice manager would need to do it. But in big hospitals with a big number of staff, it might be difficult to be controlled. As an example

> "*How do you do it, if somebody suggested that you need to ring and just say to someone you know, have you got your card, what's their number, all that while card in their hand, that doesn't prove that they are not lending it to their colleagues, so it is quite difficult.*"

Any healthcare organisation has an information security policy and a data protection policy. These are supposed to cover all security and confidentially issues and obviously anybody that is working, any record, has to be aware of the responsibility for confidentiality. Every employee has to sign the information security policy. It is very much based on what other Trusts are using. It covers everything and it covers e-mails and internet usage, it could be quiet long document such as fifty pages. According to participants' views, this policy document should be reduced in size because it is pretty comprehensive and the data protection policy is obviously more about the confidentiality and sharing information and consent.

Access control is an issue and a concern to many healthcare professionals. It is usually done on a role-based access. For an example, the clinic receptionist would probably only has access to the demographics. But the clinician would have access to slightly more specific information. Currently in clinics and hospitals, there is not a huge amount of clinical information on the records, but it includes the history of patients such as when they came in, where they were seen, where they then went, that sort of thing. And not everybody would have that access.

Standardisation is a big concern for information security strategy. Each individual health organisation has its own policy. It was suggested by the interviewees that they could follow the national policy to keep it simple. For instance, if it is going to be a data protection policy, it is going to be the same for everybody. It would be appropriate just to use one as more than one could lead to confusion.

The rules and principles of information security are similar in healthcare organisations. As most of the interviewees think that it could just be one centrally

developed policy for everybody. If everybody uses the same system, it is important have standardised policies around it.

The Information Governance Administrator in Hospital A said:

> "*We have an information sharing protocol at the moment in place, which is signed up to by ourselves, the PCT and the local London Borough, the social services department. And we've also got, I mean at the moment we've got to look at all of our policies in the light of this.*"

There could be a generic information sharing policy and a specific policy for specific departments such as a specific one for children's services and a specific one for mental health services. This is because different departments may be governed by a different health authority such as the mental health service.

5.6 Clinical

Clinical practice can affect information security and privacy significantly in different ways. Many security breaches occur during medical consultation or accessing medical records in a public place in the medical area. Sometimes, sharing access login details in Out of Hours or with locum doctors are ways of breaching security of EHR systems.

Some security procedures, such as a complicated login access procedure, could increase the consultation time instead of reducing it. System breakdown could cause a lot of problems such as data loss and information unavailability, temporarily or permanently. In all these cases, clinical needs should be considered when designing information security strategy for EHR systems.

The Clinical Director, Ambulatory, Diagnostic and Therapies in Hospital A said

> "*If you want to exchange information between hospital and another, we are talking about the pathology system already or X-ray system or patients' records system etc. Then ideally you should be able to exchange it or for an ideal world it should be like Hotmail.*"

According to a participant, there was an incidence when patients go from one hospital to other hospitals, pretending that they have serious painful disease. They go from one hospital to another to get morphine to relief their pain, misusing the NHS. In the participant's opinion, if hospital X could find information about what happened in hospital Y, this would not happen.

The Clinical Director, Medicine and Rehabilitation in Hospital B said

> *"they haven't understood some of the basic clinical needs of clinicians in using IT in this way. And here some clinical needs on the project haven't been fully taken into account.*"

Patients with sensitive illnesses, such as sexually transmitted dieses or alcohol abuse, particularly, can be very concerned about information that could be made available to anybody without their knowledge.

Based on the account of an interviewed clinician, at the moment there is a breach of data protection in the hospital. When a hospital has locum doctors because they don't actually have ID access because they don't have a badge and they have to get blood result for them and somebody else has to get them such as a nurse, another employer or a doctor. As a fact, sometimes the password is given to the locum doctors because nothing else can be done, that is breach of data protection. In weekends and nights the number of staff on a particular site is reduced. In the nights in this hospital, there would be lack of doctors; one of them might be a locum doctor who needs to find a way to do actually his work.

Clinicians wouldn't normally be able to access mental health records. In fact, it can be achieved, but obviously when people coming in ill, background of mental health problem may make a lot difference to what clinicians do.

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A expressed his view about the used EHR system:

> "*It does all the things like measuring performance against targets and patient administration, but it doesn't give the clinician satisfaction of being able to produce a report on what that team has done in a year.*"

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A said

> "*Well the Government has to be clear about what it wants. Does it want demographic information on illnesses? And patterns of illness and outcomes of healthcare interventions or does it want information about individuals? But at the moment there's seems to be no dividing line between the two. The individual's health record shouldn't be his or hers and it should not be accessible to anybody else for any purpose. Top line, anonymous information about disease incidents, cancer registries, or whatever! That is a public health issue and there is a reason for health systems to know about that.*"

The Information Governance Administrator in Hospital A said

> "*We need to keep things tidy and have one sort of front page that gives you your medical history and all that; you don't need to keep repeating that.*"

5.7 The most influential factor- the political factor

Figure 5.1 shows each of the six factors influences the building of the information security strategy of EHR systems and each factor is influencing and influenced by other factors. As it will be shown later, the political factor seems to be the most influencing factor among the six factors, as it influences four factors (social, financial, technical and legal), as it will be shown later, and being influenced by the (social) factor, but it doesn't seem to influence the medical factor. On the other hand, the technical factor seems to be the most influenced factor by other factors (political, legal and financial) and influencing only the clinical factor in terms of information security of EHR systems. This influence is a direct influence, but there could be indirect influence between different factors. But in this research, we are trying to show only the direct influence. As the technical factor may have indirect influence on the social factor because the technology itself is influenced by what people want and according to the political and legal views and any financial and clinical needs. The social factor doesn't influence the technical factor directly. Because when one

talks about the social factor, one talks in reality about the public. The social factor doesn't influence the technical factor directly; however, the social factor goes through other factors to influence the technology such as political, by using the democratic process, which could influence other factors.

The British government is the body that sets the spending budget, and how much the NHS should have and for what. This clarifies the relationship between the social factor and the political one. It is a mutual relationship. As the public are those who elect the government, and political views and decisions affect, in one way or another, how public should be governed and behave. While the political factor affects the financial one and has control over it, but the financial factor doesn't seem to affect the political factor when it comes to building an information security strategy for the EHR system. Meanwhile, the political factor doesn't have a direct influence on the clinical factor, but in practice with the influence of the political factor on the other four factors, it could have indirect influence on the clinical factor. As it would be a result of the other influences.

5.7.1 The influence of the political factor on the legal factor

A medical network website carried out a survey in the beginning of 2008 for a national newspaper, asking 11 questions on attitudes towards the National Programme for IT, including who should have access, how secure the system is and how confident they are that the new systems will work. According to this survey, Four-fifths of doctors are concerned that current plans for patients' health records to be available from a central database (the summary care record) will make them insecure (EHI, 2008a). Sooner after this survey, MPs called for data loss to be a crime (EHI, 2008b). In less than one month, nine out of ten doctors have no confidence in the government's ability to safeguard patient data online, a poll by BMA News magazine has revealed (EHI, 2008c). Later, the Information Commissioner said "*It has to be the likes of chief executives of NHS trusts and permanent secretaries who are held accountable when things go wrong*" (EHI, 2008d). Then, tough new laws on data breaches had been announced. MPs have passed legislation, giving the Information Commissioner the power to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act (EHI, 2008e).

There is an indirect influence of the political factor on the clinical factor through the legal factor. As the Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B said

> "*I know there is political bit about you are not allowed to know the patient's HIV positive, but it matters; if they have all the infections. We have to be trusted as healthcare professionals.*"

5.7.2 The influence of the political factor on the social factor:

The Caldecott Guardian and Clinical Lead for Health Informatics in Hospital B said

> "*I don't find it a problem for clinicians to represent patients, but it is politically not acceptable. Because we are all at the end patients.*"

Many people believe that having their EHRs shared and stored in a national data base will invade their privacy and may affect their personal life. A group of people created a campaign with a website (http://www.thebigoptout.com); they called it "The Big Opt Out Campaign". The aim of setting up this campaign is to protect patient confidentiality and to provide a focus for patient-led opposition the government's NHS Care Records System.

5.7.3 The influence of the political factor on the financial factor

The Clinical Director, Medicine and Rehabilitation in Hospital B said

> "*Now, it is not the newsworthy, it was the national press has been a number of large problems, recently one of the contractors has pulled out after unseat the government, I don't know which one, but one of them has.*" "*It is a very ambitious project, I don't know if any other country has quite same*."

The government has set out where it will cut the first £6.2 billion from public spending in 2010. The Department of Health was one of the departments left off the list, on the grounds that its funding is protected; meaning that it can recycle its own

efficiency savings (EHI, 2010b). It was thought that saving of £600m would come from the National Programme for IT in the NHS (EHI, 2010c).

5.7.4 The influence of the political factor on the technical factor

The Director of Training Programme, Lead Clinician, and Chronic Pain Service in Hospital A said:

> "*I've got a lot of worries about it from a political point of view. I don't really see the justification for a centrally held database across the whole country.* "

The British Medical Association has written in March 2010 to the government calling for the roll-out of the Summary Care Record to be suspended (EHI, 2010i). GP leaders have joined the attack on the roll-out of the Summary Care Record, because they found it bizarre to start a wider roll-out when they didn't have the results of the independent evaluation (EHI, 2010g).

The biggest three English parties are Labour, Conservatives and Liberal Democrats. The previous Labour Government proposed the NPfIT project while both the Conservatives and the Liberal Democrats have repeatedly called for the national programme to be scrapped (EHI, 2010h).

Professor Trisha Greenhalgh, lead author of the 234 page report, 'The Devil's in the Detail', said she hoped the government would look carefully at the researchers' findings before making decisions about the future of the SCR and HealthSpace (EHI, 2010a).

Summary:

In this chapter, six factors that influence implementing and developing information security strategy for EHR systems have been identified: political, financial, technical, social, legal and clinical. Each factor is influencing and influenced by other factors. The political factor seems to be the most influencing factor among the six factors, as it influences four factors (social, financial, technical and legal) and is influenced by the (social) factor, but it doesn't seem to influence the medical factor.

On the other hand, the technical factor seems to be the most influenced factor by other factors (political, legal and financial) and influencing only the clinical factor in terms of information security of EHR systems. The findings in this chapter clarify the importance of exploring and understanding the impact of different factors on building a strategy and how the strategy may be built with diverted aims rather than directed aims.

Chapter Six

A proposed framework to design information security strategy for EHR systems

This chapter proposes a solution to minimise the influence of different factors, as defined in the previous chapter, by providing guidelines for building an information security strategy for EHR systems. These guidelines are identified according to the major steps to create an information security strategy as explained in Chapter Two, which they are:

1. Analysis of the current situation.
2. Determination of the requirements.
3. Definition of the target situation.

To provide the guidelines to build an information security strategy for EHR systems, different research methods were used, as explained in Chapter Three. An analytical method was used to obtain an extensive and, to the degree possible, generic frame, capable of analysing a wide range of different shared EHR systems. England was chosen as a major case study that involves a diverse multitude of EHR systems. This choice was made in this research on the basis of the existence of many different EHR systems in the English NHS which are being used for different purposes and by different sharing levels. Interviewees were cautiously chosen based on different backgrounds, missions and responsibilities in using, designing and managing EHR systems. Furthermore, in the research data collection and review of documentation, it was very important to consider different documents that could govern information security policies and data protection that are used for technical, legal and practical purposes. By combining those different considerations in conducting and processing information, this study ended up with eight elements that compose the current situation of any EHR system, nine requirements determined to be in place, and six aims to be as a target situation to achieve a secure EHR system.

6.1 Analysis of the current situation

Eight elements were identified after observing and analysing different EHR systems, and they could serve as milestones to help analysing the current situation of any EHR system with regard to information security. These eight elements are shown in Figure 6.1.

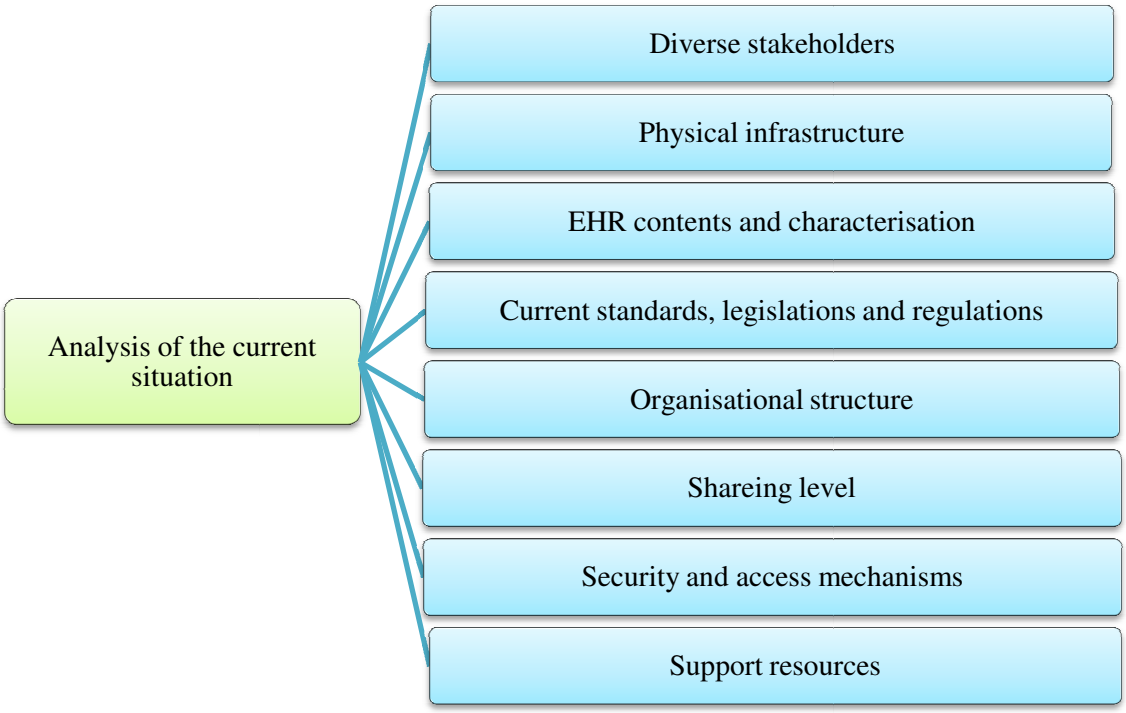

Figure 6.1: Analysis of the current situation

6.1.1 Identifying diverse stakeholders

The growth of 'shared health' led to a situation where the patients share responsibility with providers for care and this increasingly led to fragmented or episodic relationships with multiple providers (Gunter and Terry, 2005).

It is important to identify who is who in managing information sharing settings and regulations in electronic health records systems.

The main stakeholders who would be responsible for setting an information security strategy for electronic health records are identified as follows (Vries et al., 2003, The Royal Society, 2006 and Schabetsberger et al., 2006):

- Patients
- Medical professionals (general practitioners, established specialists, physicians in hospitals, rescue services)
- Pharmacies
- Researchers and consultancy (epidemiologists, medical and public health scientists, statisticians)
- Health insurance companies
- Public authority (governmental institutions, controlling institutions of health care system, civil protection services).
- Industrial organisations.
- Education institutions
- Inspection agencies
- Representative organisations
- Physical system
- Software designers

6.1.2 Physical infrastructure

The physical infrastructure includes network engineering with important factors, such as quality and quantity of the equipment used for EHR sharing, the topography distribution of the networks, etc.

This depends on the sharing level, as we will discuss later, as seen in large organisations including hospitals and different health systems that may be linked via computer-based communications channels (Shortliffe and Sondik, 2006). Fraser et al. (2005) classified EHR systems network infrastructure in terms of three types: stand-alone systems, local area network (LAN) systems and wide area network (WAN) systems. This classification plays a role in setting information security strategy as data protection policy and other information security procedures will

differ according to the topographical setting of the network that will be the platform for EHR sharing.

6.1.3 EHR contents and characterisation

"The EHR is simply a collection of all information captured electronically and available in provider-accessible form" (Covvy et al., 2003).

This information might be Summary information, detailed information, or it could be special medical information related to departmental health services, or comprehensive records that includes different types of medical information.

The contents that relate to patients' health information comprise personal data, general medical data such as information on chronic disease like diabetes, medications data (e.g. on stopping medications and reasons for break off), outpatient data such as tests and diagnoses, hospital data, address lists, laboratory report, vaccination, preventive checkups and a personal health journal (Ueckerta et al., 2003) and (Ückert et al., 2004). The Health record contents even play a major role in planning an information security strategy. Such health information could include very sensitive data that need to be protected and shared in a very confidential environment, for example, mental health records and sexual health records. These records may even need a special data protection policy and special access roles for obtain the sharing process.

6.1.4 Current standards, legislations and regulations

This depends on different policies that are set to regulate access rights and to protect patients' data. Such standards and policies depends on what kind of shared electronic health records we are looking at and what level of sharing and with whom.

Access rights policy usually "*governs the access privileges for each role within the organisation according to the category of information sought, the purpose of the request, and intended recipient of the result*" (Agrawal and Johnson, 2007). The current standards and regulations can be covered by different national or international data protection acts and information sharing acts.

Many issues must be considered when looking at EHR information security regulations such as the consent model that should be used to obtain patients' consent, access roles, access rights, data accreditation standards, monitoring and auditing. It should be kept in mind that "*since practice and technology remain moving targets, the work is never done*" (Detmer, 2003). For this reason, the lack of standardisation and organisational problems will affect planning the information security strategy (Schabetsberger et al., 2006).

In the United Kingdom, three acts govern information sharing in EHR systems. Those acts are: Access to Health Records Act 1990, Data Protection Act 1998, and Freedom of Information Act 2000. Furthermore, different British and International standards govern many aspects of information access to guarantee data protection, privacy and information security assurance such as ISO 27000 series of standards and BS7799.

6.1.5 Organisational structure

Usually, EHR design is based on organisational structure. EHR sharing depends on how many different organisations are responsible for patients' care and how those organisations are linked together and what level of sharing to be considered for each different organisation. To make this clear, access to the EHR must be made available to many parties (Longstaff et al., 2000): the General Practitioner (GP) with whom the patient is registered, other GPs, secondary care organisations, public health and other investigators for legal or research purposes and patients themselves. The sharing with different parties needs a legislation linkage among different organisational bodies.

6.1.6 Sharing level

Electronic health records can be shared on different sharing levels, such as local, national or global. The local sharing level is confined to the local area or within local organisation such as a within a hospital or between a primary care organisation and a secondary care organisation in a local area. This kind of sharing can be more controlled as the EHR sharing is limited within a small area and the auditing process is not so complicated. While the national sharing level is more complicated as it

covers a whole country and must be controlled by national bodies and national legislations and standards. In addition, it needs centralised storage data equipment and a very secure network. Global sharing level can be managed by using the Internet as the most efficient network that can be accessible globally. On the other hand, using the Internet to store confidential data, such as the electronic health records, requires more strict regulations for security mechanisms to ensure patients' confidentiality.

6.1.7 Security and access mechanisms

Security and access mechanisms can be defined by authentication and authorisation mechanisms. There are many different methods that can be used to authenticate a user such as (Speed and Ellis, 2003):

- Username and password
- Certificates (x.509v3)
- Biometric techniques
- Smart cards
- Anonymous access

Authorisation comes next; access control uses (Speed and Ellis, 2003):

- Passwords
- Tokens
- Kerberos ('guard dogs'): Kerberos is a network authentication system targeted for use on physically insecure networks.
- Single sign-on

As an example, access to EHR can be obtained by insertion of a smart card that initiates the authentication dialogue. Then a PIN number is requested which is validated against the single sign-on database like a chip-and-pin scheme (Brennan, 2005).

6.1.8 Support resources

(Financial, governmental, training, technical)

Any adoption of electronic health record system "*will require mechanisms for creating, funding, and maintaining the regional and national databases that are involved*" (Shortliffe and Sondik, 2006). Financial difficulties are also a common problem for information security (Schabetsberger et al., 2006) as it affects the level of security through affording or not the suitable solution for information security requirements. Implementing secure EHR systems requires initial costs; the extra expenses are usually targeted to support personnel and operation of such systems to have concrete data on improvement of quality of practice or return-on-investment analysis (Lakovidis, 1998).

Other support resources need to be considered, such as the governmental support, as it will help setting a general information security strategy and identifying its standards and regulations such as data protection acts. That should consider the special and confidential characteristics of the electronic health records. Furthermore, to put an information security strategy in place, training is required to assure the confidential use of the EHR systems.

6.2 Determination of the requirements

After analysing the current situation of the EHR system and its related information security issues, determining the requirements comes next. In this research, nine requirements were determined, as shown in Figure 6.2, for obtaining a secure EHR system. These requirements were defined after observing different EHR systems as explained previously.

6.2.1 Data accreditation and Encryption services

One of the companies that work on data accreditation had made a ten point checklist for successful data accreditation which they are:

- ✓ How much do you know about the information management and technology directed enhanced service IM&T DES?
- ✓ Have you done your data accreditation baseline assessment?
- ✓ Have you done training needs assessments for all your staff?
- ✓ How good is your data quality?
- ✓ How does your data compare with other practices?
- ✓ Have you submitted your data accreditation plan to the PCT?

✓ Can you achieve the organisational standards? ✓ Are you accredited 'paper-light'? ✓ Do you meet the Information Governance standards? ✓ Are you ready for assessment?

Table 1: A checklist for successful data accreditation, taken from a publicly available leaflet of the NHS PRIMIS+ service (http://www.primis.nhs.uk)

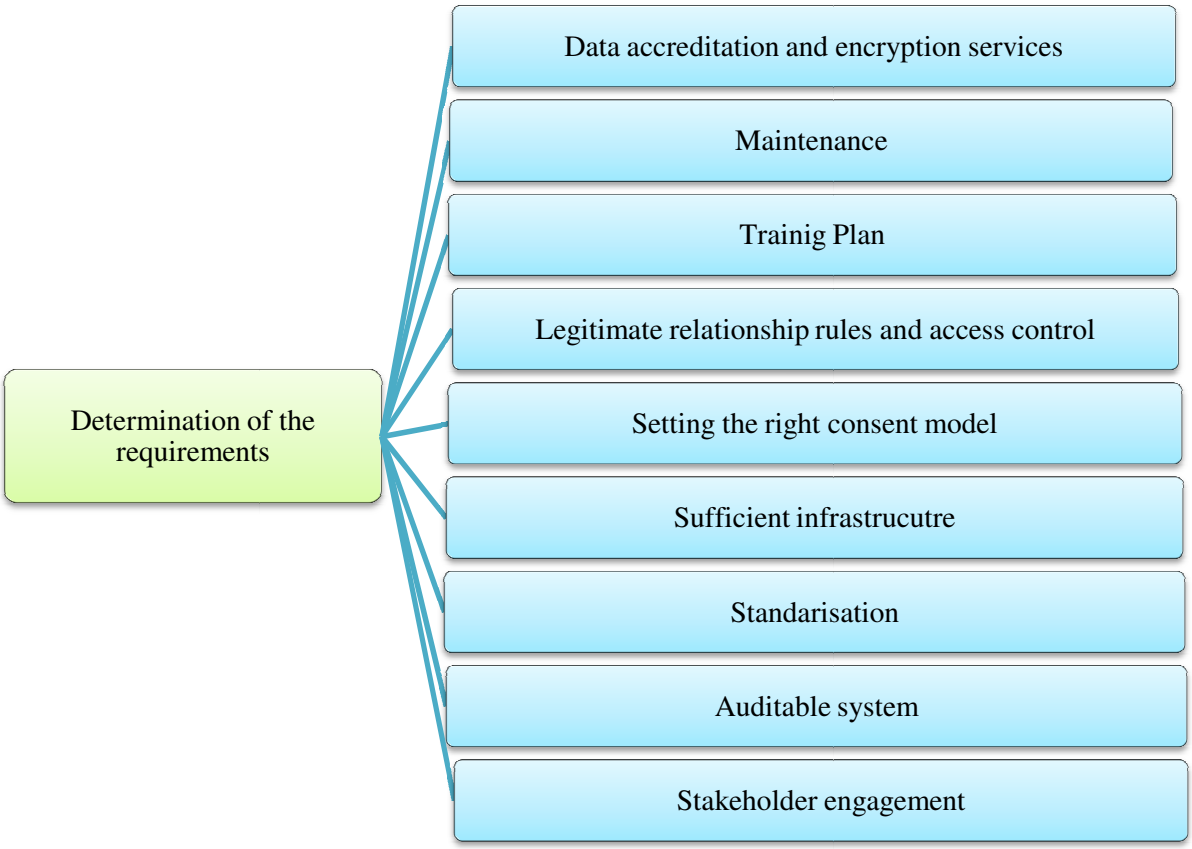

Figure 6.2: Determination of the requirements

6.2.2 Maintenance

Shared EHRs are meant to be secure and available at all times; however, any system could have breakdown times. For this reason, maintenance should be adequate and done quickly. For this reason, backup plans should put in place in case of a system breakdown. Data mirroring shouldn't take palce in the same server. In addition, 24 hour IT support should be available.

6.2.3 Training plan

Training health professionals to use shared health records and make them aware about information security policies is a very important part to be considered when setting the requirements for the information security strategy.

Different ways of training could be put in the plan, such as face to face training, training in the working place, and training using some electronic tools such as training software or online training including assessment tools.

6.2.4 Legitimate relationship rules and access control

It is very important to know who should access what and why. In addition, it should be very clear to set access control mechanisms before designing and developing the EHR software. Different access control mechanisms, as well as, legitimate relationship roles, were discussed in Chapter Four.

6.2.5 Setting the right consent model

A patient should be considered to have given prior permission for his/her medical record to be shared. If the patient or chosen proxy answered positively when asked for such permission, the health records can then be shared (Rind et al., 1997). But in some cases, health records are being shared, as long as no negative answers form patients are given. Various consent models where discussed in Chapter Two and Chapter Four.

6.2.6 Sufficient infrastructure to ensure data protection procedure

In the case that the infrastructure in the healthcare organisation is found to be insufficient for secure access to the EHRs, it is important to provide the right and sufficient hardware with considering the network and equipment layout within the working place. Furthermore, portable and secure devices should be configured in such a way as to allow the necessary accessibility and mobility for health information access.

6.2.7 Standardisation

All information that is related to a specific patient that are sent to a medical centre or hospital would become part of the patient's health record. This is necessary in order to document the basis for decisions that are made in the emergency department and to have the full medical history in the same record. These data would be permanently and clearly labelled as having been obtained from the reporting source (Rind et al., 1997). Different computerised medical systems should be able to share records. They should have common standards to accept different health information from different departments such as (radiology, laboratory, etc.), without changing the content of information, even electronic medical records are doomed to remain fragmented (Mandl et al., 2001).

6.2.8 Auditable system

It is very important to design a system that can be easily and effectively audited by setting the right way to report access history and managing access alerts. It is also very important to allocate the right staff that will be responsible for auditing within the healthcare organisation.

6.2.9 Stakeholder engagement

Once the stakeholders are known, they should be involved in designing and developing the system. They should be involved in decision making as well. This could happen by organising special interest groups and different events such as meetings, workshops and conferences to attract stakeholders and to raise public awareness.

6.3 Definition of the target situation

The final step in building an information security strategy for EHR systems is to define the target situation. This step comes after analysing the current situation and filling the list of requirements. Six aims were found in this research to obtain a secure EHR system as shown in Figure 6.3.

6.3.1 Comprehensiveness

Kane and Sands (1998) described the need for comprehensive web-based patient records because "*care is normally provided to a patient by different doctors, nurses, pharmacists, and ancillary providers, and different institutions in different geographical areas*". Each provider should know what others have done and what they are currently doing. Outpatient records should contain some information such as problem lists, procedures, allergies, medications, immunisations, history of visits, family medical history, test results, doctors' and nursing notes, referral and discharge summaries, patient-provider communications, and patient directives (Kane and Sands, 1998). Mandl and Kohane (2001) added that the records must be life-long so that a patient's medical and treatment history is available as a baseline and for retrospective analysis.

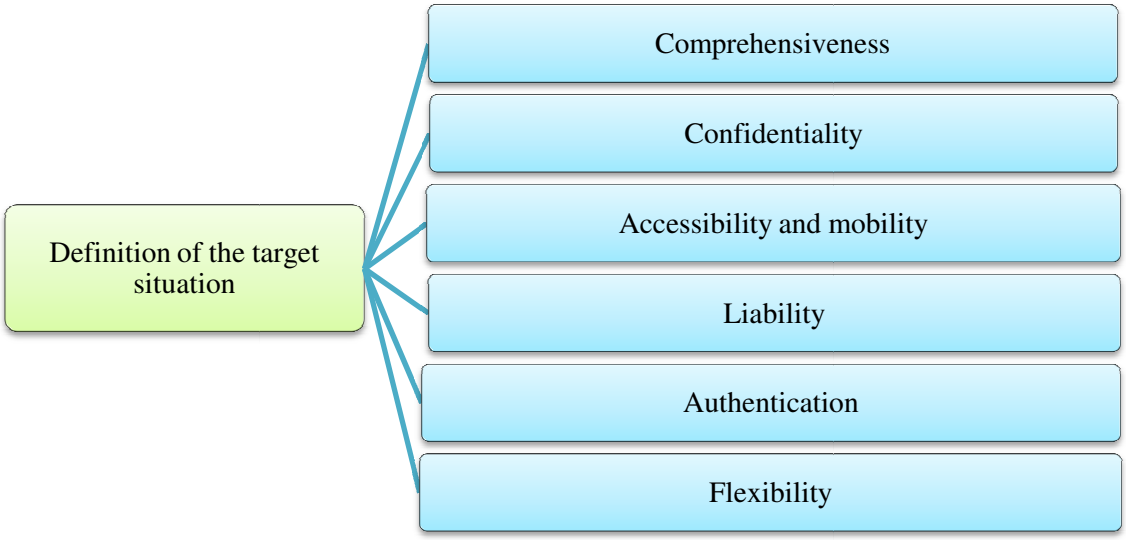

Figure 6.3: Definition of the target situation

6.3.2 Confidentiality

It is generally accepted and widely presumed that patients have/ should have an ethical and legal right to the confidentiality of their medical records. Therefore, it is considered appropriate to allow access to a patient's record only with the patient's permission. In some circumstances when the patient is unable to permit access to his records, open permission must be obtained. However, in certain serious medical situations, patients should provide consent if they were able to do so. On the other hand, if the patient has officially decided that his or her health record should not be

shared, then the record will not be accessible, even in an emergency (Rind et al., 1997).

The national programme for IT (NPfIT) is going to implement a health care system with three levels of security (NHS CfH, 2006b):

- Open information that any doctor, nurse or specialist can access.
- Confidential information which will be flagged by an alert and need permission to be accessible.
- Secret information, which is invisible. This means that no one can know if it is available or exist. This information can be kept as a secret between a doctor and his patient by a request of the patient.

Mandl et al. (2001) said that "*patients should have the right to decide who can examine and alter what part of their medical records*". In some cases, a patient declines permission of access to his or her health records, although, in this case, he/she will not be able to receive a good quality care. At the other extreme, some patients do not mind making their records completely public. For most patients, "*the appropriate degree of confidentiality will fall in between and will be a compromise between privacy and the desire to receive informed help from medical practitioners*" (Mandl et al.,2001).

Because an individual may have different preferences about different aspects of his or her medical history, access to various parts of the record should have different levels, and health record should be divided into layers according to the access right levels. For example, psychiatric notes may deserve closer protection than immunisation history (NHS CfH, 2006a). I n this case, a doctor with a legitimate relationship with the patient should have an access right.

Furthermore, patients should be able to allow different access rights to different healthcare providers. Most patients prefer to a confidentiality policy that would allow an authenticated healthcare provider in an emergency to have access to records that he or she would not normally be able to have (Mandl et al., 2001).

6.3.3 Accessibility and mobility

Health records may be needed on an regular basis or in emergency situations. Ideally, the records should be with the patient when they are needed at any time or anywhere, such as on the World Wide Web. In addition, with the patients' permission, these records should be accessible to and usable by researchers and public health authorities (Mandl et al., 2001).

The National Health Service (NHS) Care Record Service (CRS) in the UK set the Care Record Guarantee to form an important part of the public information campaign about NHS Care Records and to cover people's access to their own records, controls on others' access, how access will be monitored and policed, options people have to further limit access, access in an emergency, and what happens when someone cannot make decisions for themselves (NHS CfH, 2995).

Rind et al. suggested that access to the record of a patient could be provided if all of the following criteria are met (Rind et al., 1997):

- The patient has not recorded, at the reporting institution, a previous explicit prohibition to the release of records over the network.
- The patient consents to access for a specific incident of care at the recipient institution.
- The identity of the patient is authenticated.
- The identities of the recipient institution and provider are authenticated.

A recipient provider of shared health records should consider the need for emergency access to the record of a patient when the provider certifies that such access is appropriate. This would require (Rind et al., 1997):

- The patient is not able to give permission for access.
- The patient is at risk for serious harm to his or her health if access to the record is delayed.

6.3.4 Liability

Any access to or change in a patient's record should be recorded and visible to the patient. Thus, information entered into the record must be identifiable by their sources for example with adjustment of name and date (Baker and Masys, 1999). Patients should also be able to see who has accessed any parts of their records, under what circumstances, and for what purpose. Reliable authentication is essential to make this possible. Appropriate laws can support accountability built into the records system (NHS CfH, 2006a), (Mandl et al., 2001) and (NHS CfH, 2005).

6.3.5 Authentication

Rind et al. described two sides of authentication depending on the type of health record. For a patient and another party such as a doctor or provider, a patient would be considered authenticated if the following information was correctly transmitted: last name and first name, date of birth, gender, mother's first name, and father's first name. A patient will be considered authenticated if the following information is correctly transmitted: last name and first name, date of birth, and gender (Rind et al., 1997). On the other hand, problem with identification, such as incorrect spelling for name, will not allow access to the correct record (NHS CfH, 2006a).

6.3.6 Flexibility

Most people don’t mind to make data about themselves available to those who are trying to improve medical knowledge, the practice of medicine, the cost effectiveness of care, and the education of the next generation of healthcare providers. This sharing information availability has limits. However, patients will not be satisfied when they feel the threat of somebody breaking through their confidential information, feel a risk to privacy, or annoyance with unsolicited follow up contacts. Patients should therefore be able to accept or deny study access to selected health records. This can be based on personal policies or decisions about specific studies. An example policy might say that any study may use the data if they will be stored only in aggregated, unidentifiable form (Mandl et al., 2001).

Summary

This chapter has examined the three steps that are required in order to create an information security strategy for EHR systems, which they are: analysis of the current situation, determination of the requirements and definition of the target situation. This chapter proposed guidelines for building an information security strategy for EHR systems by identifying and discussed: eight elements that compose the current situation of any EHR system, nine requirements determined to be in place, and six aims to be as a target situation to obtain secure EHR systems.

Chapter Seven

Conclusions

This final chapter elicits the conclusions drawn from the research done and presented within this thesis. The conclusions of this research are based upon an analysis of the reviewed literature, a field study (a major national case study comprising two sub-case studies), and an analysis of the research data. While reflecting on this, the researcher engages in evaluating the validity and applicability of this research and draws upon the original contribution to research in the field of EHR information security, as well as, it presents the limitations of this research. The chapter also provides a brief overview of the future work envisaged to develop future EHR security. Finally, the chapter is concluded by a section on personal reflections.

7.1 Main conclusions

7.1.1 Understanding the information security strategy in the EHR systems

1. Information security strategy of EHR systems is a roadmap for the foreseeable future that details the progress along the path of system maturity and keeps the focus on the most important security issues while complying with legal, statutory, contractual and internally developed requirements for electronically stored and shared information to support continuing, efficient and quality integrated healthcare provided by different healthcare professionals.

2. The purpose of building an information security strategy of EHR systems is to prevent any expected threats of security breach that could affect patients' privacy and confidentiality.

3. It is essential to understand the existing information security strategy of any EHR system by bringing it all together into one document that is readable and approuchable for monitoring and development by EHR users and developers.

7.1.2 The influencing factors on building an information security strategy of EHR systems

1. By studying the CRS in the NPfIT, this research identified six factors that influence the building of an information security strategy, mainly: political, social, financial, technical, clinical and legal.

2. The political factor is found to be the most powerful factor among the six influential factors as it influences most other factors.

3. However the technical factor influences the information security strategy in different aspects, but it is still being influenced by most other factors, which implies that the technical factor is being driven by other factors and not assuring a lead role in a technical system such as an EHR system.

7.1.3 Proposed framework for building an information security strategy of EHR systems

1. The first step in building information security strategy is analysing the current situation of the EHR system by identifying the following eight elements: diverse stakeholders, physical infrastructure, EHR contents and characterisation, current standards, legislations and regulations, organisational structure, sharing level, security and access mechanisms, and support resources.

2. The second step in building information security strategy is determining the requirements of secure EHR system by providing the following nine requirements: data accreditation and encryption services, maintenance, training plan, legitimate relationship rules and access control, setting the right consent model, sufficient infrastructure to ensure data protection procedure, standardisation, auditable system, and stakeholders' engagement.

3. The final step in building information security strategy is defining the target situation in terms of six requirements to be fulfilled with any implemented EHR system which they are: comprehensiveness, confidentiality, accessibility and mobility, liability, authentication, and flexibility

7.2 Evaluation of research outcomes

The approach taken in this research was qualitative, based on interpretive methods in analysing the information collected during this research. Having different information resources with employing different research methods allowed for more analytical and thematic thinking so to avoid wrong interpretation that could be caused by conflicting information and thus, affect the final theme of the findings. This conflicting information could be provided by different stakeholders having different interests. This led to clarifying the differences between the different views of stakeholders on three different levels of the same system: the micro, the meso and the micro. In Chapter Four, the information resources to understand the information security strategy of the CRS in the NPfIT were the National-level resources, such as NHS CfH events and NHS publications, as well as, different National and International related documents. The National level which is the macro level in this research reflects the organisers and decision making in the National CRS, which at the end share the same interest of implementing the planned EHR system with proposed information security measures. In Chapter Five, the information resources to identify the influencing factors were mainly the semi-structured interviews conducted with different professionals from different health organisations, which reflect the views of the individuals themselves and the healthcare organisations they work for. This provided information from the meso and micro level. Furthermore, different published articles that focus on the National system were analysed in Chapter Five, which at the end reflect the views of different users rather than the organisers of the CRS in England.

Furthermore, in Chapter Five, the critical views towards the National system were discussed and analysed to identify the different factors that influence the building of an information security strategy of EHR systems, as it was aimed in this research.

To evaluate this research effectively, two questions need to be answered:

7.2.1 Were the research outcomes valid?

It is hard to validate most of qualitative research findings; especially in this research as most of the findings were based on the inclusion of human, social and

technological actions. The main outcomes in this research are presented in Chapter Five (the six influencing factors) and Chapter Six (the proposed frame work). Further research needs to be done to validate the two sets of outcome. The six factors that are identified in Chapter Five need to be assessed in terms of observing the NPfIT system in long time. Some research reports about the national system that have been done and published recently present evidence that could be used to support these research findings. Some of these research reports are cited in Appendix I. For example, the "Devil's In The Detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace" found that the SCR and HealthSpace programmes spanned a number of different 'worlds' (political, clinical, technical, commercial, academic) with different institutional logics, as well as the personal world of the patient. This report also explained how each world affects the system (Greenhalgh et al., 2010).

To validate the suggested framework that was presented in Chapter Six, one will need to test it and monitor it by applying it on different EHR systems.

7.2.2 Did the research outcome answer the research questions?

The answer for this question is Yes. In Chapter Five, the research aim was achieved by defining the six factors that influence building the information security strategy of EHR systems. Furthermore, the research objectives were met in this research. However, further research is needed to be done to validate the two key outcomes of this research, that is, the influencing factors and the proposed framework.

7.3 Applicability

This section discuss the applicability of the two key outcomes of this research, (the influencing factors and the strategy framework)

7.3.1 The influencing factors

The six identified factors in this research were found by studying the Care Record Service in the National Programme for IT in England. These factors could be applicable in most EHR systems when their sharing level is national. As the political factor plays role in implementing such national EHR systems. However, it is not yet

known if the political factor may also play a role in locally shared EHR systems that being implemented in private health organisations. Further research needs to be done on locally shared EHR systems. The other five factors (financial, technical, clinical, and legal) seem to be the influencing factors in all EHR systems, irrespectively of the sharing levels.

7.3.2 The strategy framework

The suggested guidelines that have been presented in Chapter Six consider all kinds of EHR systems. These guidelines can be applied on different EHR systems such as locally, nationally or globally shared systems. EHR systems differ not only by sharing level, but by their contents such as mental health care records, sexual health care records, maternity care records, child care records, social service care records and other departmental health records. Each kind of these health records requires a different information security strategy. The proposed framework for building an information security strategy can fit all different EHR systems, by taking into account, adopting, and maintaining these guidelines according to the particularities of the specific EHR system.

7.4 Research contributions

This research provides four significant contributions:

1. The development of a definition of information security strategy, to be adopted in EHR systems.
2. Elucidation of and understanding about the information security strategy in England's national EHR system.
3. Identification of six factors that influence the building of an information security strategy.
4. The development of an information security strategy framework for EHR systems.

7.4.1 Information security strategy definition in EHR systems

This research presented definitions of different terms that related to electronically stored and shared health records. It also delineated related information security

terms, leading to a definition of a strategy and information security strategy. This research contributed with new understanding of information security strategy as a significant need in EHR systems.

7.4.2 Information security strategy in England's EHR system

The National Programme for IT in England doesn't have a one-document strategy for its Care Records Service, which is the national EHR system. This research provided a comprehensive understanding of the information security strategy of England's EHR system by presenting its different information security issues such as consent mechanisms, access control, sharing level, and related legal and regulations documents.

7.4.3 Influential factors on building information security strategy in EHR

Six factors influencing the building of an information security strategy were identified in this research (political, social, financial, technical, clinical, legal). Those factors are considered to be driving the strategy directly or indirectly. EHR systems are technical-clinical systems, but having other factors that drive this technical-clinical system is a big concern.

This research makes a significant contribution by identifying these factors, and in addition, this research shows not only how these factors can influence the building of information security strategy, but also how they can influence each other. The study of this mutual influence among the six factors led to the argument that the most powerful factor is the political factor, as it directly or indirectly, influences the remaining five factors.

7.4.4 Framework to build an information security strategy in EHR

The guidelines for building an information security strategy in EHR systems are provided and discussed in this research in the form of a framework. This framework was designed after literature analysis and after completing the whole research journey. It provides a tool to help putting the strategy in line by minimising the influence of the different factors that may steer the strategy to undesirable direction.

7.5 Limitations of the research

This research has limitations as any research effort has. The limitations arise in different ways:

1. It is based on a major national case study and two local sub-case studies. The two hospital case studies were located in one city and thus do not represent all kinds of EHR systems in Acute Trusts. Furthermore, the two case studies were in Acute Trusts while Primary Care Trust uses totally different EHR systems and even the organisational structure is different. This limitation was not critical in this research as sufficient information about Primary Care Trusts and their EHR systems was gained from the Early Adaptors of the Summary Care Records during the independent evaluation project.

2. Information collected in the CfH events presented the views of CfH as the responsible organisation to implement the CRS in the NPfIT. However, this information was limited due to underlying political and organisational interests and it did not clearly reflect the real practice.

3. Only a limited number of health professionals invited to take part in this study accepted to be interviewed. The researcher found that the participant professionals were either extreme proponents of the system or extremely against it. But professionals who were using the system and didn't have strong opinions either side of the EHR system and its information security issues, they didn't participate. Their views could have helped the research to explore other ideas.

4. The interviews were based and dependent on human interactions, and so the researcher could be affected and could influence the interpretation of research findings by gained beliefs from the interviews; while the interviewees' number was not large enough to avoid such kind of influence. Such an effect can be mitigated by interviewing more people by more than one researcher, but this was not possible within the scope of this research.

5. Most of the knowledge in this research was gained by attending NHS CfH events by meeting different stakeholders, and by exchanging knowledge with them.

Furthermore, in these events, different EHR prototypes and final products were demonstrated by software providers. However, these events provided the research with valuable knowledge, but most of this information was not recorded and referenced in this thesis due to confidentiality issues.

6. The identified six factors were based on researching the NPfIT in England and there is no easy proof that they could be applied to other EHR systems within or outside England. A comparison study between different EHR systems in different countries that evaluates the applicability of these six factors is required, and will benefit by enlisting other potential issues that affect information security in EHR systems.

7. A further limitation of the research is that the proposed framework has not been tested or monitored. It can be applicable to any EHR system, but remains to be validated in its ability to improve information security in EHR systems.

7.6 Future work

This thesis presented and discussed the information security strategy of electronic health record systems and the influencing factors in building such strategy. Several directions for further research have emerged:

1. The six identified factors could be investigated further with observation through the CRS implementation across England, inspection of documents, and additional in-depth interviews. To reduce any bias, more EHR users should be interviewed by more than one researcher.

2. Further research could be carried out on other national EHR systems in different countries to see if the six factors are the same when the EHR system is implemented in a national level.

3. Studying different EHR systems on different sharing levels with different health organisations, for example studying EHR systems implemented in private health organisations and in public health organisations in order to investigate if the same six factors are influencing the information security strategy, or there could be other factors.

4. This research did not go in depth in studying the technical aspects of information security as well as some other aspects, such as the legal acts and the ISO standards that guard and cover data protection and information security in information sharing in EHR systems. Therefore, further research in this field will help to understand and develop information security strategy of EHR systems.

5. The proposed framework in Chapter Six needs to be tested and validated by adopting it in different EHR systems, monitoring any changes that could happen, and investigating if having an information security strategy bears a dramatic impact on improving information security in EHR systems.

6. More research could be done on other telemedicine and e-health applications to investigate the importance and the impact of having an information security strategy in different e-health applications.

7.7 Personal reflections

I have spent five years, which constitutes one sixth of my life time so far, doing this research. During this time I learnt many things, starting from the research process and how it changed my way of thinking towards all problems and finding solutions. I have learnt how to take initiative and how to make things happen, not just to wait or accept anything for granted; for example, I found my way in getting involved in NHS CfH events and other related research projects to support my work and achieve my aims. Moreover, working on strategies taught me how it is not possible to achieve my aims without knowing first what I already have and what I need. I have learnt how to keep going forward even when everything seemed to be pulling me backwards. Research is a journey that needs a departure first, as a famous Syrian poet once said "*my aim is not to arrive, but to depart*". Once I started my research journey, I faced many changes in my research and in my life. These changes made me believe that "*change is certain, but to what, this is not!*"

References

Ahmed, I. and Smith, C. (2007) 'Who is going to know about this', NHS CfH Conference on: The Future for Information Sharing in Sexual and Reproductive Health: Making IT Work, 15 March.

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

Anderson, J. (2003) 'Why we need a new definition of information security', *Journal of Computers & Security*, vol. 22, Issue 4, pp. 308-313.

Andress, A. (2004) *Surviving Security: How to Integrate People, Process, and Technology*, 2nd edition, Auerbach Publications, Boca Raton, Florida, USA.

Baker, D. and Masys, D. (1999) 'PCASSO: a design for secure communication of personal health information via the internet', *International Journal of Medical Informatics*, vol. 54, pp. 97–104.

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*, vol. 73, pp. 267-270.

Baldwin, L. Clarke, M. Hands, L. Knott M. and Jones, R. (2003) 'The effect of telemedicine on consultation Time', *Journal of Telemedicine and Telecare*, vol. 9, pp. 71-73

Berner, E. And Simborg. D. (2005) 'Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States', *Journal of the American Medical Informatics Association*, vol. 12, pp. 3-7.

Boddington, T. And Hill, S. (1998) *Preparing for BS 7799 Certification*, British Standards Institution, London.

Boulos, M. N. K. Curtis, A. J. and AbdelMalik P. (2009) 'Musings on privacy issues in health research involving disaggregate geographicdata about individuals',

International Journal of Health Geographics, vol. 8:46.

BS 7799-1:1999, Information security management Part 1: Code of practice for information security management.

Brennan, S. (2005) *The NHS IT Project: The biggest computer programme in the world ever*, Radcliff Publishing Ltd, Oxon, UK,

Burke, G. And Jarratt, D. (2004) 'The influence of information and advice on competitive strategy definition in small-and medium-sized enterprises', *An International Journal of Qualitative Market Research*, vol. 2/2, pp. 126-138.

Cabinet Office (2010) *e-GIF*, url: http://www.cabinetoffice.gov.uk/govtalk/faqs/egif.aspx

Carter M. (2000) 'Integrated electronic health records and patient privacy: possible benefits but real dangers', *The Medical Journal of Australia*, vol. 172, pp. 28-30.

Carter, M. (1998) 'Should patients have access to their medical records? Paradoxically, access to one's own medical records is the best safeguard to privacy', *The Medical Journal of Australia*, vol.169, pp. 596-597.

Chandler, A. (1962) *Strategy and Structure: Chapters in the History of American Enterprise*, Cambridge, MA, USA: MIT Press.

Cimino, J. Patel, V. And Kushniruk, A. (2002) 'The patient clinical information system (PatCIS): technical solutions for and experience with giving patients access to their electronic medical records', *International Journal of Medical Informatics*, vol. 68, pp. 113-127.

Clarke, J. And Meiris, D. (2006) 'Electronic Personal Health Records Come of Age', *American Journal of Medical Quality*, vol. 21, pp.

Coiera, E. (2003) *Guide To Health Informatics*, Arnold, London, UK

Coiera, E. and Clarke, R. (2004) 'E-Consent: the design and implementation of consumer consent mechanisms in an electronic environment', *Journal of American Medical Informatics Association*, vol. 11, pp. 129-140.

Covvey, H. Zitner, D. Berry, D. Cowan, D. and Shepherd, M. (2003) 'Formal structure for specifying the content and quality of the electronic health record', Proceedings of the *11th IEEE International Engineering Conference, IEEE Computer Society*, url: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.134.6451&rep=rep1&type=pdf

Crespin, P. Miller, C. and Batteau, A. (2005) 'Ethnographic research methods'. In Swanson, R. and Holton, E. (2005) *Research on organisations: Foundations and methods of inquiry*, Barrett-Koehler Publishers, San Francisco, California, USA.

Creswell, J. (2003) *Research Design- Qualitative, Quantitative, and Mixed Methods Approaches*, 2nd edition, Sage, London, pp. 191-195.

Detmer, D. (2003) 'Building the national health information infrastructure for personal health, health care services, public health, and research', *BMC Medical Informatics and Decision Making*, vol. 3, url: http://www.biomedcentral.com/content/pdf/1472-6947-3-1.pdf

Dickinson, G. Fischetti, L. and Heard, S. (2004) ' HL7 EHR System Functional Model: Draft Standard for Trial Use', Health Level Seven, url: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.4214&rep=rep1&type=pdf

DoH, Department of Health (2007) NHS Information Governance – Guidance on Legal and Professional Obligations, September, Gateway reference 8523

Eccles, S. (2007) 'Safeguards for sharing: what the National Programme for IT is providing', *NHS CfH Conference on: The Future for Information Sharing in Sexual and Reproductive Health: Making I.T. Work*, 15 March, London.

EHI (2006a) 'Newspaper prints "opt out" coupons for Spine', *E-Health Insider newsletter*, 01 Nov, url: http://e-health-insider.com/news/2235/newspaper_prints_

EHI (2006b) 'DH rejects patient opt-out request', *E-Health Insider newsletter*, 04 Dec, url: http://e-health-insider.com/news/2316/dh_rejects_patient_opt-out_requests

EHI (2008a) 'Four-fifths of doctors say electronic record insecure', *E-Health Insider newsletter*, 03 Jan, http://e-health-insider.com/news/3350/four-fifths_of_doctors_say_electronic_record_insecure

EHI (2008b) 'MPs call for data loss to be a crime', *E-Health Insider newsletter*, 04 Jan, url: http://e-health-insider.com/news/3352/mps_call_for_data_loss_to_be_a_crime

EHI (2008c) 'Medics sceptical about government data security', *E-Health Insider newsletter*, 01 Feb, url: http://e-health-insider.com/news/3438/medics_sceptical_about_government_data_security

EHI (2008d) 'NHS chief execs may be accountable for data loss', *E-Health Insider newsletter*, 28 Apr, url: http://e-health-insider.com/news/3694/nhs_chief_execs_may_be_accountable_for_data_loss

EHI (2008e) 'Tough new laws on data breaches', *E-Health Insider newsletter*, 13 May, url: http://e-health-insider.com/news/3744/tough_new_laws_on_data_breaches

EHI (2010a) 'SCR evaluation finds few benefits', *E-Health Insider newsletter*, 17 June, url: http://e-health-insider.com/news/6006/scr_evaluation_finds_few_benefits

EHI (2010b) 'Government sets out £6 billion cuts', *E-Health Insider newsletter*, 24 May, url: http://e-health-insider.com/news/5932/government_sets_out_£6_billion_cuts

EHI (2010c) 'Osborne orders review of govt spending', *E-Health Insider newsletter*, 17 May, url:http://e-health-nsider.com/news/5916/osborne_orders_review_of_govt_spending

EHI (2010d) 'MH records found in Asda car park', *E-Health Insider newsletter*, 06 May, url: http://e-health-insider.com/news/5885/mh_records_found_in_asda_car_park

EHI (2010e) 'Nurses say technology can cut lost time', *E-Health Insider newsletter*, 04 May, url:http://e-health-nsider.com/news/5874/nurses_say_technology_can_cut_lost_time

EHI (2010f) 'Rotherham: NPfIT has put us back 10 yrs', *E-Health Insider newsletter*, 28 Apr, url:http://e-health-nsider.com/news/5865/rotherham:_npfit_has_put_us_back_10_yrs

EHI (2010g) 'GPs join attack on SCR roll-out', *E-Health Insider newsletter*, 23 Mar, url: http://e-health-insider.com/news/5759/gps_join_attack_on_scr_roll-out

EHI (2010h)' O'Brien claims govt may lock-in NPfIT', *E-Health Insider newsletter*, 02 Mar, url: http://e-health-insider.com/news/5693/o'brien_claims_govt_may_lock-in_npfit

EHI (2010i) 'BMA says 'suspend SCR roll-out'', *E-Health Insider newsletter*, 10 Mar, url: http://e-health-insider.com/news/5716/bma_says_'suspend_scr_roll-out'

EHI (2010j)' BMA says SCR roll-out 'too hasty'', *E-Health Insider newsletter*, 01 Mar, url: http://e-health-insider.com/news/5686/bma_says_scr_roll-out_'too_hasty'

EHI (2010k) 'RCP and CfH launch online standards tool', *E-Health Insider newsletter*, 12 Mar, url: http://e-healt-insider.com/news/5725/rcp_and_cfh_launch_online_standards_tool

EHI (2010l) 'NPfIT future is modular and locally-led', *E-Health Insider newsletter*, 9 Sep, url: http://www.e-health-insider.com/news/6228/npfit_future_is_modular_and_locally-led

Elberg, P. B. (2001) 'Electronic patient records and innovation in health care Services', *International Journal of Medical Informatics*, vol. 64 , pp. 201–205

Electronic Record Development and Implementation Programme (ERDIP),(2003)' *Electronic Records: Lessons from ERDIP,* Version .2 May 2003', [CD-ROM].

Eysenbach G. (2000) 'Consumer health informatics', *British Medical Journal*, vol. 320, 24 June, pp. 1713-1716.

Federal Financial Institutions Examination Council (FFIEC) (1998) *Information Technology Examination Handbook*, June, url: www.ffiec.gov

Federal Financial Institutions Examination Council (FFIEC) (2006) *Information Security, Information Technology Examination Handbook*, July, url: www.ffiec.gov

Fraser, H. Biondich, P, Moodley, D. Choi, S. Mamlin, B. and Szolovits, P. (2005) 'Implementing electronic medical record systems in developing countries', *Journal of Informatics in Primary Care*, vol. 13, pp. 83–95

Fritsche, L. Schröter, K. Gabriela, L. Kunz, R. Budde, K. Neumayer, H. and Hanisch, E. (2001) *A Web–Based Electronic Patient Record System as a Means for Collection of Clinical Data, Lecture Notes in Computer Science*, Berlin and Heidelberg, Germany

Gerber, M. Solms, R. and Overbeek, P. (2001) 'Formalizing information security requirements', *Journal of Information Management and Computer Security*, vol. 9/1, pp. 32-37.

Gerber, M. Solms, R. and Overbeek, P. (2001) 'Formalizing information security requirements', *Journal of Information Management and Computer Security*, vol. 9/1, pp. 32-37.

Gert, H. (2002) 'Avoiding surprises: a model for informing patients', *Hastings Center Report*, vol.32, pp. 23–32.

Glossary of Statistical Terms, url: http://stats.oecd.org/glossary/detail.asp?ID=6903

Greenhalgh, T. Stramer, K, Bratan, T. Byrne, E. Russell, J. Mohammad, Y. Wood, G. and Hinder, S. (2008) *Summary Care Record Early Adopter Programme: An Independent Evaluation by University College London*. University College London, London, UK, url:http://www.haps.bham.ac.uk/publichealth/cfhep/002.shtml)

Guah, M. and Currie, W. (2004)' NHS information quality and integrity: issues arising from primary service provision', *International Journal of Healthcare Technology and Management*, vol. 6, pp. 173-188.

Gunter, T. and Terry, N. (2005) 'The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions', *Journal of Medical Internet Research*, Jan–Mar; vol.7, url: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550638/

Hayrinen, K. Saranto, K. and Nykanen, P. (2008) 'Definition, structure, content, use and impact of electronic health records: A review of the research literature', *International Journal of Medical Informatics*, vol. 77, pp. 291-304.

Health Connect program Office (2002) 'Consent and Electronic Health Records: A discussion paper', *A health information network for all Aust*ralians, Australia, July.

Hone, K. and Eloff1, J.H.P. (2002) 'Information security policy –what do international information security standards say', *Computers and Security Journal*, vol. 21, Issue 5, pp. 402-409.

Hyun, I. (2002) 'A waiver of informed consent, cultural sensitivity, and the problem of unjust families and traditions', *Hastings Center Report*. vol. 32 , pp. 14–22.

Iakovidis, I. (1998) 'Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe', *International Journal of Medical Informatics*, vol. 52, pp.105-15.

ISO/IEC TR 13335-1 (1996) *Information Technology -Guidelines for the Management of IT Security - Part 1: Concepts and Models for IT Security* (First Edition), ISO, Geneva.

Kane, B. and Sands, D. (1998) 'Guidelines for the clinical use of electronic mail with patients', The AMIA Internet Working Group, Task Force on Guidelines for the Use of Clinic-Patient Electronic Mail, *Journal of the American Medical Informatics Association*, vol. 5, pp. 104-111.

Katehakis, D. Sfakianakis, S. Tsiknakis, M. and Orphanoudakis, S. (2001) 'An Infrastructure for Integrated Electronic Health Record Services: The Role of XML (Extensible Markup Language)', *Journal of Medical Internet Research*, vol. 3, Issue 1, Article e7.

Keleber, D. Jha, A. Johston, D. Middleton, B. And Bates, D. (2008) 'A research Agenda for Personal Health Records (PHRs)', *Journal of the American Medical Informatics Association,* vol. 15, pp. 729-736.

Kluge, E. (2004) 'Informed consent and the security of the electronic health record (EHR): some policy considerations', *International Journal of Medical Informatics*, vol. 73, Issue 3, 31 March, pp. 229-234

Kohane, I. Greenspun, P. Fackler, J. Cimino, C. And Szolovits, P. (1996) 'Building national electronic medical record systems via the World Wide Web', *Journal of the American Medical Informatics Association*, vol.3, Number 3.

Ladan, Sh. Yari, A. And Khodabandeh, H. (2006) 'Combination of Information Security Standards to Cover National Requirements', Proceedings of *World Academy of Science and Technology*. vol. 13, Issue 1303.

Longstaff, J. Capper, G. Lockyer, M. and Thick, M. (2000) 'EHR and EPR confidentiality based on accountability and consent: tools for the Caldecott Guardian', *Health Informatics Journal*, vol. 6, pp. 45-52.

Lowe, H. Lomax, E. and Polonkey, S. (1996) 'The World Wide Web: a review of an emerging internet-based technology for the distribution of biomedical information', *Journal of the American Medical informatics Association*, vol. 3, Number 1, Jan / Feb.

Mandl, K. Szolovits, P. and Kohane, I. (2001) 'Public standards and patients' control: how to keep electronic medical records accessible but private', *British Medical Journal*, vol 322, pp. 283-287.

Markus, M. L. (1983) 'Power, Politics, and MIS Implementation', *Communications of the ACM Journal*, Vol. 26:6, pp. 430-444.

Margulis, S. (2003) 'Privacy as a social issue and behavioural concept', *Journal of Social Issues*, vol. 59 (2), pp. 243-261.

Miles, B. and Huberman, A. M. (1994) *Qualitative Data Analysis 2nd edition*, Sage, London, pp.10-11

Mintzberg, H. (1978), 'Patterns in strategy formation', *Journal of Management Science*, vol. 24, pp 934-48.

Mintzberg, H. and Waters, J. (1985) 'Of strategies deliberate and emergent', *Strategic Management Journal*, vol. 6, pp 257-272.

Myers, M. (1999) 'Investigating information systems with ethnographic research', *Journal of Communications of the Association for Information Systems*, vol. 2, Article 23.

NAO National Audit Office, Department of Health (2006) *The National Programme for IT in the NHS*, report by the Comptroller and Auditor General, HC 1173 Session 2005-2006.

NIS00 NIST: National Institute of Standards and Technology. 'An introduction to Computer Security', *The NIST Handbook*, url: www.nist.gov

NHS (1998) *Information for Health: An Information Strategy for the Modern NHS 1998–2005, A national strategy for local implementation*, Published by the NHS Executive September 1998, url: http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4014469.pdf

NHS CfH (2005) *A guide to the National Programme for Information Technology*, brochure Ref. No. 1963a.

NHS CfH (2005) *The NHS Care Record Guarantee for England*, The Care Record Development Board. Published in May 2005 and revised in May 2006.

NHS CfH (2006a) Your Care, *Your Record - Care Record Development Board Annual Conference*, NHS Connecting for Health, London, 23rd Nov.

NHS CfH (2006b) *"Sealed Envelopes" Briefing Paper: "Selective Alerting" Approach*, Crown Copyright, url: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/confidentiality/sealedpaper.pdf

NHS CfH (2007) *IGSoC information pack*, url: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc/links/infopack.pdf

NHS CfH (2008) *Supporting Transformation: A practical guide to NHS Connecting for Health*, url: http://www.connectingforhealth.nhs.uk/engagement/public/partnerships/voluntary/governance/pracguide.pdf

NHS CfH (2010) *Introduction to ISO 27000*, url: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/standards/iso27000

Orlikowski, W. J. (1993) 'CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development', *MIS Quarterly Journal*, Vol. 17, No. 3 (Sep.), pp. 309-340

Peltier, T. (2001) *Information Security Risk Analysis*, Auerbach Publications, div. of CRC Press LLC, Boca Raton, FL, USA, 2001, p. 266.

Posthumus, S. and Solms, R. (2004) 'A framework for the governance of information security', *Journal of Computers and Security*, Vol. 23, pp. 638-646.

Purser, S. (2004) *A practical guide to managing information security*, Artech House, Boston. London.

Orlikowski, W. (1993) 'CASE Tools as Organizational Change: Investigating Incremental and Radical Changes in Systems Development', *MIS Quarterly Journal*, vol. 17, No. 3 (Sep.), pp. 309-340

Orlikowski, W. (1991) 'Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology', *Journal of Accounting, Management and Information Technologies*, vol.1, pp. 9-42.

Papazafeiropoulou, A. and Gandecha, R. (2007) 'Interpretive flexibility along the innovation decision process of the UK NHS Care Records Service (NCRS): Insights from a local implementation case study', *International Journal of Technology and Human Interaction*, vol. 3, pp. 1-12

Rector, A. Nolan W. and Kay S. (1991) 'Foundation for an Electronic Medical Record', *Methods of Information in Medicine*, Vol. 30, pp. 179-86.

Rind, D. Kohane, I. Szolovits, P. Safran, C. Chueh, H. and Barnett, G. (1997) 'Maintaining the Confidentiality of Medical Records Shared over the Internet and

the World Wide Web', *Annals of Internet Medicine*, 15 July, vol. 127, issue 2, pp. 138-141.

Schabetsberger, T. Ammenwerth, E. Goebel, G. Lechleitner, G. Penz, R. Vogl, R. and Wozak, F. (2005) What are Functional Requirements of Future Shared Electronic Health Records?', *Connecting Medical Informatics and Bio-Informatics*, Aug, vol. 1, pp.28-31.

Schabetsberger, T. Gross, E. and Haux, R. (2006) 'Based Transmission of Discharge Summaries to Electronic Communication in Health Care Regions' , *International Journal of Medical Informatics,* vol. 75, pp. 209-215.

Shortliffe E. (1998) 'Health Care and the Next Generation Internet', *Annals of Internet Medicine*, vol 129, Issue 2, 15 July, pp 138-140.

Shortliffe, E. Perreault, L. Wiederhold, G. and Fagan, L. (2000) *Medical Informatics: Computer Applications in Health Care and Biomedicine*, Springer, New York.

Shortliffe, E. and Sondik, E. (2006) 'The public health informatics infrastructure: anticipating its role in cancer', *Journal of Cancer Causes Control*, vol. 17, pp. 861-869.

Slade, R. (2006) *Dictionary of Information Security*, Syngress Publishing, Canada.

Solms, B. (2001) 'Information Security –A Multidimensional Discipline', Computers & Security Journal, Vol. 20, pp. 504-508.

Solms, R. and Solms B. (2004) 'From policies to culture', *Computers and Security Journa*l, vol. 23, pp. 275-279.

Speed, T. and Ellis, J. (2003*)* Chapter 6: Authentication and Authorization, *Internet Security: A Jumpstart for Systems Administrators and IT Managers*, Digital Press, Elsevier Science, USA.

Staroselsky, M. Volk, L. Tsurikova, R. Pizziferri, M. Lippincott, L. Wald, J. And Bates D. (2006) 'Improving electronic health record (EHR) accuracy and

increasing compliance with health maintenance clinical guidelines through patient access and input', *International Journal of Medical Informatics*, vol.7 5, pp 693-700.

Steward, M. (2005) 'Electronic Medical Records: Privacy, Confidentiality, Liability', *The Journal of Legal Medicine*, vol. 26, pp. 491-506

Swindle, O. and Conner, B. (2004) *The link between information security and corporate governance*, url: www.computerworld.com/securitytopics/security/story/0,10801, 92915, 00.html

Takeda, H. Matsumura, Y. Kuwata, S. Nakano, H. Sakamoto N. and Yamamoto, R. (2000) 'Architecture for networked electronic patient record systems', *International Journal of Medical Informatics*, Vol. 60, pp. 161-167.

The Royal Society (2006) *Digital healthcare*: the impact of information and communication technologies on health and healthcare, url: http://regtransfers-sth-se.diino.com/download/sfmimapp/SFMIweb/Rapporter/Ref%20litt/Digital_healthcare_the_impact_of_information_and_communication_technologies_on_health_and_healthcare.pdf

Thick, M. (2007)' The Clinical Office: one year on', *Annual NHS Connecting for Health Clinicians Conference*, 15 November.

Tipton, H. And Krause, M. (2004) *Information Security Management Handbook*, Fifth Edition, pp. 1485, Boca Raton London New York Washington, D.C.: A CRC Press Company, Auerbach Publication

The American Heritage Dictionary (2000) 4th edition. Houghton Mifflin Publishing Company.

The NHS Care Record Guarantee for England, The Care Record Development Board. Published in May 2005 and revised in May 2006.

Ueckerta, F. Goerza, M. Ataianb, M. Tessmanna, S. and Prokoschc, H. (2003) 'Empowerment of patients and communication with health care professionals

through an electronic health record', *International Journal of Medical Informatics*, vol. 70, pp. 99-108.

Ückert, F. Müller, M. Bürkle, T. and Prokosch, H. (2004) 'An electronic health record to support patients and institutions of the health care system', *German Medical Science*; 2: Doc06

US CDC Public Health Law 101 Foundational Course for Public Health Practitioners - Unit 6: Privacy and Confidentiality [http://www2a.cdc.gov/phlp/phl101/docs/PHL101-Unit%206%20-%2016Jan09-Secure.ppt]

Vermeulen, C. And Solms, R. (2002) 'The information security management toolbox-taking the pain out of security management', *Journal of Information Management and Computer Security*, Vol. 10/3, pp. 119-125.

Vries, H. Verheul, H. and H. Willemse,H. (2003) 'Stakeholder identification in IT standardization processes', Standard making: A critical Research Frontier for Information Systems, *MISQ Special Issue Workshop*.

Walsham, G. (1995) 'Interpretive case studies in IS research: nature and method', *European Journal of Information Systems*, vol. 4, pp. 74-81.

Whiddett, R. Hunter, I. Engelbrecht, J. and Handy, J. (2006) 'Patients attitudes towards sharing their health information', *International Journal of Medical Informatics* , vol. 75, pp. 530-541.

Win, K. (2005) 'A review of security of electronic health records', Health *Information Management Journal*, vol. 34, pp. 13-18.

Win, K. and Fulcher, J. (2007) 'Consent Mechanisms for Electronic Health Record Systems:A Simple Yet Unresolved Issue', *Journal of Medical Systems*, vol. 31, pp.91-96.

Winker, M. Flanagin, A. Chi-Lum, B. White, J. Andrews, K. Kennett, R. DeAngelis, C. And Musacchio, R. (2000) 'Guidelines for Medical and Health Information

Sites on the Internet', *Journal of the American Medical Association*, vol. 283, No. 12.

Whiddett, R. I Hunter ,J. Engelbrecht and J. Handy (2006) 'Patients attitudes towards sharing their health information', *International Journal of Medical Informatics* , vol. 75, pp. 530-541.

Wylder, J. (2004) Strategic Information Security, USA: Auerbach Publications.

Yin, R. (1993) *Applications of case study research*, Sage Publishing, Beverly Hills, USA.

Appendices

Appendix A

Staff Information Sheet

Information Security in Electronic Health Records

Case study at (A or B) Hospital

The research study

You are being invited to take part in a research study. Please read this Information Sheet before deciding whether you are happy to take part. I am a researcher conducting a study looking at the patient data security issues involved in Electronic Health Record Systems (EHR). (A or B) Hospital is one of the sites that the study has permission to focus on. I would like to interview you to find out what you would consider to be a satisfactory level of information security in shared health records, and your views towards the development of a security strategy and its implementation in the hospital. This will include you reflecting on current working practices, providing a description of the system you are currently using, specifying particular problems you are facing in the current phase of implementation and making some predictions about expected problems in the future.

Why have I been chosen?

As you are a professional employed by this hospital, and we wish to explore the perceptions of hospital staff who are involved in implementing, developing, maintaining or using the electronic health record system, you have been deemed a suitable participant for this study. Overall, approximately 60 members of staff (30 from this hospital and 30 from another) representing a broad range will be interviewed for this study (e.g. doctors, nurses, IT support staff and managers).

Do I have to take part?

No. Taking part in this research is entirely your own choice. If you decide to take part, you are still free to withdraw at any time without giving a reason. A decision to withdraw at any

time or a decision not to take part in the first place, will not affect your working life in any way.

What are the risks and benefits of taking part?

The information you provide will not adversely affect your working life in any way. The results may help key stakeholders with planning changes and improvements to information security strategies. The interviews will give you the opportunity to express your views and any concerns you may have.

What should I do now and what happens next?

If you are willing to take part, then please sign the Consent Form. I will conduct an interview with you lasting around 30-45 mins. The questions will be focused around your views towards the electronic health record system at Northwick Park Hospital. You are free to decline to answer any question, or withdraw from the interview at any time, without giving a reason.

Confidentiality

Interviews may be tape-recorded and/or notes taken. All tape recordings and notes will be kept confidential and unidentifiable. This means no names will be written on the tapes or transcripts, but a code used instead. The information held on the tapes will only be used for research purposes. On completion of the study all information held on tapes will be stored in a secure place and destroyed after 3 years. All information you provide will be kept strictly confidential and will only be known to the researchers (and not the other professionals you work with). You will not be identified in any future report of the findings.

How will the findings be used?

The findings may be published in professional journals, presented at conferences, and will also be used for a PhD (academic course, resulting in a final PhD report focusing on how to design a framework for developing and implementing an information security strategy in electronic health record systems) being undertaken by myself Yara Mohammad at Brunel University - but remember that your name will not be mentioned. This may help the hospital

and other hospitals develop and improve the services they provide in this area of patient data protection. The findings will be made available to those who wish to see them.

Thank you very much for your time.

Please keep this information sheet in a safe place

If you need more information, please contact:

Yara Mohammad

School of Information Systems, Computing and Mathematics

Brunel University

On 01895 265971

Dr Lampros Stergioulas

Academic Supervisor

School of Information Systems, Computing and Mathematics

Brunel University

Tel. 01895 266044

Fax: 01895 251686

Appendix B

RESEARCH PROJECT
CONSENT FORM (INTERVIEWS)

Title of Project: Information Security in Electronic Health Records

Principal Investigator: Yara Mohammad
(PhD Student at School of Information Systems,
Computing and Mathematics, Brunel University)

PART A: TO BE COMPLETED BY THE INVESTIGATOR:
I confirm that I have explained this research project to the respondent in terms which, in my judgement,
are suited to his/her understanding.

_____ _____ _____

Name of Researcher ***Signature***
Date

PART B: TO BE COMPLETED BY PARTICIPANT:

Please tick

1. I have read the Information Sheet and had the opportunity to ask questions ☐
2. I understand that my participation in being interviewed is voluntary and that I am free to withdraw at any time, without giving any reason ☐
3. I understand that my identity will not be disclosed in any published or written data resulting from this study ☐

_____
Name of Respondent

_____ _____
Signature ***Date***

Appendix C

The semi structure interview schedule

Brief view of what the interview involves:

- This is going to be a fairly short discussion and I'm going to just ask a few basic questions around your opinion and your views about using the electronic health records securely and confidentially.
- You don't have to tell me anything you don't want to and if there is anything you don't want to talk about you must say so and we will move onto another question
- If you want to stop the interview for any reason then let me know - that is not a problem at all and will not affect your care in any way whatsoever…
- Everything you say will be kept totally confidential and your name will not be attached to this information - it will only be known to us as the researchers and not the doctors and nurses involved in your care - this is very important to understand and I absolutely guarantee this
- Are you still happy to go on?
- Please could you read this short information sheet and sign the consent form.

MAIN BODY

Questions – start with lighter/non-sensitive questions

- What do you know about the NPfIT and about the shared health records? (national policy, strength and weakness in the policy)
- Are you involved in developing the EHR services in the hospital? (access control rules, security themes, and data quality)
- Did you have any training on any new EHR system you are currently using or going to use?
- Is everyone in the hospital (staff, health carers) involved in the decision making?
- Do you have any reservations about the implementation of EHR and about the security policy? (what, why, how could they be overcome)
- How do you feel the information security policy should be? (Confidentiality, security, data accuracy)

- Do you feel that security and confidentiality are major issues in EHR?

- Who you do think should have the lead for decision making in setting data protection policy?
- How do you think the patients should take part in decision making about security?
- What are the major problems you face or expect to face with information security and confidentiality (local implementation of EHR security)?
- How usable a smart card system could be for everyday practice? Who do you think should have a smart card? Can you propose any alternative?
- What concerns do you have about system security and data confidentiality?
- Is the available infrastructure sufficient for the implementation of the designed system?
  If not, what additional infrastructure would you like to use/ see in place?
- Is the current EHR system well designed and technically sound?
  If no, how do you think the system should look like?
- Do you think that the system should be compatible with other web applications? Should the system allow patients and doctors to have access to health records from other countries?
  If yes, how should confidential data transmission conducted?

Appendix D

Relevant Legislation

The Act	Date
The Public Records Act	1958
The Access to Medical Reports Act	1988
The Access to Health Records Act	1990
The Computer Misuse Act	1990
The Data Protection Act (DPA)	1998
The Data Protection (Processing of Sensitive Personal Data) Order	2000
The Electronic Communications Act	2000
The Freedom of Information (FOI) Act	2000
The Privacy and Electronic Communications (EC Directive) Regulations	2003
The National Health Service Act	2006

Appendix E

ISO standards

Standard	Standard description
ISO 27001	This is the specification for an information security management system (an ISMS) and replaces the old BS7799-2.
ISO 27002	This is the potential new standard number of the existing ISO 17799 standard (which itself was formerly known as BS7799-1) and outlines a code of practice for information security.
ISO 27003	This will be the official number of a new standard intended to offer guidance for the implementation of an ISMS (IS Management System).
ISO 27004	This is the designated number for a new standard covering information security system management measurement and metrics.
ISO 27005	This is the ISO number assigned for an emerging standard for information security risk management.
ISO 27006	This standard will provide guidelines for the accreditation of organizations offering ISMS certification.

Appendix F

Attended NHS CfH events

Date	Event
10th November 2009	Building a Health Research Support Service - London
17th June 2008	A conference for Nurses, Midwives & Healthcare Practitioners: Cultural Change in Professional Practice - The Information Revolution, London
11th March 2008	Electronic Health Records For Research (London)
13th February 2008	Using Information in the NHS - London SHA (London)
11th January 2008	London Information Managers Forum
15th November 2007	Annual NHS CFH Clinicians Conference
24th October 2007	Summary Care Record & HealthSpace Conference - BY Invitation Only - London
11th September 2007	Management of security for the CRS applications used by London Trusts : the second workshop with BT and NPfit
27th June 2007	Consent and Confidentiality for the London NHS Care Records Service
14th June 2007	London Programme for IT : NHS CRS London Clinical Engagement Conference
15th March 2007	NHS CFH - The Future for Information Sharing in Sexual and Reproductive Health: Making I.T. Work - London
6th March 2007	Quality Data, Quality Care: Unlocking The Language Of Snomed Ct In The Electronic Health Record (Birmingham)
1st March 2007	Half day London Clinical Network Forum
13th February 2007	SUS Data Quality Briefing for London Trusts
19th December 2006	Workshop 5: LORENZO 3.5 Increment 3 - Legitimate Relationships and Data confidentiality
23rd November 2006	Your Care, Your Record - Care Record Development Board Annual Conference
16th November 2006	Health Informatics Workforce Development Workshop
5th October 2006	London Cluster - The NHS Care Records Service - half day

	London Clinical Network Forum
5th October 2006	London Cluster - The NHS Care Records Service - How can London nurses and midwives be involved?

Appendix G

NHS CfH documents

Document title	Publishing Year	Notes
"Sealed Envelopes" Briefing Paper: "Selective Alerting" Approach	2006	
Health care records, whenever and wherever you need them: A guide for NHS staff in England	2006	Ref. No. 2062
A guide to the NPfIT	2005	Ref. No. 1963a
N3 Customer Handbook	2007	Ref. No. 50379
How to register for your NHS CRS Smartcard	2006	Ref. No. 3557
Joint Guidance on Protecting Electronic Patient Information	2006	
PACS- The Story so far DVD	2006	Ref. No. 3257
PACS stakeholder brochure: Celebrating success and looking to the future	2008	Ref. No. 4077
A practical guide to NHS CfH	2008	Ref. No. 4046
An Introduction to NHS HealthSpace	2006	Ref. No. 3567
What you should know about Information Governance	2006	Ref. No. 3453
How Clinicians can get involved with the NPfIT in the NHS	2006	Ref. No. 3502
The NHS Record Service: Better information for better, safer care		Ref. No. 3716
Personal Demographics Service PDS: A guide for general practice	2007	Ref. No. 3955
Summary Care Records- the story so far CD	2007	Ref. No. 4042
Quick Reference to Summary Care Record	2007	Vision 3
The Care Record Guarantee	2007	Ref. No. 3984
The Care Record Guarantee	2006	Ref. No. 2228
The Care Record Guarantee	2009	Ref. No. 3984

Appendix H

E-Health Insider Articles

Article	Date
SCR evaluation finds few benefits	17 Jun 2010
Government sets out £6 billion cuts	24 May 2010
Osborne orders review of govt spending	17 May 2010
MH records found in Asda car park	06 May 2010
Nurses say technology can cut lost time	04 May 2010
Rotherham: NPfIT has put us back 10 yrs	28 Apr 2010
PCTs push on with SCR despite DH stop	22 Apr 2010
SCR roll-out suspended	16 Apr 2010
SCR evaluation costs £1m	09 Apr 2010
GPs join attack on SCR roll-out	23 Mar 2010
O'Brien claims govt may lock-in NPfIT	02 Mar 2010
BMA says 'suspend SCR roll-out'	10 Mar 2010
Letter errors fuel SCR roll-out row	09 Mar 2010
BMA says SCR roll-out ‘too hasty’	01 Mar 2010
RCP and CfH launch online standards tool	12 Mar 2010
Call to scrap 'illegal' NHS patient database	23 Mar 2009
Health coaches get access to patient records	16 Mar 2009
Operating Framework stresses savings and Darzi	09 Dec 2008
Different consent models for coaching services	08 Sep 2008
Tough new laws on data breaches	13 May 2008
NHS chief execs may be accountable for data loss	28 Apr 2008
Medics sceptical about government data security	01 Feb 2008
MPs call for data loss to be a crime	04 Jan 2008
Four-fifths of doctors say electronic record insecure	03 Jan 2008
Patient confidentiality extends beyond death	03 Oct 2007
Call for electronic consent for secondary uses	30 Aug 2007
Patients need assurance on online health records	22 Aug 2007
Overseas data work under review, say reports	26 Nov 2007

Information Governance will be ongoing challenge	01 May 2007
Opt-out consent model to be kept for SCR	18 Dec 2006
DH rejects patient opt-out requests	04 Dec 2006
Newspaper prints "opt out" coupons for Spine	01 Nov 2006

Appendix I

Other documents

Document title	Author	Publisher	Date
Fixing NHS IT: plan of action for a new government	John Cruickshank	2020health.org	March 2010
The Devil's In The Detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes	Trisha Greenhalgh, Katja Stramer, Tanja Bratan, Emma Byrne, Jill Russell, Susan Hinder, Henry Potts	University College London	7 May 2010
Summary Care Record Early Adopter Programme An independent evaluation by University College London	Trisha Greenhalgh, Katja Stramer, Tanja Bratan, Emma Byrne, Jill Russell, Yara Mohammad, Gary Wood, Susan Hinder	University College London	6 May 2008
Government ICT Strategy	Chief Information Officer for the Cabinet Office	Cabinet Office	27 January 2010