An evaluation model for information security strategies in healthcare data systems

Mutiq Mohammed Almutiq

PhD

December 2018

Keele University

Abstract

This thesis presents a newly developed evaluation model, EMISHD (An "Evaluation Model for Information Security Strategies in Healthcare Data Systems") which can address the specific requirements of information security in healthcare sector. Based on a systematic literature review and case study, the information security requirements and the existing evaluation models used to examine the information security strategies of healthcare data systems have been analysed. The requirements of information security in any sector generally vary in line with changes in laws and regulations, and the emergence of new technologies and threats, which require existing information security strategies to be strengthened to deal with new challenges. The systemic review of the existing evaluation models identified from the previous research resulted in the development of a new evaluation model (EMISHD) specifically designed to examine the information security strategies in healthcare data systems according to the specific requirements. A case study of a healthcare organisation in Saudi Arabia is conducted in order to apply the newly developed evaluation model (EMISHD) in a real life case and to validate the evaluation results through observation.

Table of contents

List of Figures

List of Tables

Acknowledgements

In the name of Allah, the most merciful and the most gracious, I praise and thank Him for supporting me with the strength to complete this research, and for surrounding me with knowledgeable and caring individuals during the research process.

This thesis was completed with the support of a number of people and organisations. I particularly appreciate the help and support of my supervisor, Dr Thomas Neligwa. I also would like to thank the participants of my case study. I am grateful to the staff of the School of Computing and Mathematics for their observations and support during the period of the research. This research would not have been possible without the sponsorship of Al-Qassim University, Saudi Arabia. Therefore, I also gratefully acknowledge the support of my sponsors.

During the process of this research I have not been able to share enough time with my family especially my parents, brothers, sisters, and friends. I truly appreciate their patience, support, and good wishes.

I will never forget the support of my wife, daughter, and son, whom I always found patient and supportive of my unusual schedules in the research.

DEDICATION

To my Parents:

Mohammed Almutiq & Norah Al Khafajy

Chapter One:

Introduction

This research aims to develop a model to evaluate the information security strategies of healthcare data systems because, like any other sector, healthcare has its own particular information security requirements (Shoniregun et al. 2010). The set of specific requirements can be derived with reference to the nature of the existing threats to the data, the business requirements to carry out required functions, and the legal, statutory and regulatory requirements of compliance with existing laws and regulations (Shoniregun et al. 2010; Sunyaev 2011). If those requirements are not considered in the development of the information security strategies, it is more likely that data systems will remain comparatively vulnerable, risking consequences in terms of legal or business repercussions (Shoniregun et al. 2010). Increasing numbers of data breaches could make the organisations accountable before law, and negatively affect the trust of their important stakeholders. Therefore, the model for healthcare data systems aimed at in this research can potentially evaluate information security strategies according to their specific requirements. The model can also be expected to avoid legal penalties for healthcare organisations and to build the trust of their stakeholders by curtailing data breaches through the development of strategies based on the specific requirements of data systems.

This chapter presents overviews of general information security requirements in section 1.1, and of information security strategy in section 1.2. Section 1.3 highlights the main information security concerns in healthcare data systems. The intended contribution to knowledge of the study, its objectives, the chosen research methodology, and the structure of the thesis are set out in sections 1.4, 1.5, 1.6 and 1.7 respectively.

1.1 Information Security Requirements

Information can take many forms, and be stored and communicated in many ways, such as electronic or printed copies, transmission over networks, and microfilm records. Regardless of the form in which the information exists, it should be carefully protected throughout its lifecycle. The information lifecycle starts when the information is created, and continues through processing, storage, transmission, copying, usage, through to destruction, loss, or corruption. The general purpose is to protect information assets against existing threats in order to ensure the confidentiality, integrity and availability of the information during its lifecycle according to the business and legal requirements of the organisation (Biskup 2009).

Organisational information security requirements can be divided into two categories. The first category includes the generic requirements common to all organisations irrespective of their type, and the sector or industry to which they belong (Meingast et al. 2006; Ekelhart et al. 2007; Saleh et al. 2007). The second category designates requirements specific to the organisation due to its industry or sector type (Park et al. 2010). For example, the generic requirements or information security goals such as availability, confidentiality, integrity, authenticity and non-repudiation of banking, military or healthcare organisations might be similar, but the specific requirements for each industry are likely to differ depending on their three particular types of information security needs: first, the laws and regulations applicable to them such as US Gramm-Leach Bliley-Act of 1999, Securities and Exchange Commission (SEC) requirements, the USA patriot Act applicable to the American financial sector;

second, the core functions of their businesses that is the main objective of the healthcare organisations is to provide safe and efficient healthcare services to patients, and; third, the nature of the threats they face such as chances of accidental exposure/disclosure of information by internal employees or intentional theft by third party or secondary users of information who are not properly checked or motivated hackers attracted towards information for their personal benefit.

Common security threats that any information system might face include the disclosure of a customer's private data, threats resulting from end users' negligence, information misuse, unethical hacking, unauthorised access to data centres, malware, and viruses (Tipton & Krause 2004; Wiant 2005). Such threats also include network or system failure, version control problems, inadequate documentation, natural disasters, and destruction by fire (Purser 2004; Tyson & Slocum 2012). Any of these threats might lead to significant management concerns, such as the loss of customer confidence, business losses, security costs, and loss of market reputation and/or business continuity (Siougle & Zorkadis 2002; Park et al. 2010). For further details on these threats, see section 3.3 in Chapter Three.

1.2 Information Security Strategy

Information security, as implemented through a systematic application of technical and non-technical resources according to a pre-articulated plan, is often referred to as an information security strategy (Hamill et al. 2005; Schumacher et al. 2006; Knapp et al. 2009; Vladimirov et al. 2010; Park et al. 2010). ‘Technical’ in this context refers to hardware, software and firmware, while non-technical resources comprise policies and procedures (Hamill et al. 2005). Strategies are primarily based on the standards which have been generically developed for general information systems by national, regional or international organisations such as the British Standards Institute (BSI), the European Standards Organisation (ESO), and the International Standards Organisation (ISO). Different types of businesses can develop and apply chosen strategies by selecting the relevant controls from the existing standards according to their business objectives, relevance, and available resources. Controls are selected and applied from a range of broader control categories to reflect the overall strategy of the organisation (Chandler 1962; Mintzberg 1978; Burke & Jarratt 2004; Mohammad 2010).

An effective strategy is expected to ensure the smooth functioning of data systems in line with organisational business requirements, and to highlight any vulnerabilities (Dogaheh 2010). A successful strategy utilises the available resources in the form of human workers, technology, and processes in a manner that allows the development of a secure system (Eminağaoğlu et al. 2009; Tarwireyi et al. 2011). This secure system should provide sufficient security against malicious attacks, unauthorised access and accidental damage to information assets, in line with the security objectives of the organisation (Norman 2011; Jirasek 2012).

The effectiveness of a strategy can be measured with the help of plans, templates, or representations which can be used as models to execute evaluation activity from start to finish (Yoo et al. 2007; Jafari et al. 2009). The common parts of an evaluation activity include pre-evaluation planning, evaluation, analysis, and reporting (Hamill et al. 2005; Yoo et al. 2007; Dogaheh 2010). The ability of an evaluation model to measure the strengths and weaknesses of a strategy in the context of specific requirements can be helpful in highlighting and addressing information security issues, thus improving an organisation’s strategies and enabling it to achieve better future results (Yoo et al. 2007; Jafari et al. 2009).

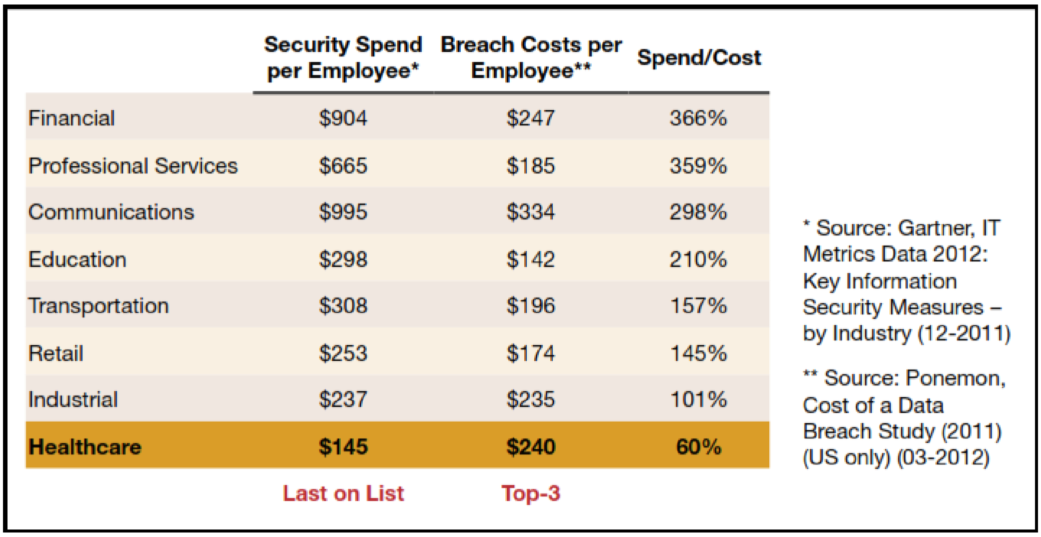
1.3 Information Security Concerns for Healthcare Data Systems

Healthcare recognises the benefits of the adoption of information technologies in the form of more efficient data processing, storage, sharing and management (Shoniregun et al. 2010). The development of Electronic Healthcare Records (EHRs) makes the storage, processing and retrieval of health-related data easier and quicker. However, the improved ease of access is offset by an increased level of information security risk; therefore, a trade-off is required between the levels of access and of information security.

While controls have been introduced to increase privacy, healthcare providers require uninterrupted access to information in order to ensure the timely delivery of critical health services. Given that many partners are involved in healthcare, some of whose trustworthiness may not be guaranteed, the level of risk is increased in distributed environments (Smith & Eloff 1999). Therefore, the development of strategies that facilitate the required balance between privacy and availability so that all legal and business requirements for privacy are adequately met can be challenging. The data must also be accurate to enable providers to deliver the correct services (Brooks & Warren 2006). This requirement is arguably more critical in healthcare than in any other type of organisation, because human health and lives are at stake (Smith & Eloff 1999).

The situation becomes more complicated because organisations often have their own security strategies which may be inconsistent and incompatible with each other, and with those of the EHRs (Kuang & Ibrahim 2009). Patient consent is required prior to the adoption of EHRs, and the consent mechanisms required by law to ensure the privacy and confidentiality of patient data are significant, and represent a much-debated hindrance to the growth of EHRs (Kluge 2004).

Information security concerns in relation to EHRs are significant, as more than 18 million patient records were exposed between 2009 and 2011 in the USA, costing the healthcare industry $6.5 billion per year on average (Tyson & Slocum 2012). The reported number of breaches resulting in the accidental exposure of the records in the USA increased to 29.3 million between 2012 and 2014, marking a significant increase on the previous period (McCann 2014). Experts also believe that if unreported cases of such breaches were also taken into account, the actual number would be between 40 to 45 million, an approximate 138 percent increase on the reported figures (McCann 2014). A study in 2011 revealed that 96 percent of healthcare providers had faced at least one data breach during the previous two years (Tyson & Slocum 2012); at around the same time, another report disclosed that two of the top six data breaches in 2011 had occurred in the healthcare sector (Tyson & Slocum 2012). Each year in the USA, 90 percent of all businesses are affected by security breaches of some kind, costing a total of $17 billion (Doherty et al. 2009). Although the cost per breach in healthcare is higher (see Figures 1.1 & 1.2) than in other sectors, the sector's spending on information security is far lower (see Figure 1.1).



	Security Spend per Employee*	Breach Costs per Employee**	Spend/Cost
Financial	$904	$247	366%
Professional Services	$665	$185	359%
Communications	$995	$334	298%
Education	$298	$142	210%
Transportation	$308	$196	157%
Retail	$253	$174	145%
Industrial	$237	$235	101%
Healthcare	**$145**	**$240**	**60%**
	Last on List	Top-3	

* Source: Gartner, IT Metrics Data 2012: Key Information Security Measures – by Industry (12-2011)

** Source: Ponemon, Cost of a Data Breach Study (2011) (US only) (03-2012)

Figure 1.1 Spending compared to the overall cost of a breach (Tyson & Slocum 2012)

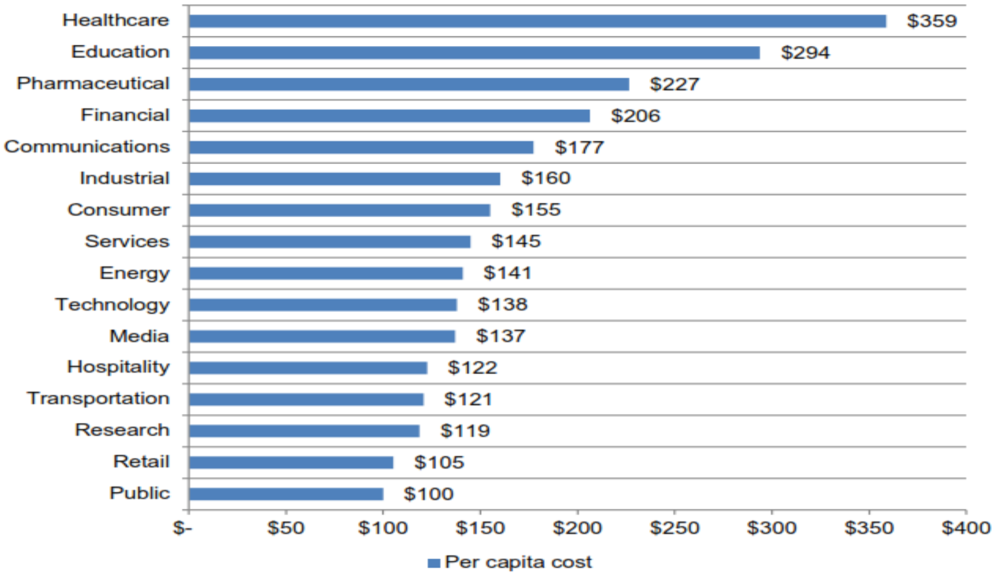
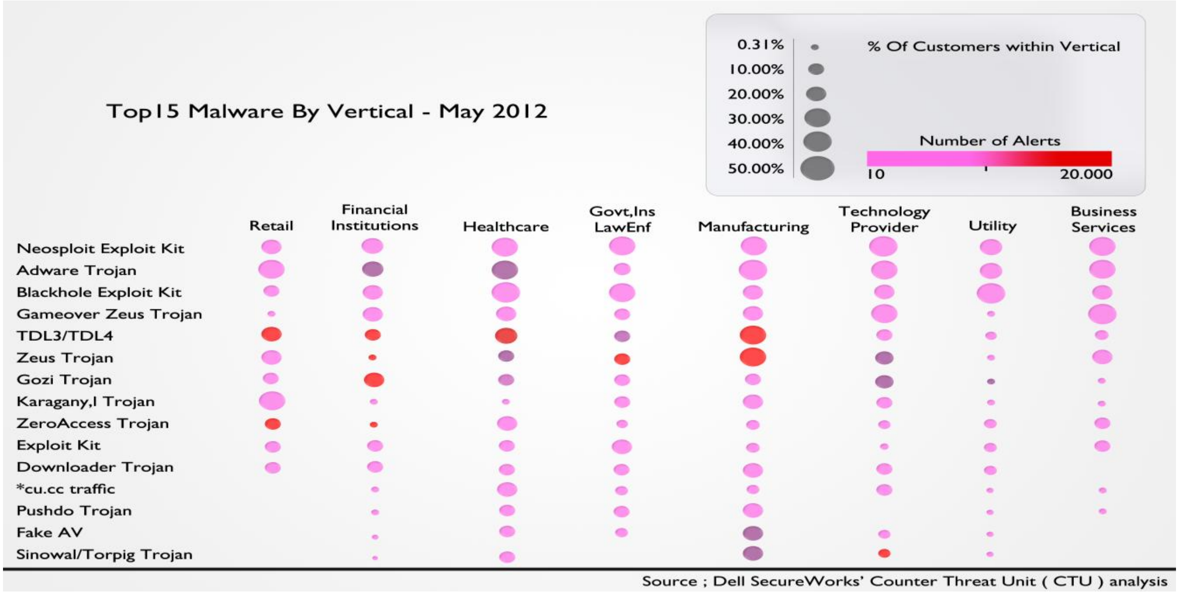


Figure 1.2 Breach cost per capita by industry classification (IBM 2014)

Another reason for the higher cost per breach in healthcare compared to other sectors is that it is subject to more breaches. Figure 1.3 shows a comparison of malware attacks on different organisations during May 2012: healthcare is one of the most-attacked sectors (Tyson & Slocum 2012). Accordingly, the privacy of patients' data is a matter of great concern and is subject to legal requirements in any electronic healthcare system, which must be considered from the early stages of the system's analysis and design.



Source ; Dell SecureWorks' Counter Threat Unit (CTU) analysis

Figure 1.3 Top 15 Malware by Vertical—May 2012 (Tyson & Slocum 2012)

The number of breaches in information security is increasing over time. The cost per breach is also increasing, with the result that IT is particularly costly for healthcare providers. The costs incurred because of breaches includes the damages, penalties and fines specified by the laws of the country involved (Tyson & Slocum 2012). Other challenges, such as the relatively higher number of communicating partners, inconsistent information security strategies, and the legal requirements of privacy, can further complicate the situation. Therefore, in order to minimise the cost per breach and to increase the level of trust in EHRs, strategies must be able to restrict (or, ideally, eliminate) information security breaches (Jafari et al. 2009). Abandoning the use of IT is not an option, so the only solution lies in the improvement of the state and quality of the strategies which organisations employ.

1.4 Contribution to Knowledge

The information security strategies applied in data systems can be improved to restrict data breaches more effectively, if those strategies are based on the specific information security requirements of organisations in a sector. Evaluation models can help healthcare providers to achieve this goal by detailing the specific requirements of information security. However, the existing audit oriented approaches to evaluation utilise audit checklists based on the information security standards in order to evaluate the security controls selected and implemented in healthcare organisations. Such approaches lack a clear and precise criteria to determine if a selected or implemented control meets the specific requirements of information security in healthcare sector. This research contributes into existing knowledge by devising such an evaluation criteria by developing a questionnaire to test healthcare specific information security requirements (Table 4.1) which can help the evaluators to judge if a security control meets the information security requirements of healthcare sector.

1.5 Research Objectives

This research has the following research objectives to:

- Compare an information security strategy for healthcare data systems and its specific requirements, as distinct from generic information security strategies;
- Analyse the existing evaluation models for information security strategies in healthcare data systems;
- Develop a new evaluation model which can address the specific requirements of information security strategies in healthcare data systems; and
- Apply and validate the new evaluation model using an actual case study of a healthcare organisation.

1.6 Research Methodology

This is an empirical research study and involves both qualitative and quantitative data, so these two research methods were both applied to collect the data. A systematic literature review was carried out to collect and analyse the related evidence using a systematic and scientific method to collect qualitative data, mainly from articles located in selected databases (for more details, see section 2.1). The case study method was applied to collect quantitative data via a checklist for the evaluation of the information security strategy of a hospital in Saudi Arabia (for more details, see section 2.2).

1.7 Structure of the Thesis

This thesis is organised into six chapters. Chapter Two explains the research methods, describing how the systematic literature review (SLR) and the case study were applied to achieve the objectives of this research.

Chapter Three describes the application and findings of the systematic literature review (SLR) in relation to the research questions. The findings of the chapter help to build understanding of the requirements of information security and strategy in general, and in the specific context of healthcare in particular.

Chapter Four presents the new evaluation model which was developed in this study based on the SLR findings.

Chapter Five discusses the application of the newly developed model to evaluate the information security strategy of a healthcare provider. The objective of applying the evaluation model was to validate the model.

Chapter Six is about conclusions of this research.

Chapter Two:

Research Methodology

In this thesis two methods have been used, namely: a systematic literature review (SLR) and a case study of a hospital. The systematic literature review (SLR) is discussed generally in Section 2.1. Further, the planning of the SLR for this research is explained in section 2.2, and subsequently the research questions in 2.1.1 are set out. These sections include some of the key parts of the SLR protocol for completeness of discussion (the full protocol is attached as Appendix-A). Then the case study is set out in section 2.3. A summary of the chapter is given in section 2.4.

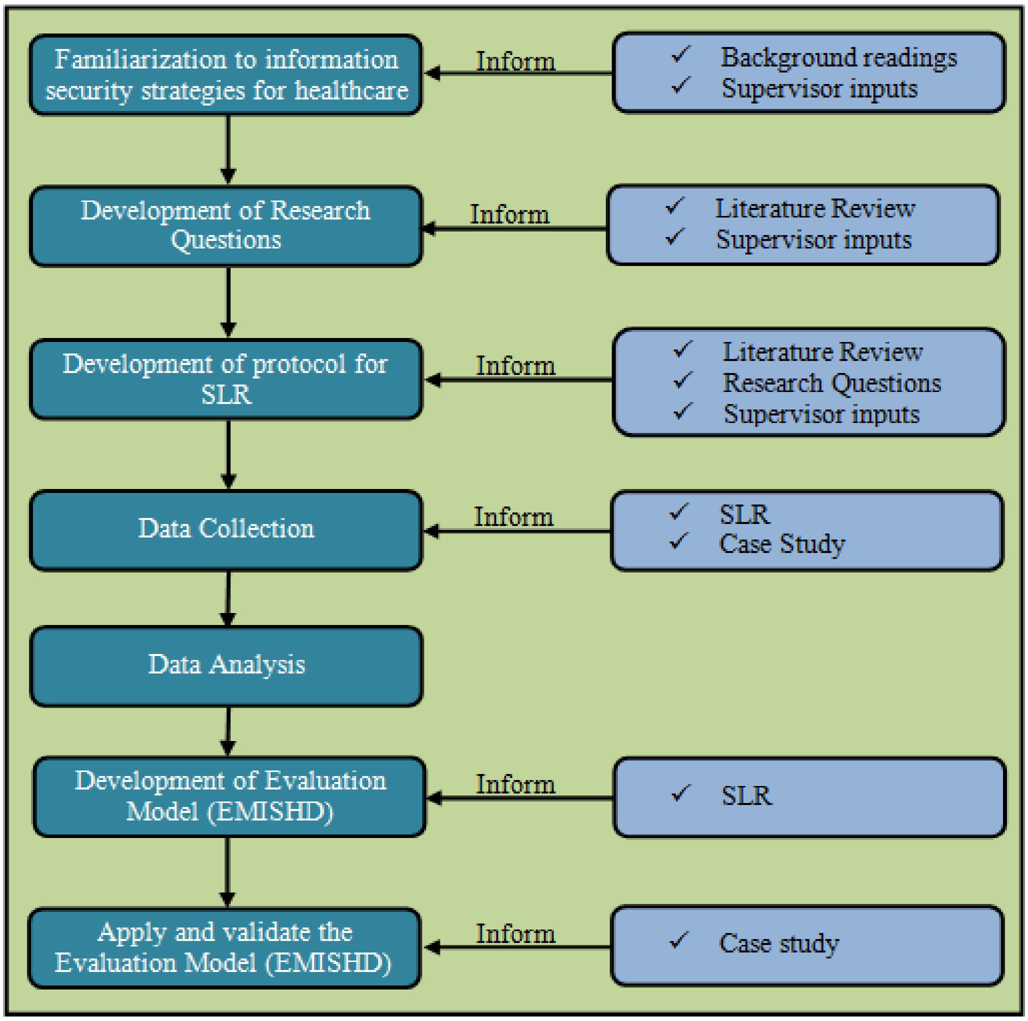


Figure 2.1 Research stages and activities

2.1 The systematic literature review (SLR)

The systematic literature review (SLR) in the present study was used to collect and analyse the evidence to answer the five research questions (set out in Chapter 3) in order to develop an evaluation model capable of evaluating the information security strategies of healthcare data systems. Kitchenham (2004) defines the SLR as “a means of evaluating and interpreting available research relevant to a particular research question, topic area, or phenomenon of interest”. The aim of this research is to collect and analyse the available evidence about the information security strategies of healthcare data systems and evaluation models and to evaluate them so that existing practices can be recommended, or a change suggested in the evaluation methods for healthcare data systems. The SLR was proposed to conduct this present study because it involves five questions, and is deemed an effective method to deal with the multiple questions posed in research (Da Silva et al. 2011). Moreover, the SLR was also chosen in the present study because it is a well-defined-process for the identification, assessment, and analysis of primary studies in order to answer specific research question(s) (Kitchenham & Charters 2007). Systematic reviews require formal planning and systematic and scientific execution, in contrast to ordinary literature reviews which do not necessarily have such features. SLRs are scientifically significant, as they aim to be replicable by independent researchers and are used to present “a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology” (Kitchenham 2004).

Furthermore, SLRs are also significant as a method of investigation as they are able to support the development of evidence-based software engineering. The objectives of evidence-based studies include the identification of the most relevant evidence with which to answer the research questions, and the critical evaluation of evidence by assessing its validity and usefulness (Kitchenham 2004). Therefore, SLRs are important not only as an approach to finding, reading and evaluating the previous research and comprehensively and impartially summarising its results, but also to selecting the right studies (Greenhalgh 2010). After a careful reading of the most valid and useful studies, it is possible to suggest changes to practices, or to endorse existing practices (Da Silva et al. 2011). Therefore, the SLR has potential to support "research and education, and informing practice on the impact or effect of technology" (Da Silva et al. 2011).

However, like every other methodology, the SLR is not without some weaknesses, despite the strengths just listed here. For example, the SLR is a well-defined methodology, argue Kitchenham and Charters (2007), that attempts to minimise biases in results, but it is unable to protect against publication bias in primary studies, which means more positive results having been published in them than negative ones. In medicine, Cochrane Collaboration facilitates researchers in registering controlled trials, then follows up the trials, whether they are published or not. At present, there is no equivalent support in software engineering which will help to follow and check the overestimation of the effect of size in systematic reviews or the under-estimation of risks in order to check for publication bias (Kitchenham et al. 2004).

Informed by the strengths and challenges of evidence-based software engineering, guidelines by Kitchenham (2004) cover the three important phases of SLR research: planning, conducting, and reporting the reviews. In the planning phase, it is necessary to determine if an SLR is required, and any existing SLR in the area of interest has already been done, and should be critically reviewed. Review protocols are developed to specify the methods to be used and to reduce researcher bias (Kitchenham 2004). In the conducting phase, the relevant research is identified, selected and assessed for quality; the relevant data is carefully extracted, and the data is synthesised (Kitchenham

2004). Finally, in the reporting phase, the results of the SLR are reported in a journal or conference paper, or in a technical report or research thesis (Kitchenham 2004).

2.2 Planning the Review (SLR Protocol)

The first important phase of a systematic review is the planning and development of the protocol, which explains all the steps involved in the review in a logical and structured manner and sets out the rationale for selecting the topic and a description of the research questions, along with specifications of the population(s) of interest, intervention(s) and the outcomes, exclusion/ inclusion criteria for the selection of studies, the chosen process for data extraction, and the quality assessment criteria for the selected studies (Kitchenham & Charters 2007). The SLR protocols developed by other experts in the field were consulted in this research (Staples & Niazi 2008; Khan 2011; Niazi et al. 2006; Niazi et al. 2005) and the proposed protocol was reviewed by one internal and two external experts, then improved according to their feedback (see protocol in Appendix A).

2.2.1 Research questions

Healthcare is an essential services sector and needs dependable information security to ensure safe and efficient delivery of healthcare services. However, information security in healthcare is a challenging task because information security strategies being used in the sector cannot meet the specific requirements of the sector. Not only the delineation of specific requirements seems lacking, but also the evaluation models seem missing which can actually measure the information security strategies of healthcare data systems according to those specific requirements. Therefore, the purpose of this thesis is to develop such an evaluation model to measure the effectiveness of information security strategies of healthcare data systems according to the specific requirements of the sector.

In order to accomplish these objectives and to ensure the collection of all the most pertinent data, several research questions were produced, to guarantee a comprehensive study of the research area while also providing a deep analysis of the past use of information security strategies in healthcare data systems. The research questions for this study were:

RQ1. What is information security?

RQ2. What is an information security strategy?

RQ3. What is an information security strategy for healthcare data systems?

RQ4. How can the effectiveness of an information security strategy be measured?

RQ5. How can the effectiveness of an information security strategy in healthcare data systems be measured?

2.2.2 Search strategy

Identifying search terms

In line with Kitchenham & Charters (2007), the following search strategy was used for the construction of the search terms:

a. Use the Research Questions for the derivation of major terms, by identifying the population, intervention and outcome;

b. For these major terms, find alternative spellings and synonyms;

c. Verify the key words in any relevant paper;

d. Use Boolean Operators for conjunction if the database allows, in such a way as to use the 'OR' operator for the concatenation of alternative spellings and synonyms, whereas 'AND' is for the concatenation of major terms.

The results in relation to each of the above were as follows:

Results for (a)

The following details assisted in designing appropriate search terms related to the research questions:

Population: Information security strategy in healthcare data systems

Intervention: To measure the effectiveness of the strategy

Outcomes of relevance: Trust, meeting the information security requirements.

Experimental Design: Theoretical studies, empirical studies, case studies.

Results for (b)

Keyword	Alternatives or Synonyms
Information	Data, records
Security	Safety, Protection, Assurance
Strategy	Policy, Approach, Plan, Model, Framework
Healthcare	Patient care, Health, Hospital, Medical, Clinical
Systems	Database, Data Systems
Measure	Evaluate, Assess, Monitor, Appraise, Audit
Effectiveness	Success

Table 2.1 Alternative or Synonyms of the Research Questions

Results for (c)

Information

Security

Strategy

Healthcare

Systems

Measures

Effectiveness

Results for (d)

RQ1: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance")).

RQ2: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”)).

RQ3: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Patient care” OR “Healthcare” OR “Hospital” OR “Clinical” OR “Health” OR “Medical”)).

RQ4: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Measure” OR “Evaluate” OR “Assess”

OR “Monitor” OR "Appraise" OR "Audit") AND (“Database” OR “Data Systems” OR “Systems” OR “Effectiveness” OR “Success”)).

RQ5: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Patient care” OR “Healthcare” OR “Hospital” OR “Clinical” OR “Health” OR “Medical”) AND (“Measure” OR “Evaluate” OR “Assess” OR “Monitor” OR "Appraise" OR "Audit") AND (Database” OR “Data Systems” OR “Systems” OR “Effectiveness” OR “Success)).

2.2.3 Resources searched

The search strings already developed in the protocol were used to conduct searches (see the Protocol in Appendix A). Initially, nine electronic databases were searched. After a careful examination of the results, and based on their relevance and a discussion with the author’s research supervisor, six of the nine databases were identified as potentially useful: ScienceDirect, ACM Digital Library, IEEE Xplore, EBSCOhost, Cite Seer Digital Library and Google Scholar. Trial searches were made to test the effectiveness of the search strings, and the results confirmed that they were appropriate. On applying the search strings, 8473 relevant results were initially found.

2.2.4 Search documentation

It was decided that the search results should be documented in the format shown in Table 2.2, below:

Name of database	Search strategy	Search string no.	Date of search	Years covered by search	Total Results Found	Initial selection	Final selection
ScienceDirect	((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Patient care” OR “Healthcare” OR “Hospital” OR “Clinical” OR “Health” OR “Medical”) AND (“Measure” OR “Evaluate” OR “Assess” OR “Monitor” OR "Appraise" OR "Audit") AND (Database” OR “Data Systems” OR “Systems” OR “Effectiveness” OR “Success)).	Trial search	30 of March 2012	All years			

Table 2.2 Search Documentation form

2.2.5 Selection criteria

2.2.5.1 Inclusion criteria

For inclusion criteria, it was decided that a set of research conducted and published as papers or articles would be created. This review would then be used for data extraction. The criteria are listed below:

- Studies that identify information security in general, and health care systems in particular;
- Studies that identify the models which can be used to measure the level of information security in healthcare data systems;
- Studies that identify factors which affect information security in healthcare data systems;
- Studies of the constraints and limitations affecting information security strategies in healthcare data systems;
- Studies that identify strategies and guidelines relating to information security in healthcare systems.

2.2.5.2 Exclusion criteria

Exclusion criteria were also formulated to determine which pieces of literature would be excluded due to being outside the scope of the research. These criteria were as follows:

- Studies that are not related to the research questions;
- Studies that do not describe information security in general or healthcare data systems in particular;
- Studies that are only related to healthcare, not information security;
- Studies where only the abstract is available, not the full text;
- Studies written in a language other than English;
- Studies which have not been peer reviewed.

2.2.5.3 Selection process

The initial selection was done by reviewing the title, keywords and abstract in order to exclude results that were not related to the research questions. The final selection was verified from the primary sources selected in the initial selection process according to the criteria for inclusion/ exclusion by carefully reviewing the full text of each study.

2.2.5.4 Publication quality assessment

The assessment of quality in publications was to be completed concurrently with the data extraction, and the measurement of quality was achieved after the final selection of publications. The quality checklist comprised the following questions:

1. Is the paper based on research, or is it a "lessons learned" report based on expert opinion?

2. Is there a clear statement of the aims of the research?
3. Is there an adequate description of the context in which the research was carried out?
4. Was the research design appropriate to address the aims of the research?
5. Was the recruitment strategy appropriate to the aims of the research?
6. Was there a control group with which to compare treatments?
7. Was the data collected in such a way that addressed the research issue?
8. Was the data analysis sufficiently rigorous?
9. Has the relationship between researcher and participants been considered to an adequate degree?
10. Is there a clear statement of findings?
11. Is the study of value for research and practice?

A spreadsheet was created so that each study could be assigned a value of either 1 (Yes) or 0 (No). The first three of the above criteria were used to exclude non-research items and studies without sufficient clarity of aims from the review. These factors represented the minimum quality threshold.

2.2.5.5 Data extraction strategy

Primary Study Data

The aim of the present study was to gather data for review from prior publications which focused on the given research questions. The following data was extracted from each publication (Kitchenham & Charters 2007):

- Publication details (Title, Author(s), Journal/Conference title, etc.)

- Data that addresses the research questions.

The following Table, 2.3, presents the data captured and the extraction form used.

Data extracted by the SLR
✓ Reference
✓ Goals and Requirements of Information Security and Information Security Strategy.
✓ Goals and Requirements for Healthcare Information Security Strategy.
✓ Evaluation Models used to assess the effectiveness of Information Security Strategy.
✓ Evaluation Models used to assess the effectiveness of Information Security Strategies of Healthcare Data Systems.

Table 2.3 Data Extraction Form

2.3 Case study

A case study is used to carry out a detailed study of a limited, small number of cases (Rugg & Petre 2007). Normally, such studies are based on one or two specific cases (Mohammad 2010; Aldajani 2012) which help the researcher to achieve an in-depth focus and gain rich understanding (Rugg & Petre 2007). A limitation of case studies is that similar practices in other cases remain unknown (Rugg & Petre 2007). However, a case study can provide a basis for a detailed survey for future research.

Since the use of SLR leads to developing an evaluation model with which to evaluate the information security strategies of healthcare data systems (for more details, see Chapter three and four of this present thesis), the case study of a hospital in Saudi Arabia was also chosen for use in this research, for two purposes. First, to apply the evaluation model developed through the SLR findings to a real case setting in healthcare; and second, to observe the information security practices of the healthcare professionals related to the hospital's information security strategy to validate the evaluation results based on the application of the evaluation model. The total period for this case study was 30 days, equally divided into two tasks: applying the evaluation model, and performing observation.

2.3.1 Applying the evaluation model

As was mentioned above, the first purpose of the chosen research methodology was to apply the evaluation model to a real-life case of healthcare data systems. The Information Technology Department of the hospital is responsible for developing and implementing information security strategy. The first task was to evaluate the information security controls applied by the hospital using a checklist (described later in Chapter Five), with the assistance of one of the staff members responsible for information security according to the evaluation criteria.

2.3.2 Validation of the evaluation model through a disclosed non-participant observation

Knowledge based on short-term and long term memories exists in predictive, tacit, semi-tacit, or explicit forms (Rugg & Petre 2007). Predictive knowledge is based on information about future behaviour, while explicit knowledge refers to the information that humans know precisely and can easily explain through language. Implicit knowledge is based on the information about skills that can be demonstrated by, but not expressed exactly, through words. Semi-tacit knowledge is based partly on both explicit and implicit types of knowledge (Rugg & Petre 2007). Knowledge in the real world may exist in explicit, implicit, or semi-implicit forms, and can be accessed through different types of research approaches such as case studies, field experiments, controlled experiments, surveys, and case studies. Case study is deemed the most suitable method when variables cannot be controlled and implicit or semi-implicit knowledge attached to natural/real life practices needs to be accessed.

This present study aims not only to develop an evaluation model to evaluate information security strategies for healthcare data systems, but also to apply and validate this model by noting the practices of users of the information technology in healthcare environment who are tasked with implementing the information security strategies. Information security practices at a healthcare facility can be studied in different ways, such as using direct or indirect, participant or non-participant, and disclosed or undisclosed types of observation. Direct observation means that the phenomenon is directly observed while it is happening, while indirect observation is made possible through observing relevant records, registers, and papers describing past events. Participant observation means working with the group under study as part of the group, while non-participant observation requires no direct participation in the process. Disclosed participation, for ethical reasons, requires that the subject group is informed about the intentions and objectives of the study; in contrast, undisclosed participation is ethically unacceptable for educational purposes as the group under study is not informed about the objectives and intentions of the participation (Rugg & Petre 2007).

This present study uses both direct and indirect disclosed non-participant observation to understand the practices related to the information security strategy of a case study healthcare facility. Document analysis was used for indirect observation, and disclosed non-participant observation was used to observe the practices of healthcare professionals, as the most important users of healthcare data systems.

Documents such as information security policies, directions and guidelines, evaluation reports, official hospital webpages, records of information security issues, and relevant laws and regulations, were accessed and analysed in order to understand the information security strategy of the hospital. The purpose of the non-participant direct observation at the hospital was to cross-check the evaluation results derived through the evaluation model. The identified weaknesses in the strategy would potentially allow some practices by healthcare providers which may violate the legal and business requirements of healthcare data systems, and leave them vulnerable to the external threats.

2.3.3 Ethical considerations

Any research at Keele University involving human participants requires ethical approval from the Ethics Research Committee, which was duly sought for this research to ensure the protection of subjects from harm, deception or loss of privacy. Ethical considerations require the research to be conducted in such a manner that respects the interests of the participants at all times. Approval from the host organisation (the hospital in Saudi Arabia) was also acquired in advance. All the research participants were provided with an information sheet describing the aims and processes of the study. The role of the researcher and the participants was also made clear, and informed consent from the participants was sought and received in writing. The privacy and confidentiality of participants has been maintained throughout this research and thesis.

2.4 Summary of the Chapter

The SLR was chosen and deployed as a systematic research method by which to collect data from previous research articles, in order to develop an evaluation model for healthcare data systems. The newly developed model was then applied and validated through a case study by means of document analysis and disclosed non-participant observation.

Chapter Three:

A Systematic Literature Review of Information Security Strategies

This chapter describes the process of conducting Systematic Literature Review in Section 3.1. Further, it gives the research findings of the SLR for the five research questions: RQ1, RQ2, RQ3, RQ4 and RQ5, which are discussed in sections 3.2, 3.3, 3.4, 3.5 and 3.6 respectively. The limitations and lessons learned from the SLR are discussed in section 3.7, and a summary of chapter is given in section 3.8.

3.1 Conducting the Review

3.1.1 Selection of studies

The following table (Table 3.1) describes the final selection of articles found in each of the databases using the search strings. Of the initial 8473 articles found in the six databases, the number was reduced to 231 (after reading the title and abstract) in the next phase, using the inclusion/exclusion criteria. Many of the articles in the rejected group were about healthcare or information technology, but from various different perspectives. The number was further reduced to 114 after a thorough reading of each article. A very small number of studies did not meet the minimum quality threshold. Ultimately, **109** articles were identified as useful and relevant to the present research. The search results are given in Table 3.1

Sr. No	Database	Final selection
1	Google Scholar	36
2	ScienceDirect	29

3	IEEE Xplore	22
4	ACM Digital Library	8
5	EBSCOhost	7
6	Cite Seer Digital Library	7
Total of selected articles		**109**

Table 3.1 Total Results Found in the SLR

3.1.2 Data extraction

Data extraction was carried out systematically through a detailed and careful examination of the relevant studies. A data extraction form was developed, and the following data was extracted:

- Publication details (Title, Author(s), Journal/Conference title, etc.);
- Data which addresses the research questions.

The form for data extraction is attached as Appendix B at the end of this thesis.

3.1.3 Quality assessment

All 114 selected articles were assessed for quality at the same time as data extraction. The quality of each study was determined by pre-set criteria based on a prior study (Dybå & Dingsøyr 2008). These criteria were used in the SLR when faced with a number of different study types. The present SLR pulled together studies of different types; therefore, these criteria were considered appropriate and useful.

The questions in the quality assessment process were answered Yes or No, with corresponding values of 1 or 0 assigned to reflect the answer. The first three criteria were used to exclude non-empirical research items and studies lacking sufficient clarity of aims. This factor represents the minimum quality threshold. In total, five studies were rejected due to not meeting the minimum quality criteria (Brenner 2010; Anthes 2010; Lampson 2009; Hoffmann 2009; Saydjari 2006). The aims of the remaining eight criteria were to determine the rigour and credibility of the research methods applied, and to determine the relevance of each of them to the SLR (see Appendix C for the results of the quality assessment).

Testing and Validation of Question Responses

The SLR was based on a validated protocol which contained clearly defined search strings. It was ensured that these search strings were replicable. Similarly, the quality assessment criteria were explicitly identified. Based on the clearly explained logic behind the attributed values, quality assessment could be applied by any researcher in future. This quality assessment thus had an objective repeatability feature.

3.1.4 Data synthesis

As mentioned above, 109 articles were finally considered as relevant to the SLR and were accepted. The cut-off date for the SLR was 01.11.2016 and after this date no new studies were included in the review. The relevant data for all the research questions was extracted and further analysed individually in relation to each research question. The results based on the data extraction and data analysis for the SLR are discussed in chapters 3 and 4.

3.2 Findings for RQ1: What is information security?

In total, 38 articles were selected to answer the RQ1. The purpose of this question was to understand the concept, goals, and requirements of information security. The findings are discussed below.

No	Areas covered	Selected studies from the SLR for Research Question One
1	Contextualising Information security	(ISO/IEC13335-1 1996), (Bakker 1998), (Gritzalis & Lambrinoudakis 2000), (Loef et al. 2002), (Kankanhalli et al. 2003), (Kotulic & Clark 2004), (Hamill et al. 2005), (Blyth & Kovacich 2006), (Booker 2006), (Kiely et al. 2006), (GAO 2006), (Schumacher et al. 2006), (Pishva et al. 2007), (Doherty et al. 2009), (Biskup 2009), (Jafari et al. 2009), (Kuang & Ibrahim 2009), (Sunyaev 2011), (Kumar & Puri 2012), (Mohapatra & Singh 2012).
2	• Availability • Confidentiality • Integrity • Authenticity and non-repudiation	(Bakker 1998), (Siougle & Zorkadis 2002), (Speed & Ellis 2003), (ISO/IEC17799 2005), (Blyth & Kovacich 2006), (Biskup 2009), (Jafari et al. 2009), (Rosenthal 2010), (Mohammad 2010), (Afanasyev et al. 2011), (Mohapatra & Singh 2012).
3	Information security Specific requirements: • Legal requirements • Business Objectives • Threat Landscape	(Anderson 2000), (Siougle & Zorkadis 2002), (Kankanhalli et al. 2003), (Wiant 2005), (Meingast et al. 2006), (DH/Digital Information Policy 2007), (Saleh et al. 2007), (Pishva et al. 2007), (Hawkey et al. 2008), (Gerber & von Solms 2008), (Eminağaoğlu et al. 2009), (Biskup 2009), (Mohammad 2010), (Humaidi et al. 2011), (Jirasek 2012), (Mohapatra & Singh 2012), (Tyson & Slocum 2012), (Kazemi et al. 2012).

3.2.1 Contextualising Information security

The worldwide growth of information technologies has offered huge benefits for users. These technologies have helped to increase organisational efficiency in many sectors by allowing business activities to be performed at much higher speed and with comparatively lower costs, serving more people with better outcomes (Loef et al. 2002; Pishva et al. 2007; Mohapatra & Singh 2012). For example, new technologies enable decision makers to make informed decisions while being able to quickly fuse data from multiple sources, and to disseminate managerial decisions immediately (Hamill et al. 2005). The dependence on information technologies further increases in business environments where the trading of goods and services is done electronically (Kankanhalli et al. 2003). Such a scenario, in which the importance of information systems has increased sharply, has turned information assets into even more valuable commodities for businesses (Pishva et al. 2007).

Doherty et al. (2009) claim that due to the increased importance of information, it is often viewed as an "organisation's lifeblood", which is necessary for the survival of the organisation. Information, as a highly important asset of any organisation, must therefore be protected by the use of information security measures (Pishva et al. 2007; Doherty et al. 2009). In doing so, the most important goals of information security are to ensure the confidentiality, integrity, and availability of information (Doherty et al. 2009; Jafari et al. 2009; Kuang & Ibrahim 2009), as organisations need to perform their core business activities while maintaining efficiency, goodwill, competitive advantage, and compliance to laws and regulations (Bakker 1998).

There is a consensus in the literature over the existence of at least three goals of information security to protect information as a key organisational asset: ensuring confidentiality, integrity, and availability (Bakker 1998; Gritzalis & Lambrinoudakis 2000; Loef et al. 2002; Blyth & Kovacich 2006; GAO 2006; Kuang & Ibrahim 2009; Mohammad 2010; Humaidi et al. 2011). Other authors have listed further attributes such as authenticity and non-repudiation (Hamill et al. 2005; Schumacher et al. 2006; ISO 27799:2008 2008; Biskup 2009; Jafari et al. 2009; Sunyaev 2011; Kumar & Puri 2012). These goals are discussed in more detail in the sub-sections below.

3.2.1.1 Availability

If the information which is required to perform the business activities is withheld without due authorisation, this may hinder the continuity of the business (Jafari et al.

2009). According to this perspective, one of the most important goals of information security is to prevent any unauthorised withholding of information (Bakker 1998) by ensuring that it is accessible and usable upon demand by an authorised entity (Mohammad 2010). There may be several causes of non-availability, such as a failure of the information system, a failure of the network, program errors, human errors, or environmental conditions such as fire, floods, or earthquakes (Bakker 1998). Information services are important for an organisation as they will have been put in place to serve a useful purpose. The interest holders of the organisation need to see these services working to achieve the intended utility of the services. Anything that hinders the functioning of such services through restricting their availability and/or functioning will affect the interests of stakeholders. For example, if an account holder of a bank is unable to execute certain transactions because of the non-availability of the system, this will affect his/her interests in the system. The bank as a service provider is also affected, as it may suffer a negative image or a loss of business.

3.2.1.2 Confidentiality

Blyth & Kovacich (2006) define confidential information as "*information that is private or secret carried out or revealed in the expectations that anything done or revealed will be kept private… for a select group not available to the public, e.g. because it is commercially or industrially sensitive or concerns matters of national security...*". Further, according to ISO17799, confidentiality means *"ensuring that information is accessible only to those authorised to have access"* (ISO/IEC17799 2005). Mohammad (2010) describes confidentiality as the privacy interests that result because of a specific relationship such as doctor/patient, solicitor/client, teacher/student, or researcher/subject which, on the basis of the relevant legal and ethical requirements, binds each of the parties to maintain the privacy of others in the relationship. In other words, confidentiality means that the availability of information must be restricted and not disclosed to unauthorised individuals, entities, or processes, ensuring that the information is only accessible to authorised parties (Bakker 1998; Jafari et al. 2009; Mohammad 2010). There may be different reasons for requiring confidentiality in the system, such as protecting sensitive information or business secrets, protecting personal data as required by law, or maintaining goodwill towards a company (Siougle & Zorkadis 2002). However, the main purpose remains to ensure that information is accessed only by the authorised and correct receivers.

3.2.1.3 Integrity

ISO17799 defines integrity as *"safeguarding the accuracy and completeness of information and processing methods"* (ISO/IEC17799 2005). Blyth & Kovacich (2006) define integrity as a situation in which information is of "professional standards... the state of being complete or undivided...sound or undamaged". Integrity in the sense of being an information security goal entails preventing the modification of information by unauthorised sources, and ensuring that information is accurate and complete both in storage and in transport. It must therefore be presented to authorised users without unauthorised modification, deletion, or addition (Bakker 1998; Biskup 2009; Jafari et al. 2009; Mohammad 2010). The integrity of information may be compromised by program errors, hardware failures, communication failures, human errors, or malicious alteration of the information by unauthorised or authorised users (Bakker 1998). If data is modified or altered in an undesired manner, this has the potential to affect the organisation's functioning, and the confidence of its system users (Jafari et al. 2009). Therefore, integrity is also one of the prime goals of information security.

3.2.1.4 Authenticity and non-repudiation

An entity attempting to access the resources of information system must be identified and authenticated as true before being authorised to access the information, as per its entitlement under organisation's policy (Mohapatra & Singh 2012). In this context, authenticity means the necessary verification of the claimed identity of a user, process, or device before being granted access to the resources of an information system (Jafari et al. 2009; Mohammad 2010). A user must therefore establish his/her right to an identity before accessing the information system (Speed & Ellis 2003). Normally, if a user logs into a system with their username and password, the system recognises the user and grants access to the requested information (Speed & Ellis 2003). Authenticity also facilitates non-repudiation, which means that an entity participating in a communication process, in full or in part, cannot make a false denial of its actions (Jafari et al. 2009). Thus, authenticity and non-repudiation are not only meant to recognise legitimate users in order to authorise them access to information, but also to ensure that those legitimate users act responsibly by preventing them from denying any actions carried out with their authenticated identity.

3.2.2 Information security Specific requirements

All organisations share some common goals for information security, such as availability, integrity, and privacy. However, the information security required may differ from business to business depending on driving factors such as laws and regulations, business objectives, and specific security threats (Gerber and Von-Solms 2008, Jirasek 2012). Therefore, it is important for information security experts to understand not only the common goals but also the specific requirements of information security of the organisation within which they are working.

3.2.2.1 Legal requirements

An organisation, its trading partners, contractors, and service providers, all have to comply with laws and regulations by meeting the legal, statutory, regulatory, and contractual requirements (Siougle & Zorkadis 2002; Gerber & von Solms 2008). In order to protect the interests of individuals, businesses, and of the societies in which businesses operate, governments introduce laws and regulations to regulate and control the utilisation of information systems (Siougle & Zorkadis 2002). With the passage of time, and with the emergence of new threats via the use or misuse of information systems, new laws are introduced, thus increasing the overall quantity and relevance of regulations and legislation (Gerber & von Solms 2008). However, the complexity of information security requirements further increases with the emergence and introduction of multiple laws (Meingast et al. 2006). For example, financial services in the US must comply with requirements determined by different national regulations such as the US Gramm–Leach Bliley Act of 1999 (GLBA), the Basel Accords, Securities and Exchange Commission (SEC) requirements, the USA Patriot Act, as well as international or regional laws such as EU Directives in the European Union and Basel II in banking (Gerber & von Solms 2008).

The legal and regulatory requirements of information security generally include data protection legislation, copyright restrictions, organisational record preservation, and observing agreements between parties while serving as a provider/supplier of products or a customer of products and services (Siougle & Zorkadis 2002; Gerber & von Solms 2008). All organisations are obliged to observe all applicable laws and regulations in order to avoid legal action or fines (Gerber & von Solms 2008; Jirasek 2012). Data protection legislation is an example of such information security requirements. The term "data protection" refers to the set of laws, policies, and procedures generally intended to minimise intrusion into the privacy of individuals which can result due to the collection, storage, and dissemination of personal data (Siougle & Zorkadis 2002; Mohammad 2010). For example, in the UK, the Data Protection Act 1998 regulates the processing of personal data, and details the statutory requirements for organisations such as healthcare providers, banks, and human resources and occupational health departments (DH/Digital Information Policy 2007). Likewise, the General Data Protection Regulation (EU) 2016/679 abbreviated as GDPR is also a regulation in European Union (EU) which details the legal requirements for all individuals within the EU region.

3.2.2.2 Business Objectives

In addition to legal requirements, the business objectives that differ from one industry to another also determine the requirements of information security with regard to meeting its security goals (Saleh et al. 2007). On the basis of business objectives, the purpose of data processing and requirements of information security can vary even if different organisations are processing the same type of data (Siougle & Zorkadis 2002). For example, the same personal data can be processed in a healthcare organisation and by financial institutions for completely different purposes due to different requirements, as determined by very different respective business objectives.

A set of business objectives is generally set by organisations in order to maximise their profits (Jirasek 2012). The task of information security is intended to support those business objectives by securing the information which is used to perform the business activities/processes (Kankanhalli et al. 2003; Pishva et al. 2007; Saleh et al. 2007; Jirasek 2012). For example, one of the major business objectives of Microsoft is to generate and maximise profits by selling licences for Windows operating systems, and it therefore needs to protect its source code. If Microsoft's information security fails to provide the required security to the source code for Windows, the business objectives of Microsoft are likely to be undermined due to unauthorised copying and/or security breaches. Information security that supports a company's business objectives by facilitating efficient business operations is important if that company is to have "a competitive edge, cash flow and/or profitability" (Gerber & von Solms 2008; Mohammad 2010). Hence, an organisation's information security requirements are directly related to its business objectives.

3.2.2.3 Threat Landscape

Security threats are important in the determination of the information security requirements of an organisation because they work against the other two information security requirements, that is, against the existing laws and regulations, and the business objectives, while at the same time driving the need for information security (Jirasek 2012). Threats might be directed against one or more of a company's information security goals; for example, the availability of information to continue its business activities in pursuance of business objectives, the confidentiality of information as required by law and business, the integrity of information to establish trust regarding the accuracy of data, and the authenticity of users to ensure that information is only accessed by authorised users, and to enable the system to ensure non-repudiation so that users of information cannot deny their actions (Biskup 2009). Furthermore, the purpose of information security is to ensure that information is protected from a wide range of threats in order to achieve business continuity, minimise the potential damage to the business, and maximise financial returns on investment and business opportunities (Mohammad 2010). These threats to the information security of an organisation can originate from either its internal or external environments (Anderson 2000).

The threats that emerge from the internal environment of an organisation are the most common (Wiant 2005; Tyson & Slocum 2012). For example, the internal environment implies that the accidental exposure/disclosure of information is due to the carelessness, ignorance, and/or negligence of employees of the organisation (Wiant 2005). Tyson & Slocum (2012) explain that internal threats have historically been more common, as between 2009 and 2011 49 percent of reported information security breaches in the US were due to lost or stolen information devices or laptops used by the employees of an organisation. Although information security with regard to printed reports, paper records, and hard copies of documents represented a challenging task, it is more challenging to protect information in electronic formats, especially due to the rapid development and growth of information systems and networks, the increased use of email, blogs, wireless networking, laptops, smartphones and other mobile devices, and USB storage devices (Mohapatra & Singh 2012).

Threats originating from the external environment of an organisation tend to be comparatively more systematic and determined, and therefore cannot be considered as any less dangerous (Tyson & Slocum 2012). External threats may involve third party information users and secondary users of uncontrolled information, or motivated hackers (Wiant 2005; Humaidi et al. 2011). Third party information users may include a separate organisation or individual(s) providing auxiliary products or services which are not delivered by the main supplier of products and services such as pharmacies, insurance companies, or teaching hospitals in the case of healthcare organisations (Humaidi et al. 2011). The secondary usage of information may include the utilisation of information for purposes other than the main purpose for which information was originally collected and stored, such as using medical information collected and stored by a healthcare organisation for medical research or national health planning (Wiant 2005). Hackers may be said to include all unauthorised people who attempt to break into computer systems to steal, destroy, or alter the information for their own interests (Humaidi et al. 2011).

Eminağaoğlu et al. (2009) note that "effective countermeasures, technologies, and solutions" are available to protect information against most existing threats. However, such solutions are often not implemented in a correct and effective manner, because the people tasked with doing so have often not been properly trained, deployed, and monitored (Eminağaoğlu et al. 2009). Risk assessments can help to identify existing threats to assets, vulnerabilities in the system, determinations of the likelihood of threat occurrence, and the estimated value of the potential impact on the organisation (Gerber & von Solms 2008).

To conclude, information security can be understood on two levels: one is broader and generic, and includes goals such as confidentiality, integrity, and availability, which every organisation seeks to attain. The second is more specific and is based on the information security requirements arising from drivers like laws and regulations, business objectives and existing threats. Therefore, an effective information security strategy is likely to be one which considers the more specific requirements of the organisation in question.

3.2.3 Summary of findings for RQ1

This section has discussed information as an important asset for organisations which therefore needs to be protected. The common goals of information security are availability, confidentiality, integrity, authenticity, and the non-repudiation of data, and these are therefore required in every organisation using information systems. However, the nature or priority of those common goals may vary from organisation to organisation depending upon its specific information security requirements, such as laws and regulations, business objectives, and particular threat landscape.

3.3 Findings for RQ2: What is an information security strategy?

In total, 44 articles were selected to answer RQ2, and these helped to build understanding of the concept, definition, and the process of developing and implementing the information security strategy of an organisation in order to meet its specific information security requirements. The findings of the SLR in relation to this question are discussed below.

No	Areas covered	Selected studies from the SLR for Research Question Two
1	Information security strategy	(Chandler 1962), (Mintzberg 1978), (FFIEC 1998), (Fung et al. 2003), (Gupta et al. 2003), (Kankanhalli et al. 2003), (Wylder 2004), (Burke & Jarratt 2004), (Saleh et al. 2007), (Knapp et al. 2009), (Doherty et al. 2009), (Commonwealth of Australia 2009), (Mohammad 2010), (Goel & Chengalur-Smith 2010), (Jirasek 2012), (Stahl et al. 2012).
2	Information Security Management Systems (ISMS)	(Chandler 1962), (Mintzberg 1978), (Von-Solms 1998), (Kankanhalli et al. 2003), (Burke & Jarratt 2004), (Farn et al. 2004), (Tipton & Krause 2004), (Thigarajan 2006), (Yoo et al. 2007), (Gerber & von Solms 2008), (Mohammad 2010), (The Office of Cyber Security and Information Assurance, Cabinet Office 2011), (Tarwireyi et al. 2011), (Kazemi et al. 2012), (ISO/IEC 27001:2013 2013), (ISO/IEC 27002:2013 2013), (Calder 2013).
3	Planning information security strategies and the establishment of information security management systems	(Park et al. 2010), (ISO/IEC 27001:2013 2013), (ISO/IEC 27002:2013 2013), (Calder 2013).
4	Risk Assessment	(Brooks & Warren 2006), (Gong et al. 2009), (Dogaheh 2010), (Sajko et al. 2010), (Vladimirov et al. 2010), (Tyson & Slocum 2012)
5	Development of Information Security Policies to Mitigate Risks	(Gerber et al. 2001), (Höne & Eloff 2002), (Andress 2003), (Wiant 2005), (Blyth & Kovacich 2006), (Saleh et al. 2007), (Doherty et al. 2009), (Mohammad 2010), (Goel & Chengalur-Smith 2010), (Kumar & Puri 2012).
6	Do’ phase – the implementation of strategies to mitigate risks	(Bottino 2006), (Persusco 2006), (Blyth & Kovacich 2006), (Saleh et al. 2007), (Doherty et al. 2009), (Mohapatra & Singh 2012), (ISO/IEC 27001:2013 2013)

3.3.1 Information security strategy

Mintzberg (1978) argues that unlike the common usage of the concept of a ‘strategy’ in literature, which involves an opponent or a set of competitors, in business theory the idea is wider in scope and includes collective perception and actions deployed in order to achieve business objectives. Chandler (1962) explained strategy as a process that not only determines the wider long-term goals of the business, but also helps it to adopt a course of action and to deploy sufficient resources to achieve those goals. However, Mintzberg (1978) also explains that a strategy can be conceptually wider and more than just an overt plan of action, and that it may involve any intentional or unintentional actions in the pursuit of business goals. For that reason, Burke & Jarratt (2004) explain strategy with reference to the broader perspective and argue that it can be seen as a plan, pattern, ploy, perspective, or position. Therefore, Mohammad (2010) argue that Mintzberg (1978) and Burke & Jarratt (2004) each made significant contributions to defining this concept, which have helped to explain strategy as constituting more than mere planning.

Goel & Chengalur-Smith (2010) note that "Security policy" is a term which is used in two different contexts. First, in the context of computer/network security it describes the formal rules of access control for information systems. Second, it is used in information security management in an organisation to describe the overall strategy and plan for information security. An information security strategy is considered an "important business document which covers a broad set of security concerns" (Stahl et al. 2012) and comprises a set of policies developed to meet information security requirements (Jirasek 2012). An organisation’s information security strategy is also considered the first step to prepare it to mitigate internal and external threats to information security (Knapp et al. 2009).

An information security strategy is based on three important factors, as Jirasek (2012) explains: information security drivers, management, and stakeholders of information security (see Figure 3.1). These factors are closely linked, as an information security strategy provides management with direction and support according to their organisation's information security requirements (Saleh et al. 2007), and gives an overall sketch on how to prevent or at least minimise risks in order to ensure compliance with the legal, statutory, contractual, and internally developed requirements of the business, thus protecting the interests of its stakeholders (FFIEC 1998; Wylder 2004; Mohammad 2010). Jirasek (2012) further observes that information security drivers include factors such as laws and regulations, business objectives, and security threats, that drive the need for information security and drive organisations to seek protection for their information assets, by formulating their set of organisational requirements for information security. Management can be said to include the people entrusted with the responsibility to develop, publish, and distribute strategies, policies, procedures/processes and frameworks in order to meet the information security requirements determined by the security drivers (Doherty et al. 2009, Jirasek 2012). Stakeholders are the individuals, groups, or companies who are likely to benefit from effective information security, and/or who will be affected by any damage to the information systems (Jirasek 2012).

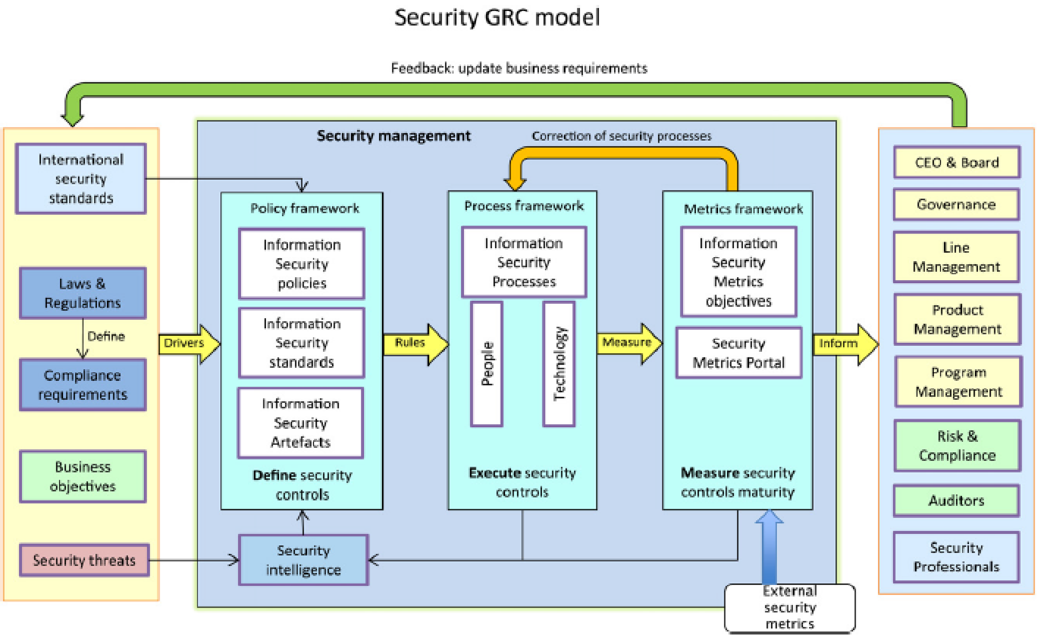


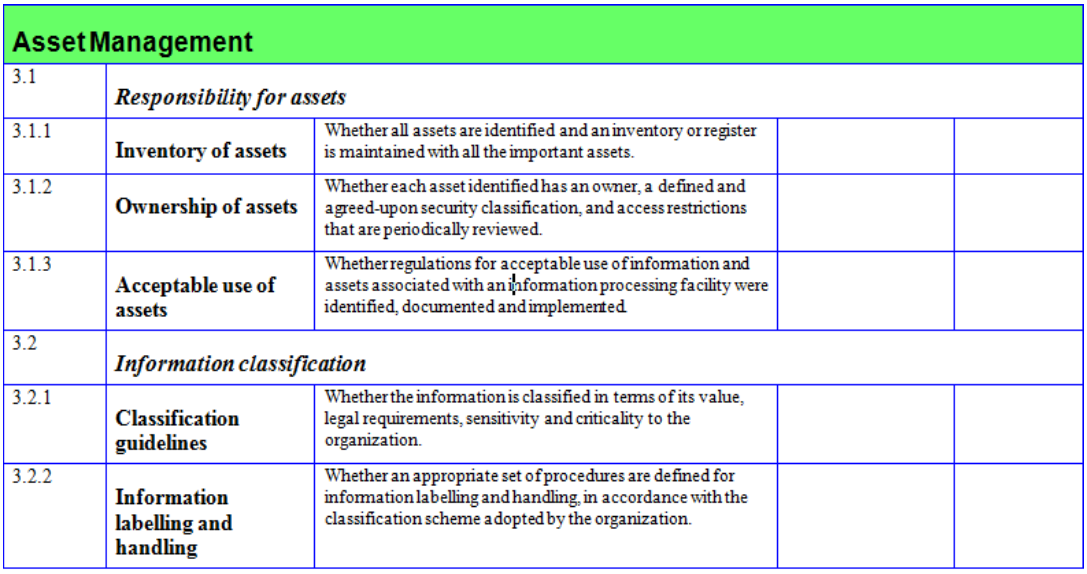
Figure 3.1: Security GRC model that describes the constitution of Information Security (Jirasek 2012)

3.3.2 Information Security Management Systems (ISMS)

Information security strategies are primarily based on standards which have been generically developed for general information systems regardless of the type, size, nature, or geographical location of an organisation, and for every sector including commercial, government, and non-profit organisations (ISO/IEC 27001:2013 2013). Standards are developed by national, regional or international organisations such as the British Standards Institute (BSI), the European Standards Organisation (ESO), and the International Standards Organisation (ISO). ISO/IEC 27001 and 27002, replacing ISO/IEC 17799, were first published in 2005 and then updated in 2013, and are the international standards for information security management. ISO/IEC 27001 details the specifications for an Information Security Management System and is used by organisations to develop, implement, evaluate, and revise their information security strategies (ISO/IEC 27001:2013 2013). ISO/IEC 27002 provides a code of practice for the management of information security as specified by the ISO/IEC 27001 (ISO/IEC 27001:2013 2013; ISO/IEC 27002:2013 2013; Calder 2013).

In business, a standard is a rule or collection of rules that spells out a course of action in a specified situation. Standards are significant in the achievement of business goals and in meeting business requirements as their purpose is to facilitate management's policies, as framed under their overall strategies. They are mandatory and can also be used to measure the compliance of strategies (Calder 2013). Standards are not strategies in themselves; rather, they are designed to promote the particular strategies of an organisation (Burke & Jarratt 2004). Therefore, standards provide different possible options with which to address different issues, from among which organisations may chose according to their own information security requirements.

Thus, different types of businesses can choose, develop and apply an information security strategy appropriate to their needs by selecting the relevant controls from the existing standards according to their information security drivers/requirements (ISO/IEC 27001:2013 2013). The information security controls selected and applied from a range of broader control categories help to form the overall strategy of the organisation (Mohammad 2010; Burke & Jarratt 2004; Chandler 1962; Mintzberg 1978). For example, ISO/IEC 27002 has been increasingly popular among members of the international e-commerce community for its information security management utility (Gerber & von Solms 2008). The standard offers 114 controls or sub-clauses under 14 major clauses, control areas, or control categories (ISO/IEC 27002:2013 2013). The control categories of the standard represent wider information security control areas in the form of organisational and technological measures of an information security strategy (Yoo et al. 2007, Calder 2013). The control categories include information security policies, the organisation of information security, human resources security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, systems acquisition and development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, and compliance (ISO/IEC 27002:2013 2013; Calder 2013). The standard is further divided into subcategories, each of which is further divided into detailed control items (Yoo et al. 2007, ISO/IEC 2013, Calder 2013). Figure 3.2 (Thigarajan 2006) shows that asset management is divided into two subcategories: '3.1 Responsibility for assets', and '3.2 Information classification'. Moreover, Figure 3.2 shows that the 'Responsibility for assets' sub-category is further subdivided into three detailed control items, 3.1.1, 3.1.2, and 3.1.3.



Asset Management				
3.1	*Responsibility for assets*			
3.1.1	**Inventory of assets**	Whether all assets are identified and an inventory or register is maintained with all the important assets.		
3.1.2	**Ownership of assets**	Whether each asset identified has an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.		
3.1.3	**Acceptable use of assets**	Whether regulations for acceptable use of information and assets associated with an information processing facility were identified, documented and implemented.		
3.2	*Information classification*			
3.2.1	**Classification guidelines**	Whether the information is classified in terms of its value, legal requirements, sensitivity and criticality to the organization.		
3.2.2	**Information labelling and handling**	Whether an appropriate set of procedures are defined for information labelling and handling, in accordance with the classification scheme adopted by the organization.		

Figure 3.2 Part of the List of Control Categories, Subcategories, and Detailed Controlled Items Reflecting Information Security Strategy (Thigarajan 2006)

Management is one of the most important dimensions of any information security strategy, as it is not only responsible for devising the strategy, but is also duty bound to plan, implement, evaluate, and update the strategy in order to achieve the organisation's strategic objectives of information security (Calder 2013). Kankanhalli et al. (2003) present an empirically tested model to support the argument that top management support for an information security strategy that results in better preventive efforts is positively related with the overall information security effectiveness of the organisation. Similarly, Kazemi et al. (2012) more recently show that support from an organisation’s top management in the development of an information security strategy, spreading awareness of it among staff, and the proper training of staff, are the critically important success factors for the information security program of an organisation.

Standard ISO/IEC 27002: 2013 recommends the adoption of the Plan-Do-Check-Act (PDCA) model in information security management, which originated in the 1950s having been designed by W. Edwards Deming as a business process model (Calder 2013). The PDCA implies that business processes should be developed in a "continuous feedback loop" to ensure a continuous improvement of the business processes (Calder 2013). The process or improvement to the process should be planned, implemented, measured for effectiveness, and subsequently improved (Calder 2013).

3.3.2.1 Planning information security strategies and the establishment of information security management systems

The planning of an appropriate information security strategy and the establishment of information security management systems involve defining the organisation and its context, setting the scope of the information security management system, setting out information security policies, taking a systematic approach to risk assessment, carrying out a risk assessment to identify the important information assets and the associated risks to them in the context of the policy and the information security management system's scope, identifying and evaluating different options to deal with the identified risks, the selection of controls and objectives for those controls which are highlighted in the response to the decisions taken to deal with identified risks, and preparing a statement of applicability to clearly list all those controls which are finally identified, recommended, and selected for the implementation (ISO/IEC 27001:2005 2005; Calder 2013).

Risk Assessment

The planning phase of information security strategy starts in practical terms with a risk assessment based on the identified information security requirements of the organisation. Sajko et al. (2010) notes that "the generally accepted and most widely used way of [information security] management is risk analysis". Risk analysis or assessment is an activity used to determine the existing risks that can threaten an organisation’s information security. Sajko et al. (2010) further explain that risk assessment activity is expected to be able to effectively identify the existing risk factors while collecting information about them, such as threats, vulnerabilities, and the possible impacts of those risks, thus highlighting the critical spots within the organisation. The activity should be able to report and present a useful analysis of the results based on risk identification, analysis, and prioritisation (Sajko et al. 2010).

Risk assessment can be qualitative or quantitative. A quantitative assessment cannot be done without assigning monetary values to the objects of evaluation in order to estimate the value of potential losses (Dogaheh 2010), while a qualitative assessment is scenario-based (Brooks & Warren 2006) in that it considers different active or passive scenarios and their outcomes, and qualitative results are generated (Brooks & Warren 2006). The reason for undertaking qualitative assessments is that normally, auditors are not supplied with sufficient information about the monetary values of the assets. However, the results of the evaluations should be presented in a quantified manner. This facilitates the prioritising of different risks and their seriousness (Vladimirov et al. 2010). Effective risk assessments also help to create a layered approach to security

(Tyson & Slocum 2012). In a layered approach, information security is applied and assessed at different levels, for example by conducting risk assessments, managing mobile devices, applying encryption and endpoint controls, implementing data centres and network security controls, and implementing continuous monitoring (Tyson & Slocum 2012). Informed by the existing risks based on the information security requirements, the organisation's management develops a strategy to effectively deal with those risks by selecting and applying the most appropriate information security controls.

Development of Information Security Policies to Mitigate Risks

Blyth & Kovacich (2006) explain a policy as a *"written principle or rule to guide decision-making"*. Policies are broad statements of principles that represent the position of management in a specific area. They are generally long term, and are intended to serve as a guide with the help of specific rules to deal with specific issues. Policies are developed as a part of overall strategy in the light of identified risks and appropriate controls. Mohammad (2010) suggests that they should be few in number, approved and monitored by top management, and provide general direction to the organisation.

An information security policy is an important, high level business document(s) with the purpose of describing the security controls to be applied in the organisation to meet its information security requirements (Andress 2003; Doherty et al. 2009). It gives clear instructions for the implementation of information security, and not only helps to meet organisational requirements, but also to determine the management's commitment towards information security (Höne & Eloff 2002). It also provides guidelines for the processing, storage and transmission of information to avoid unauthorised disclosure or modification (Andress 2003).

Hence, as Doherty et al. (2009) explain, an information security policy is an important business document developed to protect the information assets of the organisation. Saleh et al. (2007) argue that this document provides management with direction and support to secure information according to their organisation's business, legal, and regulatory requirements. Saleh et al. (2007) further note that to meet an organisation's information security requirements, a written information security policy has to be developed, approved, published, and reviewed by the management, and communicated to all employees and external parties.

Wiant (2005) suggested that while formulating formal information security policies, the relevant laws and regulations, business requirements, the employees of the organisation, and all external parties and partners should each be considered, and policies should be given continuous attention both before and after their formulation and application. A comprehensive written policy covering the issues highlighted by the literature and international standards should set out individual responsibilities, detail the authorised and unauthorised uses of information systems, enable staff to report identified or suspected threats, stipulate penalties for violations, and offer mechanisms for reviewing and updating the policy itself (Doherty et al. 2009; Kumar & Puri 2012).

Goel & Chengalur-Smith (2010) devised criteria to evaluate the effectiveness of information security policies which can be helpful in planning new policies or improving existing ones. They found that high levels of brevity, clarity, and breadth can increase the effectiveness of policies (Goel & Chengalur-Smith 2010). Brevity means that a policy is not unnecessarily lengthy, and that it presents information in a compact manner so that any repetition and unnecessary use of words is avoided. However, the aspiration to brevity should not compromise clarity, as a policy should also be clear in its content and language so that it is easy to read and understand. The policy should be written using common English words and phrases which can be easily understood without referring to reference materials such as dictionaries (Goel & Chengalur-Smith 2010). Moreover, a policy should have sufficient breadth that it is effective in protecting against the legal consequences of violations, specifies the legal ramifications of violations, and contains all the necessary elements of information security (Goel & Chengalur-Smith 2010). Furthermore, information security policies should be regularly evaluated and reviewed to ensure that they continue to address the information security requirements of the organisation (Kumar & Puri 2012).

3.3.2.2 ‘Do’ phase – the implementation of strategies to mitigate risks

This second phase of information security management involves the formulation, documentation, and implementation of a risk treatment plan, including planned processes and detailed procedures (ISO/IEC 27001:2013 2013). Additionally, this involves arranging the appropriate employee training and awareness programs, managing operations and resources in line with the information security strategy, and implementing procedures in order to promptly detect and respond to any security incidents (ISO/IEC 27001:2013 2013).

Information security policies cover a wide range of issues, including violations and breaches, user access management, contingency planning, physical security, disclosure of information, malware, encryption, mobile computing, software development, personal usage information, internet access, responsibilities, enforcement, awareness and training, compliance with legislations, and information classification (Doherty et al. 2009).

Technological controls need to be implemented in order to address issues of communication and operations management, access control, and for the development, acquisition, and maintenance of the information systems, keeping in mind the organisation’s overall strategic objectives (Saleh et al. 2007). Organisations must deal with new and emerging threats on an ongoing basis, so different technological solutions have been introduced to deal with these threats such as firewalls, intrusion prevention systems, network scanning solutions, antivirus programs, spam detection and quarantine, and others, in order to mitigate the risks (Mohapatra & Singh 2012). A single technology or solution will not address all issues of security, so a complete package of technological solutions must be assembled and applied. However, applying a full suite of the technologies listed above may involve considerable costs; therefore, organisations adopt the “Probability-Impact-Priority” technique which calculates risk on the basis of assessed threats, vulnerabilities, and assets (Mohapatra & Singh 2012). Though technical controls are crucial, Persusco (2006) argues that while planning and implementing the technical aspects of information security, it is also important to consider the social impacts of the technology being acquired and implemented.

Generally, information security policies reflect "a high techno-centric view" of information security management (Blyth & Kovacich 2006; Doherty et al. 2009; Mohapatra & Singh 2012). Since information security also involves a social perspective, management must be conscious of the possible threats associated with people having access to the information systems either from within or outside the organisation (Blyth & Kovacich 2006; Saleh et al. 2007; Doherty et al. 2009; Mohapatra & Singh 2012). The socio-technical information security policy perspective is about governing the behaviour of people while they interact with the information systems. The social perspective defines the level of technical competence for the system administrators, and specifies the rules governing the disclosure of information to a third party.(Blyth & Kovacich 2006)

3.3.3 Summary of findings for RQ2

This section has analysed the concept and process of an information security strategy which can be chosen and developed on the basis of information security standards such as ISO/IEC 27001 and ISO/IEC 27002. Information security management is a process which facilitates the planning and implementation of information security strategies on the basis of risk assessment. Information security strategies are high level written documents which are developed to detail the implementation process and information security controls put in place to mitigate risks associated with certain information assets. An information security strategy, as a collection of information security controls, has a major role to play in an organisation's overall information security, and therefore needs to be developed in line with the organisation's business, legal and regulatory requirements regarding information security.

3.4 Findings for RQ3: What is an information security strategy for healthcare data systems?

A total of 50 studies were selected to answer this question. The objectives of the question were to comprehend the goals and requirements of information security in healthcare data systems, and to understand the particular issues involved in healthcare organisations' development of information security strategies to meet their specific requirements. The findings are discussed below in the following sub-sections.

No	Areas covered	Selected studies from the SLR for Research Question Three
1	Electronic Healthcare Records (EHR)	(Anderson 2000), (Stewart 2003), (Ceusters & Smith 2006), (Clarke & Meiris 2006), (Win & Fulcher 2007), (Appari & Johnson 2008), (Otieno et al. 2008), (Häyrinen et al. 2008), (Mohammad 2010), (NHS 2010), (Liu et al. 2011).
2	Contextualising information security in healthcare data systems	(Von-Solms 1996), (Anderson 2000), (Loef et al. 2002), (Wiant 2005), (Brooks & Warren 2006), (Wozak et al. 2007), (Appari & Johnson 2008), (Chi et al. 2008), (Jafari et al. 2009), (Kuang & Ibrahim 2009), (Linden et al. 2009), (Mohammad 2010), (Liu et al. 2011), (Humaidi et al. 2011), (Tyson & Slocum 2012), (Wang et al. 2012),
3	Information security goals of healthcare organisations	(Bakker 1998), (Purser 2004), (Blyth & Kovacich 2006), (Goel et al. 2007), (Kuang & Ibrahim 2009), (Mohammad 2010), (Humaidi et al. 2011)
4	Information security requirements of healthcare organizations	(Bakker 1998), (Smith & Eloff 1999), (Takeda et al. 2000), (Tzelepi et al. 2002), (Reni et al. 2004), (Kluge 2004), (Wiant 2005), (Meingast et al. 2006), (Schumacher et al. 2006), (DH/Digital Information Policy 2007), (Win & Fulcher 2007), (Safran et al. 2007), (Appari & Johnson 2008), (Gerber & von Solms 2008), (Papazafeiropoulou & Gandecha 2008), (Sheppard et al. 2009), (Shoniregun et al. 2010), (Mohammad 2010), (NHS 2010), (Abraham et al. 2011), (Sunyaev 2011), (Jirasek 2012), (Mohapatra & Singh 2012), (Tyson & Slocum 2012), (HSCIC 2014).
5	Information security strategy of healthcare data systems	(Gaunt 1998), (ISO 27799:2008 2008), (Mohammad 2010),
6	Information security management system (ISMS) for healthcare data systems	(DH/Digital Information Policy 2007), (ISO 27799:2008 2008), (ISO/IEC 27001:2013 2013), (ISO/IEC 27002:2013 2013)

3.4.1 Electronic Healthcare Records (EHR)

Electronic Healthcare Records (EHR), also known as Summary Care Records, are believed to be the single most important tool in improving healthcare quality and reducing costs (Appari & Johnson 2008; Otieno et al. 2008; Mohammad 2010; Liu et al. 2011). EHRs are used to collect patients' medical data from different participating sources including clinics, hospitals, laboratories, and insurance companies (Liu et al. 2011). Their purpose is to keep a central record of a patient's information to facilitate improved care through continuous, safe, effective, efficient, timely, patient-centred and quality-oriented healthcare which may be provided by different healthcare professionals at different times (Otieno et al. 2008; Häyrinen et al. 2008; NHS 2010; Liu et al. 2011). Electronic records contain important information about any medicines a patient is taking, any allergies he/she suffers from, and any reactions to specific medicines which patients have had in the past, and these records are designed to be conveniently shared among different healthcare professionals working within a single organisation, or even across different organisations (NHS 2010; Liu et al. 2011). In other words, an EHR is an IT-based compilation of health information for each patient that is generally gathered and maintained by a healthcare provider, i.e., a hospital or a clinician, in order to deliver better healthcare services on the basis of managed care and using integrated delivery systems (Anderson 2000; Mohammad 2010).

3.4.2 Contextualising information security in healthcare data systems

Although EHRs are most beneficial if they can be shared across various healthcare providers, the promise and the prospect of interoperability or sharing the information across a wide range of users also raises privacy and other security concerns (Anderson 2000; Loef et al. 2002; Wiant 2005; Chi et al. 2008; Jafari et al. 2009; Linden et al.

2009; Liu et al. 2011). Consequently, information security concerns have been one of the major impediments to the growth and adoption of EHRs (Chi et al. 2008). The increased accessibility means that records can be accessed, changed, viewed, copied, used, disclosed, and deleted more easily than paper based records or electronic records restricted to local use within an individual healthcare organisation (Loef et al. 2002; Wiant 2005; Linden et al. 2009; Humaidi et al. 2011; Liu et al. 2011). Concerns regarding the privacy and security of patient data have been proved genuine, for two reasons: first, there has been a history of information security breaches; and second, the data is important for its utility to different groups of stakeholders. Moreover, strong information security is required for healthcare databases because both patients and healthcare organisations need to ensure the privacy of patient information, and the delivery of reliable and efficient healthcare services (Anderson 2000; Loef et al. 2002; Wiant 2005; Jafari et al. 2009; Kuang & Ibrahim 2009; Linden et al. 2009; Liu et al. 2011).

Anecdotal evidence over the last few years has suggested that a lack of appropriate security measures has resulted in many data breaches, which have affected patients in numerous ways, including financially, mentally, and socially (Appari & Johnson 2008; Tyson & Slocum 2012). Tyson & Slocum (2012) note that the privacy of over 18 million patients' protected health records had been compromised between 2009 and 2011. Likewise, a survey on Computer Crime and Security in Australia conducted by AusCERT in 2006 with 389 respondents, gathered responses to attacks on computer networks, crime, and the misuse of computers over a 12-month period. The survey included the healthcare sector, as 6% of respondents (a total of 23 organisations) operated in this sector. The findings of the survey revealed a clear reduction in the usage of information security technologies, ICT qualifications, and the training provided to employees compared to 2004 and 2005. 20% of the respondents reported that they had experienced information security attacks during the past year. Brooks & Warren (2006) argue that the findings of the survey were sufficient evidence to demonstrate that information security (or the lack of it) is relevant and important in considering the protection of confidential data in different organisations. Another survey in 2006 concluded that 75 percent of patients were concerned that health websites had shared their personal information with other parties without their consent. The unauthorised disclosure of medical data was also reported as the second highest type of breach in 2006 (Brooks & Warren 2006). Brooks & Warren (2006) conclude that, on the basis of the above-mentioned surveys, managerial practices and the execution of information security controls are significantly deficient in several sectors, including healthcare. Therefore, healthcare organisations are among those who need to give higher priority to information security.

It is not only the history and precedence of information security breaches in healthcare organisations which increase the importance of information security therein; the nature and importance of the data makes the need for information security much more acute than in other sectors such as financial, military, and government organisations (Anderson 2000; Wiant 2005; Brooks & Warren 2006; Jafari et al. 2009; Humaidi et al. 2011; Liu et al. 2011). EHRs may contain information about a patient's identity, their history of medical diagnosis, treatment, medication, dietary habits, sexual preferences, genetic information, psychological profile, employment, income, and physician assessments (Jafari et al. 2009; Kuang & Ibrahim 2009). Therefore, the different types of information contained in EHRs may be attractive to different individuals, groups, or businesses, and can be used in numerous different ways, such as improving the efficiency of healthcare services by supporting medical staff to perform their core duties, helping policy development and administration at the federal or state level, and facilitating research in medical sciences (Anderson 2000; Humaidi et al. 2011; Liu et al. 2011). EHRs may be shared with financial organisations such as insurance companies in order to justify the bill of services provided to a patient (Anderson 2000; Humaidi et al. 2011; Liu et al. 2011), and they can also facilitate healthcare providers to manage their operations and to evaluate the quality of the services they provide, thus helping them to highlight opportunities and areas in need of improvement (Appari & Johnson 2008; Jafari et al. 2009; Liu et al. 2011).

The results of prior studies of data breaches have also shown that personal information is attractive to criminals, as such information can often be used to commit identity fraud crimes (Von-Solms 1996; Jafari et al. 2009; Humaidi et al. 2011). However, the utility of the medical data can be of both economic and social value to different stakeholders (Anderson 2000). For example, for employers, insurers, or even journalists, the patient's information may be of economic value, whereas for family, friends, or people in intimate relationships with them, such information may be of non-economic value, but still carry social implications (Anderson 2000; Loef et al. 2002; Wiant 2005; Kuang & Ibrahim 2009; Humaidi et al. 2011).

From a patient's perspective, privacy is an important principle of the patient-physician relationship, and is therefore also an important concern for healthcare providers who deploy EHRs in terms of meeting the required delivery parameters in their services (Linden et al. 2009; Mohammad 2010; Liu et al. 2011). Patients need to share personal information with their healthcare providers in order to receive a correct diagnosis, effective treatment, and make informed choices (Linden et al. 2009; Mohammad 2010; Liu et al. 2011). However, sometimes they may not wish to disclose their information to certain people if they are concerned about social stigma or discrimination, or possible financial loss (Kuang & Ibrahim 2009; Linden et al. 2009; Mohammad 2010; Humaidi et al. 2011; Liu et al. 2011). For example, in the cases of HIV or mental disorders, an unauthorised disclosure regarding the diagnosis may result in the social stigmatisation of a patient; an unauthorised disclosure regarding an abortion could even result in the breakup of a marriage or a family crisis (Kuang & Ibrahim 2009). Likewise, an unauthorised data disclosure to a patient's employer may cost them their jobs, so healthcare organisations have a social responsibility to ensure the confidentiality of patients' information and consider their consent regarding the controlled disclosure of their medical and personal information (Humaidi et al. 2011).

Similarly, for physicians and nurses, uninterrupted and smooth access to patient data in its correct form is necessary to perform their healthcare duties (Anderson 2000; Jafari et al. 2009; Linden et al. 2009; Mohammad 2010; Liu et al. 2011). They may also require the data to be protected to uphold the confidentiality of their patient's data in order to meet their ethical requirements derived from the historical Hippocratic oath (Anderson 2000; Jafari et al. 2009; Linden et al. 2009). For healthcare organisations seeking health information security, competitive advantage, or maintaining a good repute by continuously having the trust of their patients/customers, also play a part (Mohammad 2010). Thus, protecting patient privacy and security is also a key professional and business requirement for healthcare organisations.

Likewise, governments may require trustworthy medical information for the sake of national planning and budgeting (Anderson 2000; Humaidi et al. 2011). Insurance companies may need access to the medical information of their clients in order to process claims and verify their genuineness (Anderson 2000; Humaidi et al. 2011; Liu et al. 2011). Further, medical students may also need access to health data for their research and education (Anderson 2000; Liu et al. 2011), and pharmaceutical companies may wish to have access to this data for the development of new medicines and to study the effects and side-effects of previously-used treatments (Anderson 2000; Liu et al. 2011). The utility of medical information is therefore different to the different stakeholders depending on the interests and stakes of the parties involved, and healthcare organisations are responsible for respecting their patients’ privacy and ensuring the information security of patients' information while considering their consent regarding the use of their medical and personal information (Mohammad 2010).

Thus, healthcare data, as an important asset which needs protection against unauthorised access/disclosure, corruption, and denial of/delay in service, could affect the interests of many different stakeholders, that is, patients, healthcare employees, healthcare organisations, governments, and third parties such as insurance companies, pharmaceutical companies, and medical students. Information security concerns are a hindrance in reaping the potential benefits of EHRs, and therefore, good information security is required for healthcare databases to achieve the same. Moreover, the effective information security of EHRs can also facilitate their efficient secondary usages in the research/teaching of medical students, planning and budgeting of governments departments, supporting healthcare insurance procedures, and in pharmaceutical companies, to conduct their research/marketing on medicine.

3.4.3 Information security goals of healthcare organisations

Given the information security concerns outlined above regarding the use of electronic healthcare records, information security in healthcare is intended to ensure privacy/confidentiality (Purser 2004), integrity, availability, and authenticity and non-repudiation of the medical information stored in EHRs, all at the same time (Bakker

1998; Blyth & Kovacich 2006; Kuang & Ibrahim 2009; Mohammad 2010; Humaidi et al. 2011; Sunyaev 2011). Information security in healthcare is needed in the first instance to reap the benefits of quality and efficiency from EHR systems, because an increased level of sharing through the adoption of new technologies is required, which also increases the risks faced by healthcare data systems (Bakker 1998; Mohammad 2010; Humaidi et al. 2011). Subsequently, in efforts to increase the level and functionality of sharing, new technologies have been adopted to considerably reduce the time and effort required in the delivery of healthcare services, which also brings new challenges to using the technology in relation to ensuring the confidentiality, availability, and integrity of patients' data (Bakker 1998; Mohammad 2010; Humaidi et al. 2011). Therefore, Mohammad (2010) argues that it is challenging to implement a shared EHR system which is both easy and secure to use while considering the interests of all stakeholders including patients, and healthcare professionals and organisations.

Thus, in order to maximise the benefits of EHRs while ensuring the required level of information security, healthcare records should be complete and comprehensive, as well as secure enough to maintain patient data confidentiality (Bakker 1998; Blyth & Kovacich 2006; Kuang & Ibrahim 2009; Mohammad 2010; Humaidi et al. 2011; Sunyaev 2011). EHRs must also be available when and where healthcare professionals and other authorised personnel need them for legitimate and permitted purposes, thus ensuring the full accessibility and mobility of the information (Bakker 1998; Mohammad 2010; Humaidi et al. 2011). Ideally, patients, as owners of their own data, should have visibility of who is accessing their information, and for what purpose (Bakker 1998; Mohammad 2010). Therefore, EHRs should be designed and secured in such a way that anyone accessing or editing the information contained in them should be visible to patients (Bakker 1998; Mohammad 2010).

3.4.4 Information security requirements of healthcare organisations

The information security goals of healthcare data systems, that is, to ensure confidentiality, availability, integrity, accountability and non-repudiation, are to be achieved as required/determined by those factors which drive/create the need for information security in healthcare. Those driving factors, or information security drivers include legal, statutory, regulatory, and contractual requirements, business requirements, and the threat landscape faced by healthcare organisations (Schumacher et al. 2006; Gerber & von Solms 2008; Shoniregun et al. 2010; Sunyaev 2011; Jirasek 2012; Mohapatra & Singh 2012). Each of these requirements of information security in healthcare are discussed below.

3.4.4.1 Legal, statutory, regulatory, and contractual requirements for the information security of healthcare data systems

Governments are generally responsible for safeguarding public interests, including in public health services through their health departments or ministries, so they may decide or direct any changes in the use of information technology at the organisational level (Win & Fulcher 2007; Gerber & von Solms 2008; Mohammad 2010; Mohapatra & Singh 2012). The funding for the implementation of any program or any changes thereof are funded by taxpayers' money, and therefore governments have to consider public opinion and priorities (Gerber & von Solms 2008; Mohammad 2010; Mohapatra & Singh 2012). Moreover, any legislation that governs the use of information technology and patient privacy/confidentiality is enacted by national or supranational governments, e.g. the EU (Gerber & von Solms 2008). Thus, governments pass/enforce different laws, statutes and regulations which define the legitimate and permitted usage of medical information in a way which is binding upon all healthcare organisations and their stakeholders (Gerber & von Solms 2008; Mohammad 2010). If any of the stakeholders do not comply with these laws, they face penalties within the bounds of the laws and regulations (Gerber & von Solms 2008). Therefore, the information stored in electronic healthcare records can only be used within the limitations of applicable laws, and information security goals must be achieved according to the specified legal requirements.

The term 'legal' implies a rule recognised by the state which is binding upon its subjects, with the purpose of preserving order and promoting justice in society (Gerber & von Solms 2008). Statutes are written laws passed and enacted by a legislative body (generally a parliament); once passed, they are known as Acts of Parliament (Gerber & von Solms 2008). Data protection/privacy acts are the laws which specify the legitimate and authorised usage of the personal data of members of the public (DH/Digital Information Policy 2007; Win & Fulcher 2007; Gerber & von Solms 2008; Jirasek 2012). For example, according to the Data Protection Act (1998) of the United Kingdom, health information is a form of "personal data", and health records are recognised as "accessible records". Section 4(3) of Schedule 3 of the Act requires the explicit consent of the patient to process his/her personal data. Access can only be granted for legitimate activities. However, according to Article 8 of the same section, if access to the information is necessary for medical purposes, a health professional may proceed and access it without seeking explicit consent (DH/Digital Information Policy 2007; Win & Fulcher 2007; Gerber & von Solms 2008; Jirasek 2012). Likewise, the Freedom of Information Act (2000) provides exceptions to sharing information in areas such as health and safety information and personal information (HSCIC 2014). Similarly, the Access to Health Records Act (1990) grants the right of access to health records in cases where the right of access may be wholly or partially excluded, or where corrections of inaccurate health records are required (HSCIC 2014). Although patients are permitted to see their medical reports, in certain circumstances they may be prohibited from viewing all or a part of those reports if a doctor thinks that viewing the report may cause serious harm to the patient, or that third party information may be disclosed (HSCIC 2014). Furthermore, in the USA, the legitimate use and disclosure of the information contained in EHRs is governed by specific legislation such as the Privacy Rule of the Federal Regulations of The American Health Insurance Portability and Accountability Act (HIPAA). Parties who are legally authorised to collect, store, use, and disclose healthcare information, known as ‘covered entities’ by HIPAA, are required to adopt administrative, physical and technical safeguards to protect the information contained in EHRs in order to control and monitor information access within and between organisations (Meingast et al. 2006; Win & Fulcher 2007; Appari & Johnson 2008).

In addition to legal requirements governing information security, regulatory requirements are also in place on how to manage information security in healthcare organisations (Meingast et al. 2006; DH/Digital Information Policy 2007; Gerber & von Solms 2008). In this sense, the meaning of 'regulatory' is to supervise or control according to rules and regulations, whereas a regulation means "a rule or directive made and maintained by an authority" (Gerber & von Solms 2008). For example, the NHS in the UK recommends certain codes of practices to achieve the information security goals of healthcare organisations, such as NHS Code of Practice on Confidential Information (2014), the Confidentiality: NHS Code of Practice (2003), the Information Security Management: NHS Code of Practice (2007), Records Management: NHS Code of Practice, Part 1, (2006), Records Management: NHS Code of Practice, Part 2, (2009), and NHS Information Governance: Guidance on Legal and

Professional Obligations (2007). These aforementioned codes of practice recommend that information security standards as per the ISO/IEC 27000 series should be applied in the NHS. NHS Information Governance: Guidance on Legal and Professional Obligations (2007) identifies ISO/IEC 27001 as the relevant standard. Furthermore, the Code of Practice on Confidential Information (2014) and Information Security Management: NHS Code of Practice (2007) recommend that ISO/IEC 27001 is to be followed to *"provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System"* in order to achieve the NHS's information security goals.

Continuing with this chapter's look at definitions, 'contractual' means a written or verbal agreement enforceable by law (Gerber & von Solms 2008). In adhering to privacy and data protection laws, healthcare organisations must place appropriate contract mechanisms in place to consider the individual, free, and informed consent of their patients with regard to the storage, processing, and usage of their personal and medical information (Kluge 2004; Wiant 2005; Win & Fulcher 2007; Sheppard et al. 2009; Mohammad 2010; NHS 2010). This is because one of the most important objectives of information security in healthcare is to provide protection against *"any expected threats of security breach that could affect Patients' privacy and confidentiality"* (Mohammad 2010). Furthermore, according to Papazafeiropoulou & Gandecha (2008), the issue of patients' free and informed consent is important because patients may not be able to determine what will happen to their medical and personal information and who will be able to access and use their data. Therefore, acquiring *"informed, competent and voluntary consent"* is considered the legal and most ethical way of confirming consent (Kluge 2004) as it implies that a patient understands the information provided, and also understands the consequences of requesting their consent.

Thus, the information security of healthcare data systems is required to ensure that the legal, statutory, regulatory, and contractual requirements of the healthcare sector are adequately met in order to protect patients' interests and to avoid any legal penalties due to non-compliance with the legal requirements.

3.4.4.2 Business requirements

It is important that healthcare professionals have timely access to correct and complete patient information in order to provide proper and timely treatment to their patients, as failure to do so may have potentially fatal consequences (Smith & Eloff 1999; Tzelepi et al. 2002; Reni et al. 2004; Sheppard et al. 2009; NHS 2010). Healthcare professionals cannot be expected to remember data on a huge number of patients; they therefore need recorded data in an electronic format to ensure continuity of care (Bakker 1998). Further, specialisation in healthcare has increased in recent years due to progress being made in medical knowledge, so often, several specialists and professionals work together as a team to provide healthcare services on the basis of easily accessible and electronically recorded data (Takeda et al. 2000).

Furthermore, the data is also needed for some secondary but useful purposes such as to support logistics, administration, management, medical research, quality and safety measurement, public health policies, payments and insurance claims, and marketing (Bakker 1998; Takeda et al. 2000; Safran et al. 2007). The secondary use of health data has the potential to enhance individuals' healthcare experiences, expand research-based knowledge about disease and appropriate treatments, facilitate public health policies, and strengthen healthcare businesses by highlighting and meeting customers' needs (Safran et al. 2007).

Because the fast and efficient availability of the patient data is required for the delivery of healthcare services and for the aforementioned types of secondary usage, ensuring privacy/confidentiality and integrity becomes more challenging due to the need for increased accessibility (Mohammad 2010). Although confidentiality is a legal requirement, it must be balanced against patients' safety and consumer and public interests (Smith & Eloff 1999; Win & Fulcher 2007). Moreover, the privacy/confidentiality of patient data is also required by medical ethics and by good business sense (Tzelepi et al. 2002).

Thus, the delivery of reliable and efficient healthcare services is the primary focus of healthcare data systems. Uninterrupted and readily accessible patient information in the correct form is required by healthcare professionals to ensure the correct, prompt, and appropriate treatment of patients. Patient information is also required for secondary purposes such as medical research and the management of healthcare services. Although the assurance of confidentiality of patients' data is a legal requirement, it is also a business requirement related to patients' trust in the healthcare data systems. The information security of healthcare data systems is required to ensure the delivery of reliable and efficient healthcare services, and to support useful secondary usage of patients' information while maintaining the privacy/confidentiality of patients' data.

3.4.4.3 Threat landscape

Papazafeiropoulou & Gandecha (2008) note that every year, the number of people who have died due to unintentional medical errors is higher than that who died in vehicle accidents, or from breast cancer or AIDS. Incomplete patient information, unavailable drug information, and miscommunication because of poor handwriting or errors in writing are common causes of such medical errors (Papazafeiropoulou & Gandecha 2008). As well as unintentional medical errors, intentional threats are sometimes made to patients' data. For example, a healthcare organisation’s employees can gain unauthorised access to patients' data, affecting the privacy, integrity, or even availability of the same (Smith & Eloff 1999; Appari & Johnson 2008; Tyson & Slocum 2012). Such threats may emerge from internal agents such as employees who may be abusing their rights and privileges, or may simply be incompetent (Smith & Eloff 1999; Wiant 2005; Appari & Johnson 2008; Tyson & Slocum 2012).

Historically, the most common threats have emerged from the internal environment of a healthcare organisation, as 49 percent of the total breaches reported occur due to stolen or lost laptops or mobile devices used by healthcare professionals (Wiant 2005; Tyson & Slocum 2012). In addition to the accidental exposure of information, security can also be breached intentionally by a healthcare employee who wishes to steal information by 'computer abuse' in order to sell it on the black market (Wiant 2005; Appari & Johnson 2008; Tyson & Slocum 2012). Wiant (2005) defines computer abuse as "*the unauthorised, deliberate, and internally recognisable misuse of computers of any organisation's information system by individuals*". However, accidental exposure by an employee due to negligence, ignorance, or carelessness has been identified as the most common problem (Wiant 2005). More specifically, in the healthcare industry, a lack of appropriate access controls for secondary users of medical information such as insurance companies, pharmaceutical companies, and medical students, is also among the greatest threats to data security (Wiant 2005).

In addition to internal threats, other sources of threat emerge from the external environment of a healthcare organisation. External threats such as hackers (who are becoming more systematic and dedicated) are also dangerous for the information security of a healthcare organisation (Appari & Johnson 2008; Tyson & Slocum 2012). External threats exploit the vulnerabilities of the information systems of healthcare in order to achieve their objectives by compromising the systems' information security (Appari & Johnson 2008; Tyson & Slocum 2012).

Furthermore, internal and external threat agents can have different causes, motivations, and objectives. First, an accidental disclosure may result in the unintentional disclosure of patient information by healthcare personnel (Wiant 2005; Appari & Johnson 2008). Second, an insider's curiosity may result in unauthorised access to patient information by healthcare personnel arising from their own curiosity or other personal interests (Wiant 2005; Appari & Johnson 2008). Third, a data breach by an insider may result in the transmission of information to an outsider to seek profit or for personal reasons (Wiant 2005; Appari & Johnson 2008). Fourth, a data breach by an outsider via physical intrusion may result in an outsider physically entering the healthcare facility by coercion or forced entry in order to access the information systems (Wiant 2005; Appari & Johnson 2008). Fifth, a data breach by an outsider is possible through attacking the network system to access patient information or by affecting the integrity and availability of the data (Wiant 2005; Appari & Johnson 2008).

Overall, threats may be characterised by four factors: motives, resources, accessibility, and technical capability. Depending on these factors, different types of threats pose different levels of risk to organisations, and therefore may require different mitigation or prevention strategies. Systemic threats emerge when an internal or external agent exploits the disclosed data beyond its permitted and intended use (Appari and Johnson 2008). The resources of threat agents vary from basic computing, banking, and financial skills to well-organised and funded infrastructure posing serious risks to crucial healthcare services (Appari and Johnson 2008). Threat agents may need different types and levels of access to carry out the intended breaches, such as access to data authorisation, system authorisation, and site authorisation (Appari and Johnson 2008). The technical abilities of threat agents are also likely to vary from novices to high-level sophisticated programmers, and given the value and importance of data to some threat agents, expert hackers may even be hired (Appari & Johnson 2008).

Thus, the information security of healthcare data systems is required to cope with a range of internal and external sources of threats which may compromise their security intentionally or unintentionally due to different motivations, causes, and objectives.

3.4.5 Information security strategy of healthcare data systems

The information security strategy of healthcare data systems can be explained as a roadmap for the foreseeable future which intends to progress along the path to system maturity in order to achieve information security goals according to the requirements of a healthcare organisation which wishes to ensure the continuous, efficient, reliable, and legally compliant delivery of healthcare services (Mohammad 2010). A specific standard ISO/IEC 27799 based on the standards ISO/IEC 27001 and 27002 was published in 2008 to support the development of information security strategies for healthcare organisations. Healthcare organisations can choose from 11 security control categories and 39 security control sub-categories. The security control categories include controls relating to information security policy, the organisation of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, information security aspects of business continuity management, and compliance (ISO 27799:2008 2008).

3.4.6 Information security management system (ISMS) for healthcare data systems

An Information Security Management System (ISMS) as a basic requirement is recommended by ISO 27799, which notes that healthcare organisations in different jurisdictions may have different legal requirements, and clinical processes may vary on the basis of specialist devices such as scanners and infusion machines, which may also affect/change the specific information security requirements of the organisations. ISO 27799 also recommends the adoption of an "Information Security Management System (ISMS)" based on ISO/IEC 27002. The standard states that precedence of best practices and international experience show that the adoption of an ISMS, as shown in figure 3.3, below, facilitates the achievement of information security objectives according to the specific information security requirements of healthcare sector organisations (ISO 27799:2008 2008).

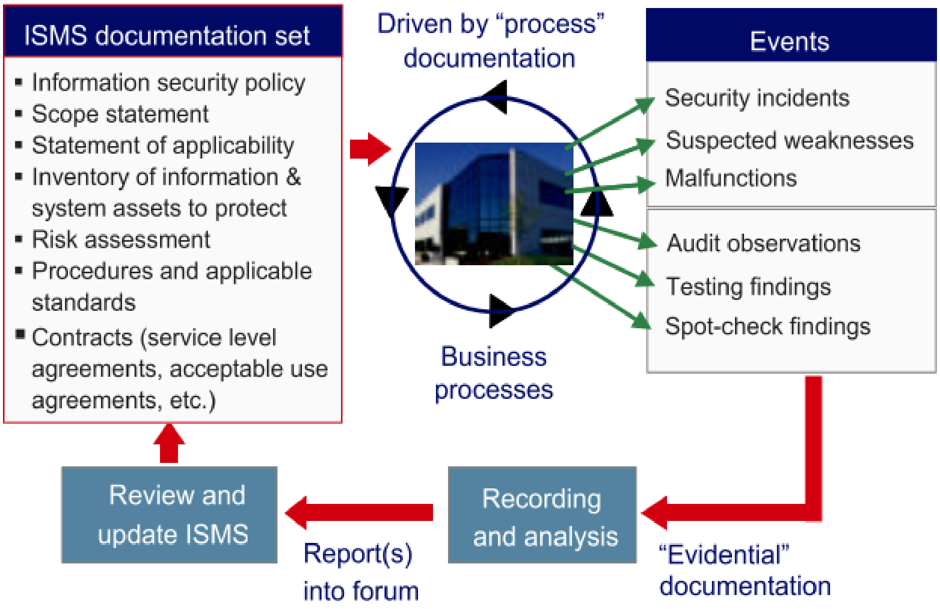

ISMS documentation set
▪ Information security policy
▪ Scope statement
▪ Statement of applicability
▪ Inventory of information & system assets to protect
▪ Risk assessment
▪ Procedures and applicable standards
▪ Contracts (service level agreements, acceptable use agreements, etc.)
Driven by "process" documentation
Business processes
Events
Security incidents
Suspected weaknesses
Malfunctions
Audit observations
Testing findings
Spot-check findings
"Evidential" documentation
Recording and analysis
Report(s) into forum
Review and update ISMS

Figure 3.3 Information Security Management System for healthcare organisations (ISO 27799:2008 2008)

Moreover, the PDCA or Plan-Do-Check-Act process is generally employed in order to establish, operate, maintain, and improve the information security management system of a healthcare organisation (DH/Digital Information Policy 2007; ISO 27799:2008 2008).

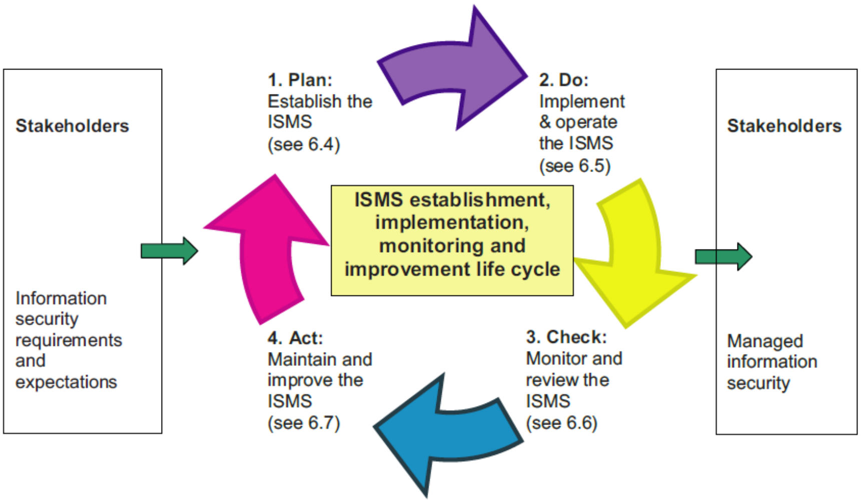

Stakeholders
Information security requirements and expectations
1. Plan: Establish the ISMS (see 6.4)
2. Do: Implement & operate the ISMS (see 6.5)
ISMS establishment, implementation, monitoring and improvement life cycle
4. Act: Maintain and improve the ISMS (see 6.7)
3. Check: Monitor and review the ISMS (see 6.6)
Stakeholders
Managed information security

Figure 3.4 The ISMS process overview for healthcare organizations (ISO 27799:2008 2008)

3.4.6.1 Planning: establishment of the ISMS for healthcare

According to ISO/IEC 27799, confidentiality/privacy, availability, integrity, authenticity and non-repudiation are the overarching goals of information security in the context of healthcare data systems. In the planning phase of the PDCA process, the legal, statutory, regulatory, contractual and business requirements of the healthcare organisation are determined and a risk assessment is carried out in relation to existing internal and external threats (DH/Digital Information Policy 2007; ISO 27799:2008 2008). Further, controls are identified to mitigate the information security risks, and to transfer or accept them on the basis of the information security requirements of the organisation (DH/Digital Information Policy 2007; ISO 27799:2008 2008).

As for any other type of organisation's data systems, risk assessment is crucial to the information security management of healthcare data systems. The identification and quantification of the risks in terms of their potential severity and the likelihood of their occurrence is required in order to prioritise them. Once identified and prioritised, risks are managed by the identification and implementation of the most suitable information security controls (DH/Digital Information Policy 2007). Moreover, a healthcare organisation needs an overall information security policy to state how it manages the security of its information assets. An information security policy should define the roles and responsibilities of information security management and specialists or other staff working in the organisation in order to ensure compliance with such a policy (DH/Digital Information Policy 2007).

3.4.6.2 ‘Do’: The implementation of an information security strategy by a healthcare organisation

In the planning phase, after the identification of information security controls to manage information security risks, action plans, training and awareness programs are developed and implemented in the ‘Do’ phase of the information security management process (DH/Digital Information Policy 2007; ISO 27799:2008 2008).

3.4.7 Summary of Findings for RQ3

The requirements of an information security strategy for healthcare data systems have been shown to be different than those found in other sectors (see Table 3.2). Electronic healthcare records need to be protected in a way that addresses their specific security concerns based on legal, statutory, regulatory, contractual, and business requirements, and which protects against internal and external threats in order to meet the information security goals of healthcare data systems (see Table 3.3). Consequently, information security strategies of healthcare data systems have to be based on those information security requirements to meet information security goals of the healthcare organisations. ISO 27799 is a specific standard which includes a range of information security controls which should be selected for relevance and applied by healthcare organisations according to their requirements.

Goals and Nature of Information Security of Healthcare Data		
No	**Name**	**Short description**
1	Information security goals of healthcare data systems	The goals of healthcare data systems (confidentiality, availability, integrity, accountability and non-repudiation) are to be achieved as required/determined by those factors which drive/create the need for information security in healthcare. (Schumacher et al. 2006; Gerber & von Solms 2008; Shoniregun et al. 2010; Sunyaev 2011; Jirasek 2012; Mohapatra & Singh 2012).
2	Why is information technology required for the delivery of healthcare services and what challenges does this technology bring with it?	In efforts to increase the level and functionality of sharing, new technologies are adopted to considerably reduce the time and effort needed in the delivery of healthcare services, but this also brings new challenges in using the technology related to ensuring the confidentiality, availability, and integrity of the patients' data (Bakker 1998; Mohammad 2010; Humaidi et al. 2011).
3	Why is healthcare data important?	Governments may require trustworthy medical information for the sake of national planning and budgeting (Anderson 2000; Humaidi et al. 2011). Physicians’ and nurses’ uninterrupted and smooth access to the data in its correct form is necessary to perform their healthcare duties (Anderson 2000; Jafari et al. 2009; Linden et al. 2009; Mohammad 2010; Liu et al. 2011). Insurance companies may need access to their clients’ medical information to process and verify the genuineness of the claims filed by their clients (Anderson 2000; Humaidi et al. 2011; Liu et al. 2011). Pharmaceutical companies may need this data for the development of new medicines and to study the effects and side-effects of previously used treatments (Anderson 2000; Liu et al. 2011). Medical students may need access to health data for their research and education (Anderson 2000; Liu et al. 2011).
4	Secondary	Data is also required for secondary but useful purposes such as

	usage of the healthcare data	to support logistics, administration, management, medical research, quality and safety measurement, public health policies, payments and insurance claims, and marketing (Bakker 1998; Takeda et al. 2000; Safran et al. 2007).
5	Why is healthcare data particularly vulnerable?	The different types of information contained in EHRs may be attractive to different individuals, groups, or businesses, and can serve different purposes (Jafari et al. 2009; Kuang & Ibrahim 2009). Data breaches have shown that personal information is attractive to criminals (Von-Solms 1996; Jafari et al. 2009; Humaidi et al. 2011). The utility of medical data can be both economic and social for different stakeholders (Anderson 2000).
6	Increased Level of Sharing of Healthcare Data: Potential benefits and challenges	Information security in healthcare is needed in the first instance to gain the benefits of quality and efficiency from EHR systems, because an increased level of sharing through the adoption of new technologies is required, which increases the risks faced by healthcare data systems (Bakker 1998; Mohammad 2010; Humaidi et al. 2011). Therefore, it is challenging to implement a shared EHR system which is both easy and secure to use while considering the interests of all stakeholders including patients, healthcare professionals, and healthcare organisations.
7	Consequences of Increased Accessibility	Increased accessibility means that records can be accessed, changed, viewed, copied, used, disclosed, and deleted more easily (Loef et al. 2002; Wiant 2005; Linden et al. 2009; Humaidi et al. 2011; Liu et al. 2011).
8	Consequences of threats to healthcare data systems	Papazafeiropoulou & Gandecha (2008) note that every year more people died due to unintentional medical errors than from of vehicle accidents, breast cancer or AIDS. Anecdotal evidence over the last few years has suggested that a lack of appropriate security measures has resulted in many data breaches, which have affected patients financially, mentally, and socially (Appari & Johnson 2008; Tyson & Slocum 2012). Therefore, EHRs should be designed and secured in such a way that anyone accessing or editing their information should be visible to patients (Bakker 1998; Mohammad 2010).

Table 3.2 Goals and Nature of Information Security of Healthcare Data

Information Security Requirements for Healthcare		
No	**Name**	**Short description**
1	Legal, Statutory, Regulatory, and Contractual Requirements of Information Security	Data protection/privacy acts are laws which specify the legitimate and authorised usage of the personal data of members of the public (DH/Digital Information Policy 2007; Win & Fulcher 2007; Gerber & von Solms 2008; Jirasek 2012). Any legislation that governs the use of information technology and patients' privacy/confidentiality is enacted by national or supranational governments, such as the EU (Gerber & von Solms 2008). There are regulatory requirements to manage information security in healthcare organisations (Meingast et al. 2006; DH/Digital Information Policy 2007; Gerber & von Solms 2008). The meaning of 'regulatory' is to supervise or control according to rules and regulations. The information stored in electronic healthcare records is to be used within the limitations of applicable laws, and information security goals are to be achieved according to the specified legal requirements.
2	Privacy requirements	Concerns regarding the privacy and security of patient data are genuine because patients and healthcare organisations need to rely on the privacy of patients' information and the delivery of reliable and efficient healthcare services (Anderson 2000; Loef et al. 2002; Wiant 2005; Jafari et al. 2009; Kuang & Ibrahim 2009; Linden et al. 2009; Liu et al. 2011).
3	Consent Mechanism Requirements	Patients, as owners of the data, should be able to see who is accessing their information, and for what purpose (Bakker 1998; Mohammad 2010). Healthcare organisations have a social responsibility to ensure the confidentiality of patients' information and consider their consent in the disclosure or non-disclosure of their medical and personal information (Humaidi et al. 2011). Hence, the utility of medical information is different for different stakeholders depending on the interests and stakes of the parties involved. Healthcare organisations are responsible for respecting their patients' privacy and ensuring the information security of the patients' information while considering their consent regarding the use of their medical and personal information (Mohammad 2010).
4	Business Requirements	It is important that healthcare professionals have timely access to correct and complete patients' information in order to provide proper and timely treatment of patients; the failure to do this may result in potentially fatal treatment (Smith & Eloff 1999; Tzelepi et al. 2002; Reni et al. 2004; Sheppard et al. 2009; NHS 2010) The purpose is to keep a record of a patient's information to facilitate improved care through continuous, safe, effective, efficient, timely, patient-centred and quality-oriented healthcare

		which may be provided by different healthcare professionals (Otieno et al. 2008; Häyrinen et al. 2008; NHS 2010; Liu et al. 2011).
5	Data quality requirements	Healthcare data must be complete, valid, consistent, available when needed, and accurate (Fraser et al. 2005; Sunyaev 2011). In order to gain the maximum benefits of EHRs while ensuring the required level of information security, healthcare records should be complete and comprehensive, as well as sufficiently secure to maintain patient data confidentiality (Bakker 1998; Blyth & Kovacich 2006; Kuang & Ibrahim 2009; Mohammad 2010; Humaidi et al. 2011; Sunyaev 2011). It is important that healthcare professionals have timely access to correct and complete patients' information in order to provide proper and timely treatment of patients; the failure to do this may result in potentially fatal treatment (Smith & Eloff 1999; Tzelepi et al. 2002; Reni et al. 2004; Sheppard et al. 2009; NHS 2010).
6	Training and awareness requirements	Continuous changes in information technology and legal legislation make training and awareness very important in the healthcare sector (GAO 2006; DH/Digital Information Policy 2007; Aldajani 2012). “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” (Mohammad 2010).
7	Threats landscape of healthcare data systems	Incomplete patient information, unavailable drug information, and miscommunication because of poor handwriting or errors in writing are among the common causes of medical errors (Papazafeiropoulou & Gandecha 2008). In addition to unintentional medical errors, intentional threats to patients' data also exist (Smith & Eloff 1999; Appari & Johnson 2008; Tyson & Slocum 2012). The most common threats have emerged from the internal environment of a healthcare organisation, as 49 percent of the total breaches reported occur due to stolen or lost laptops or mobile devices used by healthcare professionals (Wiant 2005; Tyson & Slocum 2012). External threats, such as more systematic and dedicated hackers, are also dangerous to the information security of a healthcare organisation (Appari & Johnson 2008; Tyson & Slocum 2012).

Table 3.3 Information Security Requirements for Healthcare

3.5 Findings for RQ4: How can the effectiveness of an information security strategy be measured?

The objective of this question was to understand the aims and objectives of information security evaluations in addition to explaining the processes and methods applied to achieve those aims and objectives. The findings of the 34 studies selected to answer the research question RQ4 are discussed in the sub-sections below.

No	Areas covered	Selected studies from the SLR for Research Question four
1	Why should the effectiveness of information security strategies be measured?	(Barnard & von Solms 2000), (Data Protection Audit Manual 2001), (Hart 2001), (Siougle & Zorkadis 2002), (Hamill et al. 2005),, (Wiant 2005), (GAO 2006), (Booker 2006), (Ekelhart et al. 2007), (Yoo et al. 2007), (Goel et al. 2007), (Pishva et al. 2007), (Biskup 2009), (Jafari et al. 2009), (Eminağaoğlu et al. 2009), (Goel & Chengalur-Smith 2010), (Vladimirov et al. 2010), (Dogaheh 2010), (Lukasik 2011), (Sunyaev 2011), (Kumar & Puri 2012), (Tyson & Slocum 2012), (Jirasek 2012).
2	How is the effectiveness of information security strategies measured?	(Barnard & von Solms 2000), (Hart 2001), (Siougle & Zorkadis 2002), (Ko et al. 2005), (Brooks & Warren 2006), (DH/Digital Information Policy 2007), (Kulmala 2007), (Saleh et al. 2007), (Vladimirov et al. 2010), (Shoniregun et al. 2010), (Mohapatra & Singh 2012).
3	Process of evaluation: • Pre-evaluation Preparations Phase • Evaluation Phase • Analysis Phase • Reporting Phase	(Barnard & von Solms 2000), (Hart 2001), (Siougle & Zorkadis 2002), (Niazi et al. 2005), (Brooks & Warren 2006), (DH/Digital Information Policy 2007), (Kulmala 2007), (Yoo et al. 2007), (Saleh et al. 2007), (ISO/IEC 21827 2008), (Jafari et al. 2009), (Vladimirov et al. 2010), (Sunyaev 2011), (Atymtayeva et al. 2012).

3.5.1 Why should the effectiveness of information security strategies be measured?

The development of defensive strategies to meet its information security requirements can help an organisation to manage its risks effectively (Tyson & Slocum 2012). Booker (2006) argues that in a fluid, rapidly changing, highly variable security environment featuring an increasing number of common and advanced threats, organisations need "an organised, efficient, and proactive approach to information security". Jirasek (2012) observes that the well-known general statement "What you cannot measure, you cannot manage" can be fairly applied to the field of information security. Consequently, in order to have trust in the planned and implemented security program, information security managers need to cater for an evaluation of the same on the basis of a set security standard (Hart 2001; Siougle & Zorkadis 2002; Sunyaev 2011; Jirasek 2012). PDCA, which stand for Plan - Do - Check – Act, which is generally known as the implementation cycle of information security management systems (ISMS), requires that an organisation must also check, evaluate, monitor, or measure the operation of the security controls it has implemented based on its security policy (Pishva et al. 2007). Therefore, the audit, assessment, evaluation, or measurement of information security strategies is a practical way of improving the state of information security, and is important to improving the chosen strategy and managing risks (Pishva et al. 2007; Vladimirov et al. 2010).

There may be different circumstances in which an evaluation of an organisation's information security strategies is required. Managers may decide to undertake an evaluation in order to ensure that their organisation meets compliance and regulatory demands, to counter the reoccurrence of a particular security incident, to place security at a higher priority, to cope with a situation in which information assets have become lucrative target for cybercriminals, or to exercise their internal security auditing team (Vladimirov et al. 2010). Such evaluations not only facilitate organisations to comply with laws and regulations, but can also help them to more effectively handle personal information, and to respect the interests of individual data subjects (Data Protection Audit Manual 2001). Furthermore, evaluations can be performed to achieve one or more of the following objectives: to measure the information security procedures of two or more different organisations in order to facilitate their interoperability (Jafari et al. 2009); to select a better strategy to improve information security; to achieve maximum operational capability and lower resource costs (Hamill et al. 2005); to detect and stop computer abuse by employees (Wiant 2005); to measure the breadth, clarity, and brevity of the information security strategies (Goel & Chengalur-Smith 2010); to evaluate the evaluation reports of other organisations to find common issues/problems (GAO 2006) or to compile the best practices of organisations in the same industry (Kumar & Puri 2012); to examine the information security products or systems for their claimed level of security (Ekelhart et al. 2007; Biskup 2009); to determine the level of security of the organisation at different points of time (Dogaheh 2010); or to identify the weaker and stronger areas of the current strategy (Brooks & Warren 2006; Yoo et al. 2007).

While evaluations of the functionality, correctness, and effectiveness of security controls can be performed off-site or on-site, the operational procedures can only be evaluated on-site (Barnard & von Solms 2000) because information security is not only about the use of technology; it also involves the people who use or implement the technology (Wiant 2005; Hamill et al. 2005; Eminağaoğlu et al. 2009; Lukasik 2011). Moreover, evaluations can be performed by internal information security staff or by an external individual or organisation with the requisite expertise (Data Protection Audit Manual 2001; Tyson & Slocum 2012). Since the aim of this research is to develop an evaluation model which can be used by internal or external information security experts to improve the information security strategies already in place in healthcare organisations by the determination of the weaker and stronger areas of the applied strategy, the subsequent analysis will be focused accordingly.

3.5.2 How is the effectiveness of information security strategies measured?

The use of evaluation models is an important way to measure the effectiveness of information security strategies in terms of their adequacy and quality (Kulmala 2007). Mohapatra & Singh (2012) note that "if [information security] can be measured, it will be done", and "The value proposition is weakened significantly, if it cannot be quantified and measured". Shoniregun et al. (2010) argue that the main advantage of model based evaluations is the simplicity of the analysis in deriving quantitative measures or security metrics; they can therefore be used in the estimation of quantitative or quantified security measures. Evaluation models generally explain the process and method of evaluation (Barnard & von Solms 2000; Hart 2001; Siougle & Zorkadis 2002; Brooks & Warren 2006; Saleh et al. 2007; Kulmala 2007; DH/Digital Information Policy 2007; Vladimirov et al. 2010).

3.5.2.1 Process of evaluation

The evaluation process should be systematic and clear so that the effectiveness of information security strategies can be measured in a meaningful manner. Barnard & von Solms (2000) suggest an evaluation process to facilitate the BS 7799 certification of an organisation. The process of evaluation found in literature generally includes four major stages, each of which are now discussed in turn.

Pre-evaluation Preparations Phase

Barnard & von Solms (2000) suggest that an evaluation activity should be appropriately planned before the actual evaluations are performed. This planning should be based on the understanding of the information security strategy, knowledge of the target of the organisation’s information security, identification of the target/goals/conditions of evaluation, planning of the appropriate actions, and selecting the corresponding methodologies and tools (Barnard & von Solms 2000; Hart 2001; Brooks & Warren 2006; Kulmala 2007; Saleh et al. 2007; Vladimirov et al. 2010). According to Hart (2001), the security team entrusted with the task may even decide to conduct, or not conduct, an evaluation depending upon the needs/targets of the information security of the organisation. However, in planning an evaluation effectively, a strong knowledge base will help the security team/evaluators to understand the assets which need to be protected, the types of threats and threat scenarios which threaten the assets, the vulnerabilities in the assets which may be exploited by the threats in order to compromise the information security of critical assets, and the available controls applied against the existing threats and vulnerabilities to ensure the information security of the organisational assets (Atymtayeva et al. 2012).

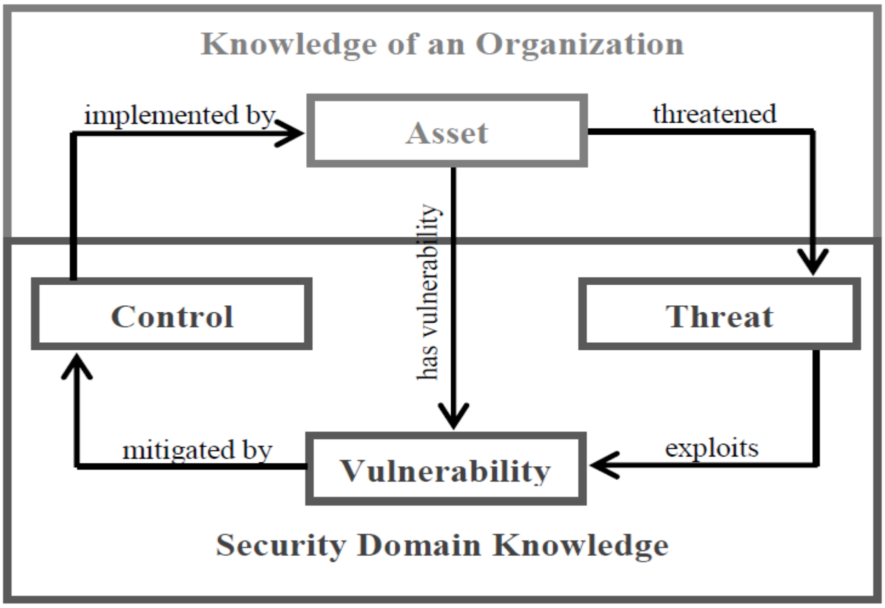


Figure 3.5 The knowledge model showing the elements of security knowledge base (Atymtayeva et al. 2012)

Evaluation Phase

The pre-evaluation preparations mentioned above facilitate the evaluators to determine why an evaluation is required, and what is to be evaluated. Subsequently, evaluations are performed with the help of certain tools and methods, such as checklists of the information security controls being applied and the information security requirements of the organisation. Since an information security strategy includes information security control items within different control categories and sub-categories, the effectiveness of each of these controls may be measured on the basis of a predefined criteria. Some of the most frequently used criteria for evaluation are the Information Security Capability Maturity Model, the INFOSEC Assessment Capability Maturity Model (IA-CMM), the IS Program Maturity Grid, and the Murine-Carpenter SW Security Metrics (Kulmala 2007).

The effectiveness of an information security management system in managing risks to information must be measured through internal reviews and independent audits (DH/Digital Information Policy 2007). One of the important parts of the measure or evaluation phase is to assess and determine the current state of information security management in the organisation in order to highlight any weaknesses in the strategy (Saleh et al. 2007). The information security controls applied by the organisation are evaluated for their functionality, correctness, effectiveness, and operational capability to ensure that the controls are correctly installed, effectively meeting the desired objectives, and being used appropriately without any errors (Barnard & von Solms 2000; Siougle & Zorkadis 2002). To make the evaluations more effective, Vladimirov et al. (2010) suggest that evaluators check and test everything they can within the limitations of time, means, finances, and information security requirements.

In order to perform the evaluation, the evaluator analyses the security countermeasures or controls by means of a checklist (Brooks & Warren 2006). To complete the security evaluation, the evaluator compares the security controls already in place against the information security evaluation criteria (Brooks & Warren 2006).

Depending upon the level of maturity of the information security control being assessed, a value may be assigned with reference to a chosen set of criteria. For example, if the purpose of the evaluation criteria is to check if an information security control has been properly installed or not, a value of 1 may be given on the checklist to identify a control which is installed and value of 0 if it has not been installed. The range of values will vary according to the evaluation criteria.

Yoo et al. (2007) offer a comprehensive illustration of the evaluation of information security strategies by using the Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM) (ISO/IEC 21827:2008), and propose an evaluation model to measure the level of information security which is capable of highlighting the weaker areas of a strategy. Their checklist is based on 12 broader control categories, 54 control items, and 89 detailed control items, the latter of which are divided into 48 function level items and 41 function process items derived from BS7799 and ISMS (Information Security Management System, a Korean security standard developed for information security management). Their model is summarised in the table below.

Control Categories	Control Items	No. of Detailed Control Items
Information Protection Policy	Information protection organisation	1
	Information protection plan	1
Risk Assessment	Assets classification	2
	Resources allocation	3
	Review security requirement	1
	Risk assessment	4
	Weakness diagnosis	1
Configuration Management	Configuration change control	3
	Configuration security setting	2
Maintenance	Maintenance tool	1
	Remote maintenance	1
Media Protection	Media output indication	1
	Media access control	1

	Media transportation method	1
	Document control	3
	Media and record destruction	1
Security Awareness and Training	Security awareness training	2
Emergency Plan/Work Continuity Plan	Emergency training	1
	Simulated training and grading of emergency plan	1
	Communication service dualization	1
	Information system backup and recovery	3
Physical /Environmental Protection	Physical access control	3
	Display media access control	1
	Physical access monitoring	1
	Power facilities and lines protection	2
	Emergency power	1
	Emergency lighting	1
	Environmental control	1
Personnel Security	Antecedents inspection	1
	Personnel management	1
	Internal human resources management	1
	Third party security	1
Accident Response	Simulated training for accident	1
	Accident monitoring	1
	Security accident report	2
Audit and Responsibility Traceability	Audit object event creation function	2
	Audit information management	1
	Audit monitoring, analysis, and report	1
	Audit record time branding function	1
	Denial prevention	1
System Access Control and Communication Protection	Account control	1
	Password control	3
	Setting control	1
	Access control	6
	Access trial failure control function	1
	Notice function of the cautions for system use	2
	Previous login information report function	1
	Session control function	2
	Isolation of system and application software	2
	Shared system resources control	1
	Protection from software defect and malicious code	3
	Tools and technologies for invasion detection and interruption	2
	Service reject protection	1

	Security communication route	1
	Creation and control of encryption key	2
	Internet telephone	1

Table 3.4 Number of control and detailed control items for each category (Yoo et al. 2007)

The abovementioned 12 control categories, 54 control items and 89 detailed control items (see Table 3.4) are assessed on a five level criteria as defined by the Systems Security Engineering Capability Maturity Model (SSE-CMM) ISO/IEC 21827 (ISO/IEC 21827 2008) which can be used for the evaluation of an information security strategy. The results of the evaluation can then be verified by conducting interviews with managers, and verifying onsite documents and onsite observations or inspections. The following table (Table 3.5) provides definitions of the five levels of evaluation.

Level	**Description**
Level 1	Detailed control items are not executed, or are executed without specific plans.
Level 2	Execution plans (e.g. detailed procedures, schedules, and budget) for detailed control items have been established and documented.
Level 3	Detailed control items are being or have been executed according to documented plans.
Level 4	Results are measured for detailed control items and are executed consistently for a certain period.
Level 5	Results are reviewed and improved accordingly.

Table 3.5 Five levels of information security level assessment (Yoo et al. 2007; ISO/IEC 21827 2008)

Analysis Phase

The results of the evaluations based on the evaluation criteria need to be analysed in order to make sense of the weaknesses and strengths of the information security strategy being tested. Jafari et al. (2009) suggest that security metrics should be considered as numbers which have been computed to support decision making to enhance organisational performance and accountability through the collection, analysis, and reporting of relevant performance-related data. Thus, the collected evidence in the evaluation phase needs to be properly analysed to achieve the objectives of the evaluation, which have generally been set in the pre-evaluation preparation phase. Saleh et al. (2007) explain that the analysis phase includes an evaluation of the strengths, weaknesses, opportunities and threats evident from the collected data, and identification of the existing risks while suggesting protection measures, in order to update policy documents. Vladimirov et al. (2010) recommends pulling the results of the evaluation together, measuring and analysing the risks, and consideration of the realistic and practical remedies, all in the analysis phase. Brooks & Warren (2006) advise a comparison of the current and the required or ideal state of security in the analysis phase using a two-dimensional evaluation histogram, where the key areas of information security strategy are shown on the vertical axis and the required or ideal security level is plotted on the horizontal axis. According to Hart (2001), the identification of security gaps is the main objective of the analysis phase.

Reporting Phase

The strengths and weaknesses identified through the analysis of the evaluation data must be reported clearly and comprehensively (Jafari et al. 2009; Sunyaev 2011). Reporting serves at least two purposes: first, it communicates the evaluation results to the concerned organisation; and second; it can be used as a reference point for future evaluations, to specifically focus on those weaker areas identified in the previous evaluations (Kulmala 2007). The certification of an information security strategy is also considered a form of reporting, which indicates the existence of the minimum required level of information security in an organisation (Barnard & von Solms 2000). However, certification may or may not be accompanied by a report which recommends areas of improvement of the strategy. Vladimirov et al. (2010) suggest that the analysis phase should be followed by the generation of a detailed report to work with the client for any follow-up actions, if needed, to enhance their security.

3.5.3 Summary of Findings: RQ4

The evaluation of an organisation's information security strategy to identify its stronger and weaker areas, is essential to its improvement. An evaluation model generally projects the process of evaluation, that is, the four major stages: the pre-evaluation preparation phase; evaluation; analysis; and reporting. Evaluation activity is expected to be planned before the actual evaluations are performed. Such preparations and planning include establishing understanding of the information security strategy currently in place, knowledge about the targets of information security of the organisation, identification of the targets of evaluation, planning appropriate actions, and selecting the corresponding methodologies and tools. Subsequently, evaluations are performed with the help of certain tools and methods such as checklists of the information security controls applied to meet the information security requirements of the organisation. Further, an analysis of the evaluation results is required to determine the strengths, weaknesses, opportunities, and threats faced in order to suggest protection measures to the organisation on how to improve the strategy. Finally, reporting is usually needed to communicate the evaluation results to the concerned organisation and to create a reference point for future evaluations.

3.6 RQ5: Evaluation of the Information Security Strategy of Healthcare Data Systems

The findings for RQ5 are discussed below.

No	Areas covered	Selected studies from the SLR for Research Question five
1	Why are evaluations of the information security strategies of healthcare data systems required?	(Bakker 1998), (Kluge 2004), (GAO 2006), (DH/Digital Information Policy 2007), (Papazafeiropoulou & Gandecha 2008), (Jafari et al. 2009), (Shoniregun et al. 2010), (Sunyaev 2011), (Jirasek 2012), (Mohapatra & Singh 2012).
2	Evaluation model currently suggested for healthcare data systems: an example from the SLR	(Brooks & Warren 2006), (Yoo et al. 2007), (Tyson & Slocum 2012).

3.6.1 Why are evaluations of the information security strategies of healthcare data systems required?

The Government Accountability Office (GAO) in the USA has stressed for the need to develop a comprehensive programme of evaluations and tests for the information security programs of healthcare organisations in the country (GAO 2006). Their report recommended that the healthcare sector ensured that the controls selected for its information security were appropriate, effective, and in accordance with security requirements and policies. The report also noted that evaluations were important because they could determine the level of dedication of management towards an information security program, remind people of their roles and duties, and ensure compliance with the stated security policies. Evaluations also help to identify weaknesses and new problem areas, and check the appropriateness and application of controls, thus suggesting and identifying requirements for new controls. The report also advised that evaluations should be able to identify the existing risks, that they must be carried out periodically, i.e., at least once a year, and that they should be done by security specialists and business managers (GAO 2006).

In the UK’s NHS, information governance performance assessment and management arrangements facilitate and drive forward the changes required for improvement. Strategic Health Authorities, the Healthcare Commission and others responsible for monitoring NHS performance each play an important role in ensuring that effective information governance systems are in place (DH/Digital Information Policy 2007).

As has been discussed, the objective of information security in healthcare is to protect patient records and key information services as stipulated by the Data Protection Act 1998 and the Civil Contingencies Act 2004. This Code of Practice makes it incumbent on all NHS organisations and those supplying or making use of NHS information to ensure that appropriate measures for information security management are taken to protect the data they own, control or use. Higher levels of information security will ensure high-quality, evidence-based healthcare and other service deliverables. Therefore, the NHS Code of Practice (2007) states that an effective information security management regime can help to ensure higher standards of information security. Managers are required to identify the chosen evaluation method and documentation process relevant to the organisation. Evaluation methods should be based on the underlying principles of the Plan-Do-Check-Act (PDCA) model (introduced above in this study), as described by the ISO/IEC 17799:2005 standard (see Figure 21) (DH/Digital Information Policy 2007).

The British Standard Institute's BS7799 standards, which have been adopted and are known as ISO/IEC 17799:2005 and ISO/IEC 27001:2005, are recommended for NHS organisations by the NHS Code of Practice (2007). All healthcare organisations are required to follow these standards for the selection of appropriate controls and other information security provisions. Compliance with these standards is also required, so evaluations of compliance should conform with them (DH/Digital Information Policy 2007).

In order to effectively highlight the weaker and stronger areas of the information security strategies of healthcare data systems, it is important that evaluators are well aware of the specific information security drivers, such as laws and regulations, business objectives, and the threat landscape with regard to the confidentiality, privacy, and integrity of healthcare data (see the findings for RQ3, above). In order to determine the existing risks, evaluations must consider the specific threats to, and vulnerabilities of, healthcare data systems (see the findings for RQ2, above). Evaluations based on the specific requirements of healthcare using common metrics can not only help to identify the weaknesses of an information security strategy, but the objectives of interoperability to achieve efficient service delivery in terms of time and cost can also be facilitated by increasing the mutual trust levels of the different healthcare providers (Jafari et al. 2009).

Jirasek (2012) argues that every organisation has its own unique information security drivers which determine information security and which are shaped by its business objectives and environment. Healthcare has its own set of security drivers which make it different from other sectors in terms of the nature and stringency of its information security requirements. Therefore, information security strategies for healthcare should not only be developed but also be evaluated according to its specific requirements.

Bakker (1998) argues that the adoption of information technologies by healthcare organisations is necessary as it promises improvement in both the cure/care process, and efficiency in terms of time and cost. However, the limitations of technology, such as limited storage capacity, slower processing speeds, the incompatibility of operating systems, complex programming techniques, vulnerable networks, the inability of some healthcare professionals to use software interface, the complex processes of healthcare, continuous improvisation and variation in healthcare services, and the limited experience of healthcare organisations in developing themselves or outsourcing complex software systems, have been some of the challenges hindering the achievement of intended objectives (Bakker 1998).

Moreover, since the 1970s there has been a growing realisation that using information technology for healthcare services will increase the chances of unauthorised access to patient data, instances of the unintended disclosure of information, the unavailability of data due to technical issues, and the loss or inaccuracy of data, each of which may seriously harm the main objective of healthcare organisations, that is, to provide efficient and effective healthcare services (Bakker 1998). Over the years, these challenges have increased due to increased government regulations, especially with regard to the privacy/confidentiality of patients' data, the growth of E-Business, and familiarity with the usages of information technology which has added to the challenges by raising patients' expectations and demand for lower healthcare costs, and minimised time for service delivery coupled with more accuracy (Mohapatra & Singh 2012).

Papazafeiropoulou & Gandecha (2008) emphasise the importance of information security in healthcare by observing that in the US, "more people die every year due to medical errors than from vehicle accidents, breast cancer or AIDS". Some of the most common reasons for medical errors are: incomplete patient information; unavailable drug information; the miscommunication of drug orders due to poor handwriting, similarly named drugs; mistakes in the use of decimal points; the confusion of metric and other dosing units; inappropriate abbreviations; a lack of appropriate labelling of medicine; and a range of environmental factors such as lighting, heat, noise, and interruptions distracting healthcare professionals from performing their required tasks. Papazafeiropoulou & Gandecha (2008) suggest that one obvious way to reduce medical errors would be to make accurate, efficient, and reliable decisions based on complete and reliable patient records by enhancing their information security.

Ensuring the confidentiality of patients' data saved in healthcare records is one of the most important challenges for healthcare organisations. Data subjects, or patients, have been increasingly concerned about the privacy of their medical information for multiple reasons, such as wishing to avoid social stigma in the case of having some disease; to avoid financial losses by losing their jobs due to their medical conditions; healthcare organisations selling their data to third parties for marketing or research purposes; and simply to avoid disclosing their medical conditions to the people around them (Shoniregun et al. 2010). Moreover, in order to protect the public interest in the protection of private and confidential medical and personal information, governments have enacted laws and regulations to ensure the confidentiality of healthcare records (Kluge 2004). Healthcare organisations’ ability to ensure the confidentiality of patients’ data and to provide efficient, secure, and reliable healthcare services has become an issue of competitive advantage and of proving their excellence within the industry (Sunyaev 2011).

On the one hand, the sharing of healthcare records in a manner that enhances the quality of service delivery and reduces the overall cost has long been desired by healthcare organisations (Bakker 1998; Jafari et al. 2009; Mohapatra & Singh 2012). On the other hand, though, healthcare organisations are concerned about the privacy and security of the healthcare data they hold (Jafari et al. 2009). In this context, interoperability among healthcare organisations have been problematic and challenging as an organisation is generally not sure about the actual information security posture/level and capability to protect healthcare data of other organisations (Jafari et al. 2009). Jafari et al. (2009) claim that this is due to the lack of common information security metrics which can be used to evaluate information security to compare the security posture of two or more organisations.

3.6.2 Evaluation model currently suggested for healthcare data systems: an example from the SLR

According to a 2006 survey in healthcare, a combination of factors including a clear reduction in the usage of information security technologies, ICT qualifications, and the training provided to employees caused an increase in security breaches compared to the years 2004 and 2005 (Brooks & Warren 2006). Tyson & Slocum (2012) claimed that this healthcare situation is expected to persist in the future, as 69 percent of healthcare providers lack proper policies and controls to detect and respond to breaches.

Brooks & Warren (2006) argue based on different surveys that managerial practices and the execution of information security controls are significantly deficient in different sectors, including healthcare. Therefore, healthcare needs to identify, apply, and evaluate controls more accurately (Brooks & Warren 2006). Maintenance of the integrity of patients' data is an important challenge for healthcare organisations, as a high level of protection against technological disasters and/or threats involving human error or sabotage is required. Therefore, any evaluations must consider both the technological and human aspects of the identified threats (Brooks & Warren 2006). The objectives of such evaluations are to identify security weaknesses and possible threats and attacks, to increase the organisational awareness of security issues, to improve the overall security of information systems, to reduce the cost and complexity of the evaluation methods, to provide results in a simple manner that non-IT professionals can easily understand, and to assist healthcare organisations to gain certification according to the required standards (Brooks & Warren 2006).

The model suggested by Brooks & Warren (2006) for healthcare organisations is similar to that proposed by Yoo et al. (2007). The purpose of their model is to highlight the weaker areas of a strategy, and the important question here is therefore whether or not such a model is sufficient to evaluate an information security strategy in the context of specific healthcare requirements. The suggested model for evaluation (Brooks & Warren 2006) adopts a case study method involving four steps. At the first step, scenario construction and modelling is done to understand the current state of the health data security systems. Document analysis and participant observation is suggested to achieve this objective.

A health information security analysis, which takes place at the second step, focuses on the countermeasures a healthcare facility has in place. This is done via a checklist based on existing good practices and recommended standards. The study suggests nine key areas for the checklist: Information Security Policy, Security Organisation, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Communications and Operations Management, Access Control, and Business Continuity Management and Compliance (Brooks & Warren 2006).

At the third step, a comparison is drawn between current security practices and the required ideal level of security, by converting the results of the checklist evaluation into percentage figures and plotting them onto a two-dimensional histogram where the key areas of information security control are shown on the vertical axis, and the percentage of ideal security (100 percent) on the horizontal axis, as shown in the following graph (Figure 3.6).

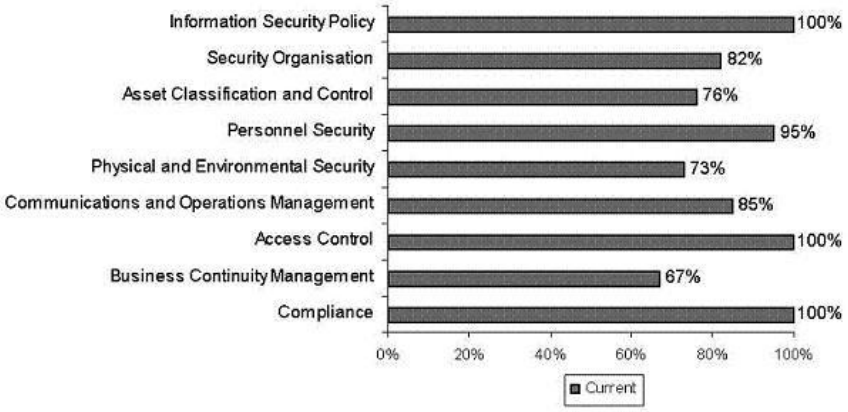


Figure 3.6 Projection of information security levels (Brooks & Warren 2006)

The final step involves a post-implementation analysis where the overall level of security is improved by suggesting new security features and analysing their possible effectiveness before they are applied. For this purpose, misuse case diagrams are suggested in order to document all the negative threat scenarios which require preventative measures. For example, an intruder could try to access unblocked ports to access the system, an attack which could be averted by installing a firewall.

After the analysis, the resulting evaluation report should be reviewed by the organisation’s management and IT staff in order to identify the existing weaknesses in the system, and to adopt the suggested security measures within their budget. A similar evaluation after a specific period would help in assessing the effectiveness of the suggested controls and establishing whether the level of information security has actually improved (Brooks & Warren 2006).

3.6.3 Summary of the findings for RQ5

The purpose of the evaluation of information security strategies in healthcare data systems is to ensure that their information security controls are appropriate, effective and in accordance with the relevant security requirements and policies. The objective of information security in healthcare is to protect electronic healthcare records according to legal requirements such as the Data Protection Act 1998 and the Civil Contingencies Act 2004, as well as the other business requirements to ensure that the required level of availability and integrity of the data is being achieved.

In the UK, the NHS Code of Practice (2007) states that an effective information security management regime can ensure higher standards of information security of healthcare data systems. It recommends a Plan-Do-Check-Act (PDCA) model to manage the information security of a system. The NHS Code of Practice also recommends that BS 7799 and ISO/IEC 17799:2005 are adopted by all its associated healthcare organisations, which means that evaluations of information security strategies in healthcare data systems in the UK must ensure compliance with these standards.

The main challenge in the evaluation for healthcare, as highlighted by the SLR, is to evaluate systems and security in such a way that will help to determine the overall information security posture of the healthcare organisation, so that it can be compared to that of other similar organisations,. In doing so, healthcare providers can grasp the security levels of their peer organisations in order to facilitate interoperability.

To reiterate, the model suggested by Brooks & Warren (2006) is similar to that of Yoo et al. (2007). Brooks & Warren (2006)'s model suggests a four-step evaluation process, which uses a checklist for data collection purposes, calculates measures in percentages for each control category of the information security strategy, and suggests that the results are projected using a graph.

3.7 Limitations and Lessons Learned from the SLR

A carefully implemented SLR is useful to a research. However, there is a chance that some important studies in other databases may not be found in the data search. There is also the chance that some relevant studies may not yet have been digitised or peer reviewed so that they can be made available on online databases. Therefore, the initial selection of the databases is crucial, as an error here may increase the possibility of overlooking important and highly relevant research. To address this issue, any study which has been missed and is later found must be checked. For example, to locate such papers, one method could be to use the latest review papers in the field that explain the state of the art of key aspects of the discipline.

In evidence-based medicine, a few recommended databases, such as Cochrane Collaboration, are available to support researchers. In software engineering, however, there are no such recommended or mandatory databases. Any online databases containing good evidence on software engineering may be considered mandatory for researchers, and any SLRs for evidence-based software engineering must include such databases.

The choice of search techniques and methods is also very important, and great care and skill is required in their application. Any mistake in the application of search techniques may substantially increase or decrease the number of studies selected, a situation which may be avoided by closely monitoring the results. If too many of the items found are found to be irrelevant, there is a possibility of error in the application of searches. Any changes in the search strings may affect all the results. Therefore, it is important to carefully test and finalise the search strings, and any updates or required changes should be made as soon as possible. Other limitations to the present SLR include the receipt of too many results from the initial searches. Therefore, very careful further selection was required.

3.8 Summary of the Chapter

Information is an important asset for organisations, which needs to be carefully protected. The common goals of information security are availability, confidentiality, integrity, authenticity and the non-repudiation of data, and every organisation using information systems therefore seeks to attain and maintain them. However, the nature or the level or priority of those common goals may vary from organisation to organisation depending upon its operating context and consequent specific information security drivers, such as laws and regulations, business objectives, and threat landscape.

An information security strategy can be chosen/developed based on information security standards such as ISO/IEC 27001 and ISO/IEC 27002. Information security management is a process which facilitates the planning and implementation of information security strategies based on a risk assessment. Information security policies are high level written documents developed to detail the implementation process and information security controls aiming to mitigate the risks associated with certain information assets. An information security policy as an information security control has a major role to play in the overall strategy, and must therefore be developed in line with the business, legal and regulatory requirements of information security of the organisation.

The information security strategy requirements for healthcare data systems have been shown to be different to other sectors. Electronic healthcare records must be protected in a way that addresses their specific security concerns based on legal, statutory, regulatory, contractual, and business requirements, and the expected internal and external threats in order to meet the information security goals of the healthcare data systems which host the records. Consequently, the information security strategies of healthcare data systems must be based on those information security requirements to meet the information security goals of the healthcare organisations. ISO 27799 is a standard offering a range of information security controls for selection and application in healthcare organisations according to their requirements.

The evaluation of information security strategies to identify their stronger and weaker areas, is essential to improving an organisation's information security strategies. An evaluation model should generally project the process of evaluation, that is, four major stages: a pre-evaluation preparation phase; then evaluation; analysis; and reporting. An evaluation activity is expected to be planned before the actual evaluations are performed. Such preparations and planning should include establishing understanding of the information security strategy currently in place, building knowledge of the targets of information security of the organisation, identification of the targets of evaluation, planning appropriate actions, and selecting the corresponding methodologies and tools. Subsequently, evaluations are performed with the help of certain tools and methods such as checklists of the information security controls being applied. Further, an analysis of the evaluation results is required to determine the strengths, weaknesses, opportunities, and threats in order to suggest protection measures to improve the strategy. Finally, reporting is done to communicate the evaluation results to the concerned organisation and to create a reference point for future evaluations.

The purpose of the evaluation of information security strategies in healthcare data systems is to ensure that their information security controls are appropriate, effective and in accordance with the organisation's specific security requirements and policies. The objective of information security in healthcare is to protect electronic healthcare records according to legal requirements such as the Data Protection Act 1998 and the Civil Contingencies Act 2004, as well as meeting patient expectations and other business requirements, in order to ensure the required level of availability and integrity of the data.

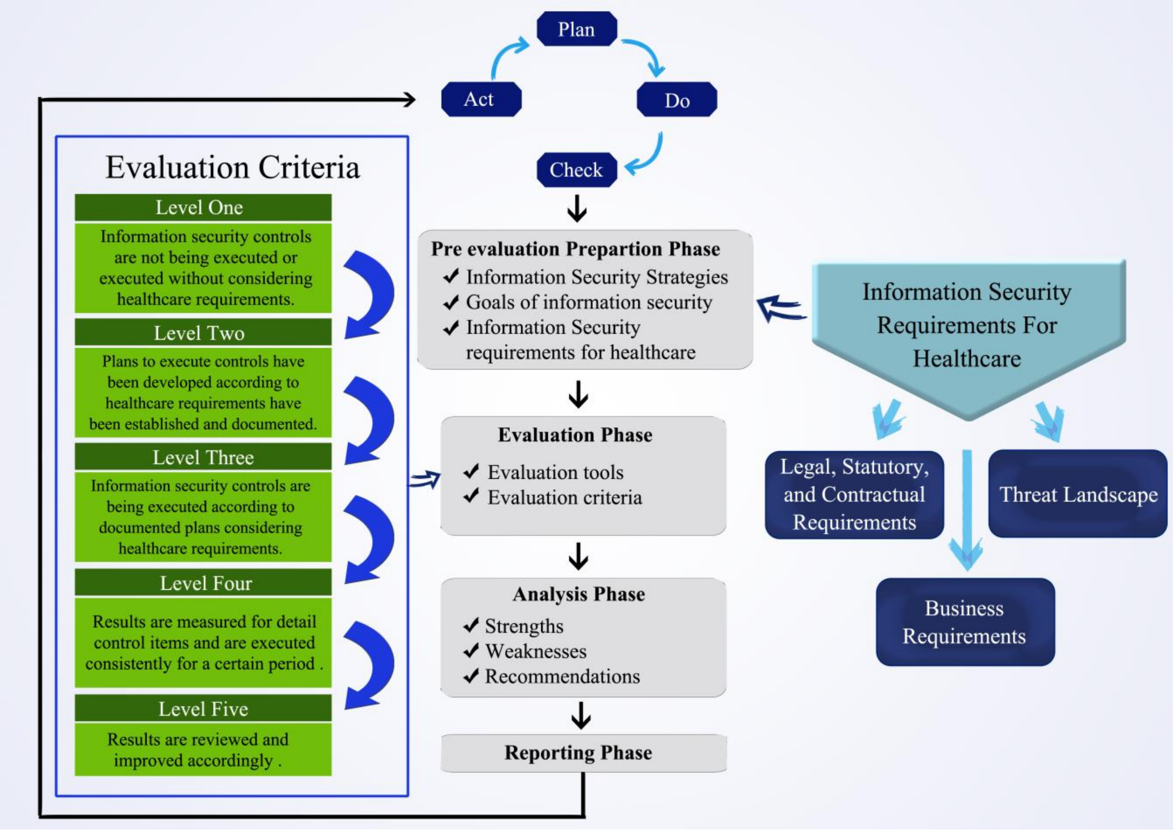
Chapter Four:

An Evaluation Model for Information Security Strategies in Healthcare Data Systems

This chapter presents an evaluation model which can be used to assess information security strategies in healthcare data systems. Section 4.1 presents the newly developed evaluation model. Section 4.2 describes the rationale for the development of an evaluation model designed to evaluate the information security strategies of healthcare data systems. Section 4.3 discusses the four steps of the evaluation process. Sections 4.3.1, 4.3.2, 4.3.3, and 4.3.4 respectively explain the four stages of the evaluation process, namely: the Pre-Evaluation Preparation Phase, the Evaluation Phase, the Analysis Phase, and the Reporting Phase. Section 4.4 gives a summary of the chapter.

4.1 An Evaluation Model for Information Security Strategies in Healthcare Data Systems (EMISHD)

In this research, a model (EMISHD) is developed to evaluate the information security strategies of healthcare data systems that is able to consider the most recent industry information security requirements (Figure 4.5). Plan-Do-Check-Act is a well-known process for the development, implementation and continuous improvement of information security strategies of information security management systems (ISMS). Evaluations of organisations' information security strategies are conducted in the check phase of this cycle. The model offers a four-step evaluation process: a Pre-evaluation Preparation Phase, an Evaluation Phase, an Analysis Phase, and a Reporting Phase. The information security requirements of healthcare data systems are determined in the pre-evaluation preparation phase, and are applied and tested in the evaluation phase. The model also uses a 5-level evaluation criteria based on the Information Security Capability Maturity Model in order to identify and assess information security at multiple levels, and to evaluate information security controls according to the most recent healthcare information security requirements.



Plan
Act
Do
Check
Evaluation Criteria
Level One
Information security controls are not being executed or executed without considering healthcare requirements.
Level Two
Plans to execute controls have been developed according to healthcare requirements have been established and documented.
Level Three
Information security controls are being executed according to documented plans considering healthcare requirements.
Level Four
Results are measured for detail control items and are executed consistently for a certain period .
Level Five
Results are reviewed and improved accordingly .
Pre evaluation Prepartion Phase
✓ Information Security Strategies
✓ Goals of information security
✓ Information Security requirements for healthcare
Evaluation Phase
✓ Evaluation tools
✓ Evaluation criteria
Analysis Phase
✓ Strengths
✓ Weaknesses
✓ Recommendations
Reporting Phase
Information Security Requirements For Healthcare
Legal, Statutory, and Contractual Requirements
Threat Landscape
Business Requirements

Figure 4.1 Proposed Model to Evaluate Information Security Strategies in Healthcare Data Systems (EMISHD).

4.2 Rationale for the Development of an Evaluation Model for Information Security Strategies in Healthcare Data Systems

Information security controls must be identified, implemented and managed according to the specific requirements of the healthcare sector, and they are driven by business needs and other associated requirements to facilitate the intended benefits of electronic healthcare records (Barnard & von Solms 2000; Sunyaev 2011). Controls also need to be evaluated to ensure that they have been implemented in line with industry requirements (Barnard & von Solms 2000).

Healthcare organisations generally develop their information security strategies in line with their business and its related obligatory requirements. Based on such requirements, they select, implement and evaluate their controls from the available international standards for information security. For example, in the UK, the NHS Code of Practice recommends that BS7799 is adopted by healthcare organisations (DH/Digital Information Policy 2007). Barnard & von Solms (2000) note that the audit-oriented evaluation techniques applied by such standards concentrate more on judging whether or not the most appropriate controls were identified and, to a lesser extent, on measuring correct implementation. Barnard & von Solms (2000) argue that the audit-oriented approach can be subjective, because when an auditor has to interpret a situation, they might do so based on their own subconscious bias. Therefore, to deal with such bias, a methodical approach to evaluation which is based on an objective questionnaire to test the information security requirements of healthcare as shown in table 4.1 can help to develop an evaluation model which will enable more reliable evaluations.

4.3 Evaluation process

In addition to defining a clear criteria for evaluation, an evaluation model must feature a process of evaluation which is clear, systematic and comprehensive (Kulmala 2007). Such a process is required to ensure that evaluations are carried out to achieve their intended outcomes. All healthcare organisations in the United Kingdom are recommended to adopt the Plan-Do-Check-Act process to plan, implement, check, and act upon their information security in a continuous manner so that their information security is reviewed and updated on a regular basis. This present research suggests a four-step evaluation process for the "Check" phase. First, a pre-evaluation planning phase is informed by the most up-to-date information security requirements of healthcare organisations. Second, the evaluation is performed using a five-level evaluation criteria in the context of the information security requirements of the healthcare sector. Third, the evaluation results are pulled together to analyse the evaluation data, in order to prepare an evaluation report. Fourth, the findings of the evaluation are documented in the reporting phase so that they can then be implemented in the "Act" phase of the Plan-Do-Check-Act process. These recommended actions are recorded and connected with the plan step so that during the next evaluation planning, the previous evaluation results can be used as reference points.

4.3.1 Pre-evaluation preparation phase

Before the actual evaluation takes place, it is important to know what has to be protected, and how it is currently being protected (Tipton & Krause 2004; Schumacher et al. 2006; Blyth & Kovacich 2006). Information about security drivers, stakeholders, organisation management and resources, along with the standards and controls adopted for information security, is required to build the knowledge base for the evaluation (Atymtayeva et al. 2012). The scope and objectives of the evaluation are also determined during the planning stage.

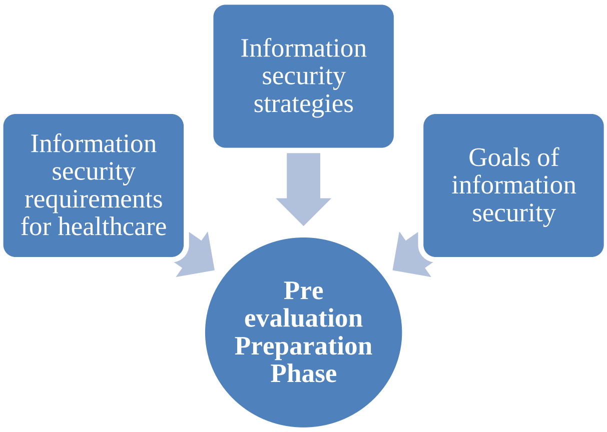

Information security strategies
Information security requirements for healthcare
Goals of information security
Pre evaluation Preparation Phase

Figure 4.2 Pre-Evaluation Preparation Phase

Information security goals such as data availability, integrity, privacy, accountability and non-repudiation are determined by legal requirements, business objectives and the threat landscape faced by healthcare organisations (Siougle & Zorkadis 2002; Gerber & von Solms 2008; Kuang & Ibrahim 2009; Jirasek 2012). For a more detailed discussion of these factors, please refer to the findings for RQ1 in Chapter three.

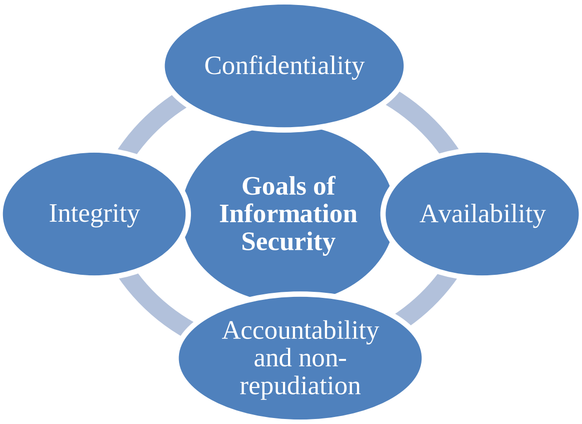
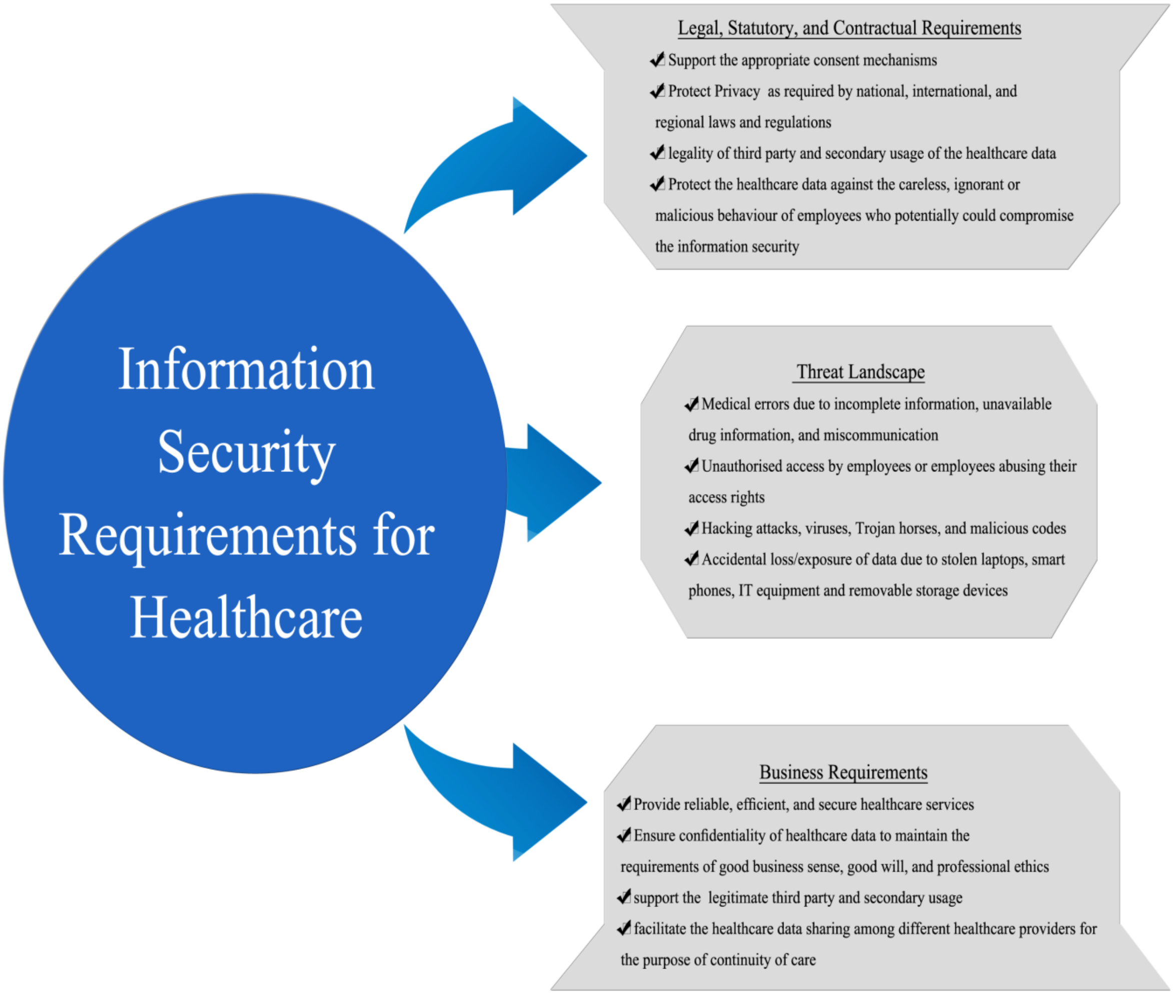

Confidentiality
Integrity
Goals of Information Security
Availability
Accountability and non-repudiation

Figure 4.3 Information Security Goals



Information Security Requirements for Healthcare

Legal, Statutory, and Contractual Requirements

✓ Support the appropriate consent mechanisms

✓ Protect Privacy as required by national, international, and regional laws and regulations

✓ legality of third party and secondary usage of the healthcare data

✓ Protect the healthcare data against the careless, ignorant or malicious behaviour of employees who potentially could compromise the information security

Threat Landscape

✓ Medical errors due to incomplete information, unavailable drug information, and miscommunication

✓ Unauthorised access by employees or employees abusing their access rights

✓ Hacking attacks, viruses, Trojan horses, and malicious codes

✓ Accidental loss/exposure of data due to stolen laptops, smart phones, IT equipment and removable storage devices

Business Requirements

✓ Provide reliable, efficient, and secure healthcare services

✓ Ensure confidentiality of healthcare data to maintain the requirements of good business sense, good will, and professional ethics

✓ support the legitimate third party and secondary usage

✓ facilitate the healthcare data sharing among different healthcare providers for the purpose of continuity of care

Figure 4.4 The Information Security Requirements of Healthcare

4.3.1.1 Information Security Strategies of Healthcare

Healthcare organisations develop their information security strategies in order to identify, select, implement and evaluate appropriate security controls from the recommended standards, such as BS ISO/ IEC 17799; 2005 and BS 7799 - 1; 2005, as recommended in the UK by the NHS Code of Practice (2007). All security controls which are selected and implemented must reflect the overall information security strategy of the healthcare organisation in question.

The objective of evaluating a healthcare organisation’s information security strategy is to ensure that it has been developed and implemented in line with the requirements of the healthcare sector (Linden et al. 2009; Shoniregun et al. 2010; Sunyaev 2011). Audit-oriented evaluation is a commonly applied approach to judge whether or not the security controls have been properly identified, selected and applied in relation to the information security requirements (Von-Solms 1996; Barnard & von Solms 2000; Häyrinen et al. 2008). Evaluation models help to evaluate information security strategies in a systematic way so that the evaluation results can be generated in a meaningful manner, and can facilitate management and security professionals to identify and improve problematic areas of their strategy (Tipton & Krause 2004; Yoo et al. 2007; Park et al. 2010; Sunyaev 2011; Kumar & Puri 2012). Since the requirements of information security in healthcare continually change with the introduction of new laws and technology, and the new threats which regularly arise, an evaluation model which is able to measure the effectiveness of strategies according to the up-to date requirements of the industry will facilitate more effective evaluations (Sunyaev 2011; Aldajani 2012; Tyson & Slocum 2012; Mohapatra & Singh 2012).

4.3.2 Evaluation phase

Audit checklists based on the information security standards applied in healthcare can be used as evaluation tools with which to evaluate the security controls which have been selected and implemented by the healthcare organisation (Thigarajan 2006). It is suggested that the detailed control items which were selected and applied by an organisation should be checked against evaluation criteria to establish whether or not they are addressing all the organisation's most recent security requirements.

4.3.2.1 Questionnaire to Test the Healthcare Requirements of Information Security

Based on the SLR findings (RQ3) of the present study, a ten-item questionnaire is proposed to assess the capability of information security controls to meet healthcare specific information security requirements. As the process shown in Figure 4.2, shows, these questions require 'yes', 'no', or 'not applicable' answers. A control assessed as having one or more 'no' answers would signify that the control is currently unable to meet the healthcare requirements of information security. The questions were given in the following format (see Table 4.1).

Is the information security control being evaluated able to:

No	Questionnaire to test Healthcare Specific Information Security Requirements	Yes	No	Not Applicable
1	Comply with the legal requirements of healthcare data systems?			
2	Support the appropriate consent mechanisms, if informed consent is required by the applicable laws or by the healthcare organisation?			
3	Ensure the confidentiality of healthcare data to meet the requirements of good business sense, goodwill, professional ethics, and laws/regulations?			
4	Protect the healthcare data against the careless, ignorant or malicious behaviour of employees who could potentially compromise information security?			
5	Check for the accidental loss/exposure of data due to stolen laptops, desktops, smart phones, IT equipment and removable/mobile storage devices?			
6	Check for illegitimate third party and secondary usage of the healthcare data in line with the legal and business requirements of healthcare data systems?			
7	Check for hacking attacks, viruses, and malicious codes?			
8	Ensure the availability of healthcare data in order to protect patients' safety, and consumer and public interest, while limiting the access to healthcare data for confidentiality reasons?			
9	Facilitate healthcare data sharing among different healthcare providers for the purpose of continuity of care?			
10	Check for medical errors due to incomplete information, unavailable drug information, and/or miscommunication because of poor handwriting or writing errors?			

Table 4.1 Questionnaire to Test Healthcare Specific Information Security Requirements

4.3.2.2 Evaluation Criteria

An evaluation model based on criteria which consider the most recent requirements of healthcare information security can also contribute to finding solutions to any identified problems. Different criteria are available for evaluation purposes. For example, evaluations based on national or international standards are generally conducted to measure the functionality of controls (Barnard & von Solms 2000). Solms & Von (1998) suggest that when the objective of an evaluation is to determine the level of information security for an entire system, that system must be evaluated in such a way that results are presented at more than one level, so that managers can understand precisely where the security of their organisation stands. The criteria for evaluation should also be precise and simple so that it is convenient to perform, and produces findings which are easy to understand (Tipton & Krause 2004; Blyth & Kovacich 2006; Sajko et al. 2010).

In order to contribute towards objective evaluations of information security strategies, the evaluation criteria must be clearly defined. Barnard & von Solms (2000) argue that at least four aspects of controls should be evaluated: first, functionality should be measured to establish whether or not the proposed controls are actually present in the information security environment. Second, assurance of correctness should be sought; that is, it should be established that the controls have been correctly installed, and are fully operational. Third, assurance of effectiveness confirms that the proposed and installed controls are adequate for the security requirements, as determined by the security policy. Finally, assurance of operation evaluates the operational procedures to confirm that the installed controls are being correctly followed (Barnard & von Solms 2000).

Brooks & Warren (2006) suggest a set of evaluation criteria which compares between the ideal level of security (which the authors regard as ‘100 percent secure’) and the actual level of security in the area. Similarly, one such criteria based on the Information Security Capability Maturity Model has also been presented by Yoo et al. (2007) in developing a methodology which assesses the information protection level, which can be used to measure an information security strategy at five levels to determine its level of security. If a control item is marked at level five, this means that the controls have been applied, implemented and reviewed according to the requirements of the recommended standard (Barnard & von Solms 2000). A control may be executed according to a documented plan and be monitored and reviewed for improvement over time, thus addressing industry requirements. For example, a healthcare provider which has applied controls for training according to specified procedures, schedules, and budget, and planned for them to be monitored and reviewed for improvement according to information security requirements, can be marked at level five.

Thus, a set of evaluation criteria which is clearly defined can evaluate an information security strategy at multiple levels and ensure its functionality, effectiveness, correctness and intended operation according to specific healthcare information security requirements. Consequently, the following five level Information Security Capability Maturity Model criteria is suggested for use in the evaluation model proposed in this study:

Level 1: Information security controls are not being executed, or are executed without considering healthcare requirements

This level is marked when the evaluator finds that a control has been selected but has not been implemented at all, or has been applied without specific plans, and without considering the specific requirements of healthcare information security, thus showing the weakness of the control in its ability to perform its required functions.

Level 2: Plans to execute controls which have been developed according to healthcare requirements have been established and documented

This level is obviously higher than level one, and is marked if specific plans based on healthcare information security requirements, detailed procedures, schedules and budget have been put in place to apply the detailed control items. However, this level indicates that the organisation has not properly followed the documented plans.

Level 3: Information security controls are being executed according to documented plans considering healthcare requirements

This level is marked if detailed control items have been implemented according to their documented plans and healthcare requirements.

Level 4: Results are measured for detailed control items and are executed consistently for a certain period

After implementation of controls according to devised plans, it is important to apply them consistently for a set period, and to record their performance for monitoring purposes. Level 4 is marked if the organisation is carrying out such an activity.

Level 5: Results are reviewed and improved accordingly

Level 5 is marked if the organisation regularly reviews the monitoring results for the sake of improvement.

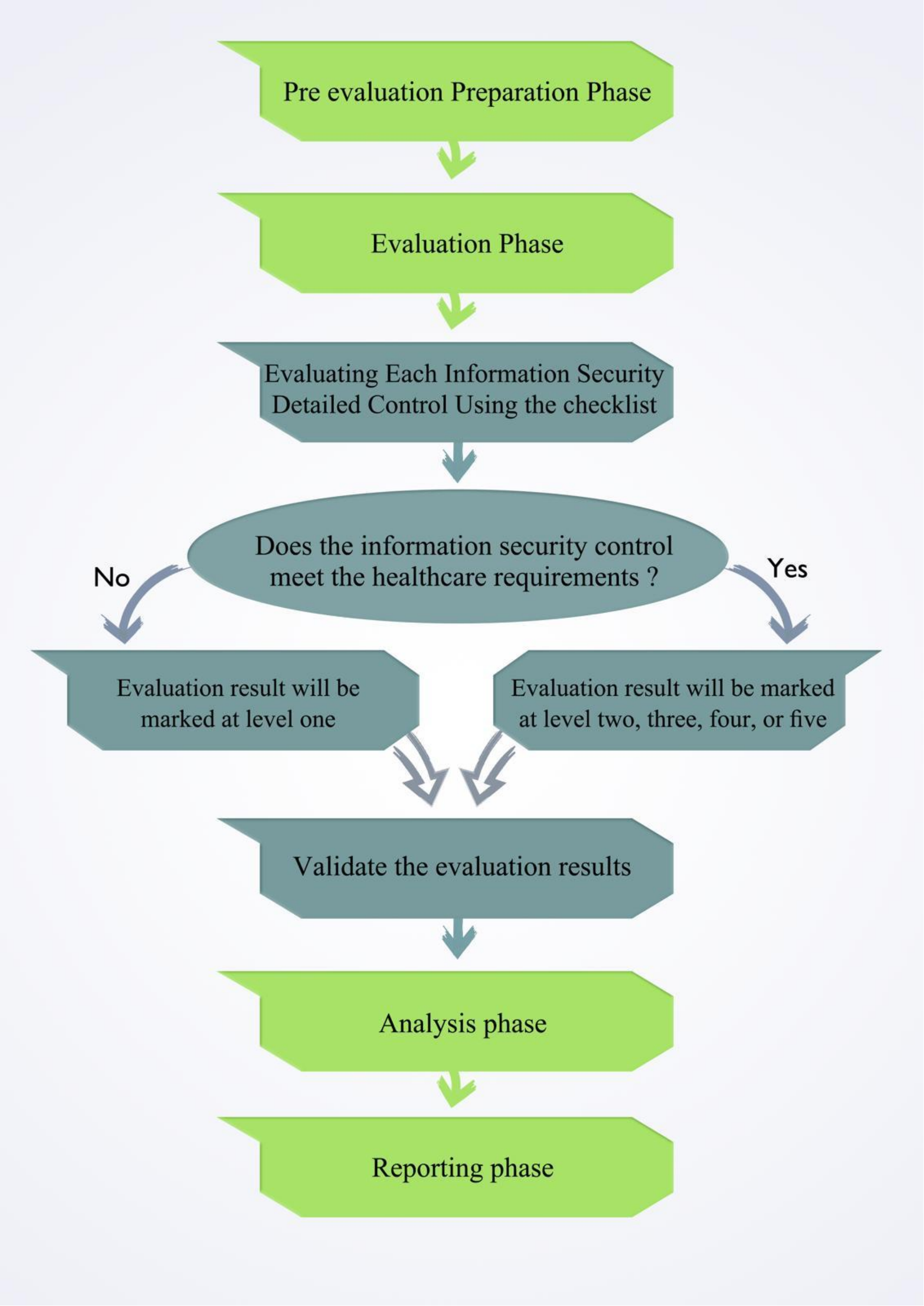
4.3.3 Analysis phase

Depending upon the criteria used in the evaluation, the results can be analysed in different ways. The purpose is to pull the results together and process them in such a way that the weaker and stronger areas of the strategy can be identified, and also that practical recommendations on how to overcome the weaknesses can be suggested. Drawing upon the structure proposed by Yoo et al. (2007), it is recommended that the security level of an organisation's strategy can be determined at the level of detailed control items and control categories. First, all the detailed control items relating to information security are evaluated on the basis of the five level criteria mentioned above in the 'evaluation phase' of the process. Second, to determine the security level of the security control category**,** the average of all the detailed control items relating to information security within a control category is determined to reflect the overall information security level of that control category.

Drawing upon the prior studies found in the literature (Brooks & Warren 2006; Yoo et al. 2007), the level of security is determined and the weaker areas are established via a spider graph, histogram or table, having used the five level criteria for evaluation, as mentioned above. Microsoft Excel or similar software could be used to process the data to generate the targeted tables and graphs.

4.3.4 Reporting phase

The results are reported using graphs, and an evaluation report is written in order to explain the strengths and weaknesses of the information security strategy. The report should also recommend the necessary corrective measures, and it should serve as a reference point for future evaluations.


Pre evaluation Preparation Phase
Evaluation Phase
Evaluating Each Information Security Detailed Control Using the checklist
Does the information security control meet the healthcare requirements ?
No
Yes
Evaluation result will be marked at level one
Evaluation result will be marked at level two, three, four, or five
Validate the evaluation results
Analysis phase
Reporting phase

.

Figure 4.5 Evaluation process

4.4 Summary of the Chapter

In summary, a new evaluation model to evaluate the information security strategy of healthcare data systems has been developed and presented here, which fits the Plan-Do-Check-Act process of ISMS, considers the specific and up-to-date requirements of information security for healthcare data systems, and uses a five level evaluation criteria based on the Information Security Capability Maturity Model. This model is expected to highlight the weaknesses and stronger areas of the strategy more effectively as per the requirements of the healthcare sector.

Chapter Five:

Applying the Evaluation Model to Healthcare Data Systems - A Case Study

This chapter briefly explains the purpose of the case study in section 5.1. The application of the evaluation model is detailed in section 5.2, before section 5.3 describes the non-participant observation of information security practices in the case study. Section 5.4 provides a comparison between the evaluation results and the observation findings. Finally, section 5.5 gives a summary of the chapter.

5.1 Case Study

A case study of a hospital in Saudi Arabia was conducted in this research for two purposes: First, to apply the evaluation model to a real-life case, and second, to perform a non-participant observation to cross-check the evaluation results derived through the evaluation model.

5.2 Application of the Evaluation Model

5.2.1 Pre-evaluation preparation phase

The evaluation process starts with pre-evaluation preparation phase. Therefore, in order to understand the specific information security strategy, information security goals and information security requirements of the case study hospital in Saudi Arabia, the necessary documentation regarding information security policies, information security guidelines, and the website of the hospital were accessed. In line with the findings of the SLR for the present study (see the findings for RQ1, RQ2, and RQ3), the main information security goals were stated as availability, confidentiality, integrity, authentication, and non-repudiation. These goals aimed to meet the hospital's legal requirements, achieve their business objectives, and to understand and respond effectively to their threat landscape (for more detailed discussions, see the findings for RQ1 in Chapter three). Close study of the aforementioned documents revealed the following information, broken down into the next few sub-sections.

5.2.1.1 Background to the use of information technology and information security in Saudi healthcare

The Health Information National Centre was established in 2013 with the objective of governing the use of electronic medical information in public and private sector hospitals, including hospitals used for teaching, in Saudi Arabia. The centre also in future intends to connect its electronic health information network with those of the Saudi Arabian Ministry of Health, the medical services of military agencies, university hospitals, and other related government agencies.

The Health Information National Centre has numerous functions and responsibilities, which can be summarised as follows:

1. It works as a communication hub for providing, sharing, and regulating electronic health information among healthcare providers and other relevant sectors;

2. It identifies the health information which must be provided by different parties related to healthcare services;

3. It establishes the necessary rules and mechanisms for information sharing, and facilitates the interlinking of the related parties;

4. It standardises phrases, names, definitions, and collection practices across all healthcare information systems in Saudi Arabia;

5. It is responsible for creating a universal health e-folder for each individual patient by integrating the medical records maintained by different health organisations, including public and private healthcare facilities;

6. It works on the implementation and regular upgrading of the international disease coding system in all healthcare facilities in Saudi Arabia;

7. It works on the establishment, development, and management of national health accounts systems;

8. It is responsible for establishing and managing a national network for telemedicine;

9. It prepares and publishes national health statistics, including statistics relating to health services activities;

10. It determines and develops the standards to be used for healthcare information systems and databases, including the maintenance and protection of standards;

11. It disseminates awareness through seminars, conferences, and published research on the importance of information technology in healthcare;

12. It is responsible for regulating the provision of healthcare information to different user groups according to national rules and regulations;

13. It ensures cooperation with institutions and agencies at the national and international level with respect to health information;

14. It creates national records of common diseases and epidemics at the national level in coordination with other related agencies;

15. It provides technical advice and support to healthcare providers to manage their information systems according to their resource availability;

16. It identifies the required information systems and helps organisations to use them more effectively to achieve better utilisation of resources and performance evaluation;

17. It facilitates the use of modern information technology to the benefit of patients, and links it to the national health information system.

5.2.1.2 Legal, statutory, and contractual requirements of Saudi healthcare organisations

The specific information security requirements in areas of privacy, availability, integrity and the accountability of data are partly determined by the particular conditions shaped by existing laws and regulations that govern the acceptable use of information systems in the healthcare data systems of Saudi Arabia.

Information Security Policies and Procedures Development Framework for Government Agencies

The Information Security Policies and Procedures Development Framework for Government Agencies, promulgated in Saudi Arabia 2011, is the official set of guidelines for government institutions in the country, which seeks to develop strategies in such a way that:

"*defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction*".

The Framework recognises that "*A Government Agency is exposed to information security risk if confidentiality, integrity or availability of information handled within its business functions is compromised*".

According to the Framework, the security requirements of each organisation may differ on the basis of various factors, including business functions, internal and external relationships, the confidentiality, integrity or availability requirements of the information handled within the agency or with external entities, the manual and automated mechanisms used to enter, store, process, communicate or destroy this information, as well as other aspects applicable to government agencies in Saudi Arabia, including, most notably, the laws and regulations with which the relevant Saudi Government Agencies are required to be compliant.

Anti-Cyber Crime Law 2007

The Saudi Arabian Cyber Crime Law, which was developed and enforced in 2007, defines cybercrimes and determines the punishments for those crimes in order to enhance information security, the protection of rights pertaining to the legitimate use of computer and information networks, as well as to boost the protection of public interests, morals, and common values, and the national economy (Article 2).

Article 3 of the law recognises the following acts as crimes punishable by imprisonment of up to one year or a fine of up to five hundred thousand riyals[approximately £100,000], or both:

1. Spying on, interception or reception of data transmitted through an information network or a computer without legitimate authorisation;

2. Unlawful access to computers with the intention to threaten or blackmail any person to compel him to take or refrain from taking an action, be it lawful or unlawful;

3. Unlawful access to a web site, or hacking a web site with the intention to change its design, destroy or modify it, or occupy its URL;

4. Invasion of privacy through the misuse of camera-equipped mobile phones and the like;

5. Defamation and infliction of damage upon others through the use of various information technology devices.

According to Article 4 of the law, a person may be imprisoned for up to three years and fined up to two million riyals [approximately £400,000] or may receive both types of punishment if he/ she commits one of the following acts:

1. Acquisition of movable property or bonds for oneself or others or signing such bonds through fraud or the use of a false name or identity;

2. Illegally accessing bank or credit data, or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services offered.

Article 5 of the law determines that if person commits one of the following acts, they could be imprisoned for up to four years or fined up to three million riyals [approximately £ 600,000], or receive both punishments:

1. Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data;

2. Causing the information network to halt or breakdown, or destroying, deleting, leaking or altering existing or stored programs or data;

3. Obstruction of access to, distortion, and causing the breakdown of services by any means.

According to Article 6 of the law, any person committing the following acts is liable to be imprisoned for up to five years or fined up to three million riyals [approximately £ 600,000] or both:

1. Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers.

Article 6, as described above, is applicable to healthcare organisations with regard to protecting the privacy of patients' data.

Law of Practicing Healthcare Professions, 2005

This Saudi law defines a healthcare professional as a person licensed to work in the following roles: physician, dentist, pharmacist, healthcare technician, psychologist, social worker, dietician, public health specialist, midwife, paramedic, speech therapist, audiologist, occupational rehabilitation and therapist, as well as other health-related professions, as agreed upon by the Ministry of Health, the Ministry of the Civil Service and the Saudi Commission for Health Specialties.

Article 5 of the law states that all *"healthcare professionals shall serve the best interest of individuals and society within the framework of respecting human right to life, safety and dignity and shall observe customs and traditions prevailing in the Kingdom, and eschew exploitation".*

Article 21 of the law binds all healthcare professionals to *"maintain the confidentiality of information obtained in the course of his practice and may not disclose it except in the following cases:*

A. If disclosure is for the following purposes:

1. Reporting a case of death resulting from a criminal act or preventing the commission of a crime; in which case, disclosure may only be made to the competent authorities.

2. Reporting communicable or epidemic diseases.

3. A professional's refuting accusations pertaining to his competence or conduct of his profession made by the patient or his family.

B. If the party concerned agrees, in writing, to disclose said information or if such disclosure to the patient's family is beneficial to his treatment.

C. *If so ordered by a judicial authority".*

In the case of a failure to observe the terms outlined in Article 21, as above, a healthcare professional could be fined up to twenty thousand riyals under article 30 of the law.

5.2.1.3 Business requirements

The major business requirements of a hospital are, clearly, to provide reliable, efficient and secure healthcare services to its patients. The Information Technology Department of the case study hospital is claimed to be "the innovative resource that continuously enhances" the quality of services using information and computing in order to meet the professional and academic needs of its staff[1]. The department expresses its dedication to ensure "the integrity of data, improving the delivery of instruction, and fostering a bright technological future" for the hospital. The department further expresses its mission using the following words:

"Our mission is to supply the technology and information services needed to fulfil the requirements of the [hospital] staff and patients, now and in the future… We are dedicated to helping the [hospital] to use these services to fully meet their professional and academic needs"[2].

The important services provided by the IT department of the hospital include providing, maintaining, and supporting hardware and software; maintaining and providing access to mission critical data within a secure environment; and providing documentation, education, and training for the hospital's staff. Integrity, a strong ethical commitment to perform professionally and responsibly, and compassion for all members of the hospital are listed as the key values of the department. The User Support and Operations, being one of the important services rendered by the IT department, include a helpdesk, PC support, PC applications support, email/calendaring/collaboration applications support, computer lab support, anti-virus and PC security, PC peripheral support, systems operations, identity management, multimedia/AV equipment support, technology equipment loaning (in conjunction with room reservations via Central Scheduling), end user technology equipment inventory management, providing assistance for technical training services. Network infrastructure services including enterprise security, network security, server security, the setup, administration and maintenance of systems/servers, the setup, administration

[1] The source for this information is the hospital's website and policy documents which cannot be detailed fully for confidentiality reasons.

[2] Ibid.

and maintenance of network (and related) equipment, wired/wireless network cabling and support, VOIP, and server and network equipment inventory management.

5.2.1.4 Threat landscape

The policy documents at the Information Technology Department of the hospital revealed that the department recognises the following threats, and aims to respond to them in the following ways:

i. *Careless/negligent, ignorant, or malicious behaviour of employees resulting in the accidental exposure/disclosure of healthcare information*. The IT department aims to respond to these particular threats by focusing on the training of employees with regard to phishing and social engineering attacks; mobile device security; the secure use of cloud services; training for senior level officers, i.e. the CEO and senior level executives; improving the assessment criteria in terms of the level of proficiency required to pass the training; incentives to employees for proactivity in protecting sensitive information or reporting potential issues; communicating the consequences of a data breach or a violation of legal or business requirements; making the training more interesting for employees; holding people accountable for negligence or malicious behaviour; appointing a senior leader whose sole responsibility is information security.

ii. *Lost or stolen information devices, laptops or other removable and mobile media used by the employees of the organisation.* The IT department aims to respond to these threats by focusing on the following areas: the encryption of data/devices; employee training; enhanced physical security to avoid the theft of data devices; improved equipment custody protocols; the retraining of employees on privacy and data security; the installation of software such as remote-wipe on portable devices; reconsidering "bring your own device" policies and mobile workers; keeping a policy in place for handling of professional devices; full disk encryption; encrypted cloud and removable media protected by strong passwords; handing over procedures when an employee leaves a job; and improvements in encryption, remote wiping, and data tracking.

iii. *Third party users such as other organisation or individuals providing auxiliary products or services such as pharmacies, insurance companies or teaching hospitals.* The hospital's IT department aims to respond to these threats by knowing where their data sets are, which vendors have access to their data, and what privacy and security measures are in place; improving their vendor management of data privacy and security at the place of their data sets, knowing which vendors have access to the data, and what privacy and security measures are in place to protect it; mapping their vendors; putting one department in charge of vendor management; putting vendor access to data in writing; clearly recording who, how, and why each vendor will access their data; using financial terms to enforce vendor compliance; planning regular data security reviews with their vendors, and reviewing contractual provisions for problematic areas before these ever become serious problems.

iv. *Hackers, viruses, malicious codes.* The IT department aims to respond to these threats by utilising the latest antivirus and firewall technologies, enhancing network security, and identifying the loopholes and weaker links in the information security of the organisation.

v. *Lack of training, inappropriate deployment, and inadequate monitoring*. The IT department aims to respond to these threats via compulsory information security training for all employees; making the training more interesting; improving the qualifying criteria for the trainings introducing incentives for people performing better in the training; hiring and deploying the right people for the right job; and improving the monitoring of employees for their information security practices.

5.2.1.5 Which assets need to be protected?

The healthcare data is most important for the hospital. The hospital primarily aims to protect its healthcare data in order to meet its legal and business requirements.

5.2.1.6 Who is responsible for information security?

The hospital's IT Department is responsible for providing information security for the healthcare data.

5.2.1.7 Scope of the evaluation

After discussions with IT Department of the Hospital, keeping in view the time constraints of this research and restrictions on access to information at hospital, this case study evaluated the following five areas of information security:

a. Communications and Operations Management;

b. Human Resource Security;

c. Asset Management;

d. Compliance;

e. Access Control.

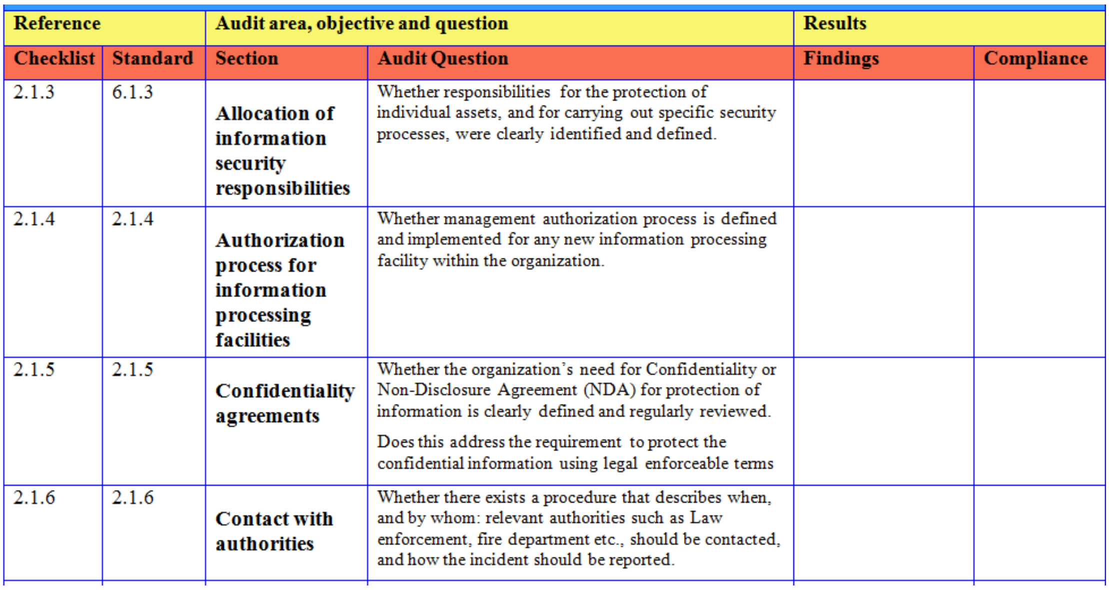
5.2.2 Evaluation phase

5.2.2.1 Evaluation tool

Evaluation must be conducted at the level of the smallest controls selected and applied by the hospital. Therefore, a systematic evaluation instrument/tool was required to collect data so that all the controls currently in place could be evaluated for their effectiveness. A checklist was adopted in line with prior research which covered all the information security controls applied in the hospital. It had 11 main categories: access control, human resource security, information incident management, security policy, asset management, physical and environmental security, information systems acquisition, development and maintenance, compliance, communication and operations management, the organisation of information security, and business continuity management (Thigarajan 2006). However, due to limitations of time, space, and access to the information, five categories were selected for evaluation in this case study. The main categories were further divided into subcategories. For example, the organisation of information security was divided into two subcategories: internal organisation, and external parties (Thigarajan 2006). The subcategories were further divided into detailed control items. For example, the subcategory of internal organisation contained eight detailed control items including management commitment to information security, contact with authorities, confidentiality agreements, etc. Each detailed control item further consisted of one or more questions describing some specific part thereof. For example, confidentiality agreements were a detailed control item consisting of the following two questions:

Question 1: Is the organisation’s need for a Confidentiality or Non-Disclosure Agreement (NDA) for protection of information clearly defined and regularly reviewed?

Question 2: Does this address the requirement to protect the confidential information using legal enforceable terms?



Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
2.1.3	6.1.3	**Allocation of information security responsibilities**	Whether responsibilities for the protection of individual assets, and for carrying out specific security processes, were clearly identified and defined.		
2.1.4	2.1.4	**Authorization process for information processing facilities**	Whether management authorization process is defined and implemented for any new information processing facility within the organization.		
2.1.5	2.1.5	**Confidentiality agreements**	Whether the organization's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed. Does this address the requirement to protect the confidential information using legal enforceable terms		
2.1.6	2.1.6	**Contact with authorities**	Whether there exists a procedure that describes when, and by whom: relevant authorities such as Law enforcement, fire department etc., should be contacted, and how the incident should be reported.		

Table 5.1 : Part of the Checklist Showing the Detailed Control Items and Security Questions Reflecting the Information Security Strategy. See Appendix-D for the full checklist (Thigarajan 2006).

5.2.2.2 Evaluation criteria

The data was collected and values were assigned according to the five level criteria drawn from the Information Security Capability Maturity Model, and also suggested by Yoo et al. (2007). The questions associated with each detailed control item shown in the checklist were evaluated against the criteria and marked according to their level of existence and application in the hospital. For example, a question marked at level four was assigned the numeric value 4.

It is pertinent to note that while using the evaluation criteria, the information security requirements of healthcare were specifically considered in assessing whether or not a control was meeting all the business and legal requirements of healthcare information security, and was also able to effectively respond to threats to healthcare data. For this purpose, the following 10-question questionnaire was developed on the basis of the findings of the SLR (for reference, please see the findings for RQ3).

5.2.2.3 Questionnaire to test healthcare specific information security requirements

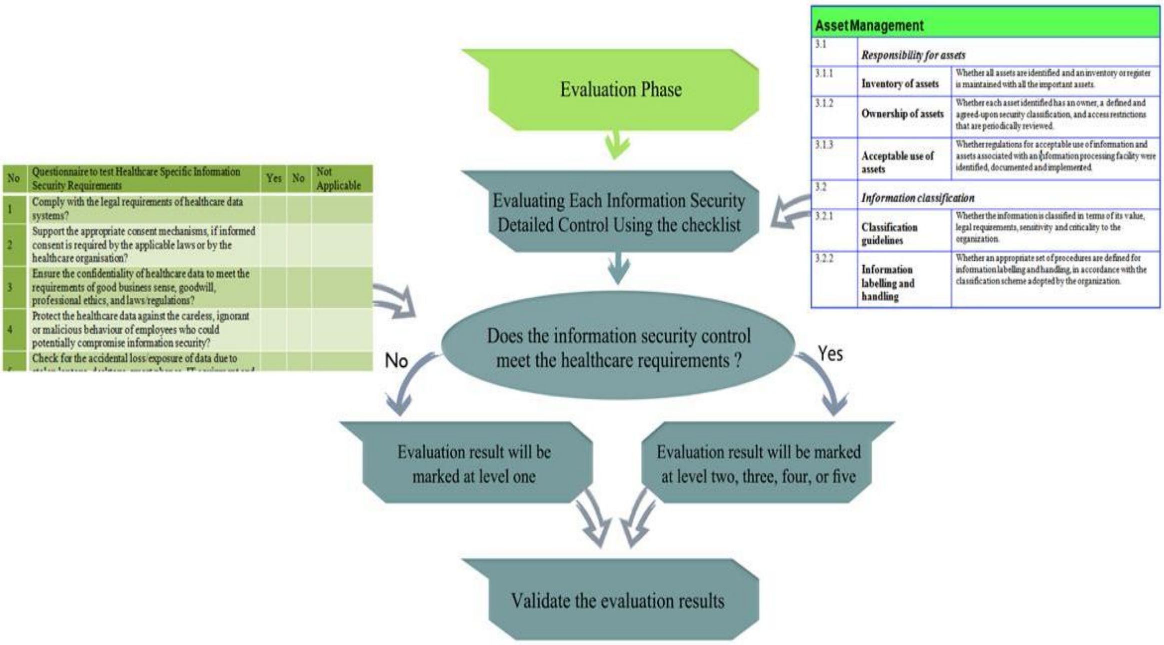
All questions in the following questionnaire need to be answered with Yes, No, or Not Applicable.

Is the information security control being evaluated able to:

No	Questionnaire to test Healthcare Specific Information Security Requirements	Yes	No	Not Applicable
1	Comply with the legal requirements of healthcare data systems?			
2	Support the appropriate consent mechanisms, if informed consent is required by applicable laws or by the healthcare organisation?			
3	Ensure the confidentiality of healthcare data to meet the requirements of good business sense, goodwill, professional ethics, and laws/regulations?			
4	Protect healthcare data against the careless, ignorant or malicious behaviour of employees who could potentially compromise the information security?			
5	Check for the accidental loss/exposure of data due to stolen laptops, desktops, smart phones, IT equipment and removable/mobile storage devices?			
6	Check for illegitimate third party and secondary usage of the healthcare data in line with the legal and business requirements of the healthcare data systems?			
7	Check for hacking attacks, viruses, and malicious codes?			
8	Ensure the availability of healthcare data in order to protect patients’ safety, and consumer and public interest, while limiting access to healthcare data for confidentiality reasons?			
9	Facilitate healthcare data sharing among different healthcare providers for the purpose of continuity of care?			
10	Check for medical errors due to incomplete information, unavailable drug information, and/or miscommunication because of poor handwriting or writing errors?			

Table 5.2 Questionnaire to test Healthcare Specific Information Security Requirements

An information security control cannot meet the healthcare specific requirements unless the answers for all ten questions mentioned above are yes, or/and not applicable.



Evaluation Phase
Evaluating Each Information Security Detailed Control Using the checklist
Does the information security control meet the healthcare requirements ?
No
Yes
Evaluation result will be marked at level one
Evaluation result will be marked at level two, three, four, or five
Validate the evaluation results

No	Questionnaire to test Healthcare Specific Information Security Requirements	Yes	No	Not Applicable
1	Comply with the legal requirements of healthcare data systems?			
2	Support the appropriate consent mechanisms, if informed consent is required by the applicable laws or by the healthcare organisation?			
3	Ensure the confidentiality of healthcare data to meet the requirements of good business sense, goodwill, professional ethics, and laws/regulations?			
4	Protect the healthcare data against the careless, ignorant or malicious behaviour of employees who could potentially compromise information security?			
	Check for the accidental loss/exposure of data due to			

Asset Management		
3.1	*Responsibility for assets*	
3.1.1	**Inventory of assets**	Whether all assets are identified and an inventory or register is maintained with all the important assets.
3.1.2	**Ownership of assets**	Whether each asset identified has an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.
3.1.3	**Acceptable use of assets**	Whether regulations for acceptable use of information and assets associated with an information processing facility were identified, documented and implemented.
3.2	*Information classification*	
3.2.1	**Classification guidelines**	Whether the information is classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
3.2.2	**Information labelling and handling**	Whether an appropriate set of procedures are defined for information labelling and handling, in accordance with the classification scheme adopted by the organization.

Figure 5.1 Evaluation Process using Audit Check List and a Questionnaire to Evaluate Information Security Strategies of Healthcare Data Systems

5.2.2.4 Five level information security capability maturity evaluation criteria

After applying the healthcare information security requirements test outlined above, the following evaluation criteria were applied to assess the level of maturity of the information security control being evaluated.

Level One: Information Security Controls are not being executed, or are being executed without considering healthcare requirements

In instances where the detailed control item being evaluated is not being executed at all, or are being executed without any particular plan or consideration of the healthcare requirements, it is assigned the numeric value 1. For example, if the organisation lacks any confidentiality agreements with its clients or employees as required by the information security strategy, it is considered to be at the minimum level.

Level Two: Plans to execute controls have been developed according to healthcare requirements, established and documented.

If plans for the execution of a detailed control have been established and documented in an organisation, the numeric value 2 is assigned. For example, if the hospital has prepared and documented the procedures, schedules, and budget for confidentiality agreements, it can be marked at level two.

Level Three: Information security controls are being executed according to documented plans having considered healthcare requirements

At the next step up, if the healthcare provider follows the approved plan and applies the control in accordance to it, the control item is assigned the numeric value 3. For example, if confidentiality agreements are executed according to an approved plan, it should be marked at level three.

Level Four: Results are measured for detailed control items and are executed consistently for a certain period

This level requires the hospital not only to apply the control according to an approved plan, but also to execute it consistently for a certain period of time, and to measure the results of the control in order to ascertain whether or not it is serving the required purpose. For example, if the hospital has confidentiality agreements in place which are consistently applied in accordance with approved plans for a period of up to one year, and the hospital also measures if the confidentiality agreements have been serving the required purposes, this control item can be marked at level four.

Level Five: Results are reviewed and improvements made accordingly

The highest level of the criteria reflects the scenario in which the hospital applies a planned control consistently and evaluates whether or not it is serving the required purpose, resulting in identifying any adjustments required to improve its effectiveness. For example, if the hospital reviews the evaluations of confidentiality agreements and makes any required adjustments in the light of the evaluation results, it can be marked at level five.

5.2.3 Analysis phase

Once data is collected it requires processing so that meaningful results can be produced. For this purpose, the data collected through the checklist, and marked against the suggested criteria mentioned above, was processed using Microsoft Excel. The objective of processing the data was to attain an information security score for each detailed control, control subcategory, and control category, based on the values assigned to each question on information security at the hospital. The replies were received for all the security questions and assigned values during the data collection process (see Column E of Table 5.3, below). In order to calculate the evaluation score of a control category, the average of all the evaluation scores within that category was taken, and is given at the bottom of Table 5.3.

A	B	C	D	E
Control category	Control subcategory	Detailed control item	Serial number	Evaluation Result
Asset Management	Responsibility for assets	Inventory of assets	1.1	5
		Ownership of assets	1.2	5
		Acceptable use of assets	1.3	3
	Information classification	Classification guidelines	1.4	4
		Information labelling and handling	1.5	3
Average evaluation score for the control category				4.00

Table 5.3 Data processing to calculate average score of control category

5.2.4 Reporting phase

After calculating the average security score for the control categories, spider graphs were produced to demonstrate the weaknesses and strengths of the information security strategy of the hospital. Figure 5.2 shows the results of this process. Access Control is the safest area, with a score of 4.48, whereas the weakest region is Communication and Operations Management, which scored 3.94. The ideal level of security is 5. Control categories which are assessed at mark 5 are regarded as mature and containing the most effective controls. However, categories marked at less than 5 represent weaknesses in some of their detailed controls. All five control categories are shown in Table 5.4 in descending order of score.

No	Control Category	Score (Descending)
1	Access Control	4.48
2	Human Resources Security	4.33
3	Compliance	4.10
4	Asset Management	4.00
5	Communication and Operations Management	3.94

Table 5.4 Score of Control Categories in Descending Order

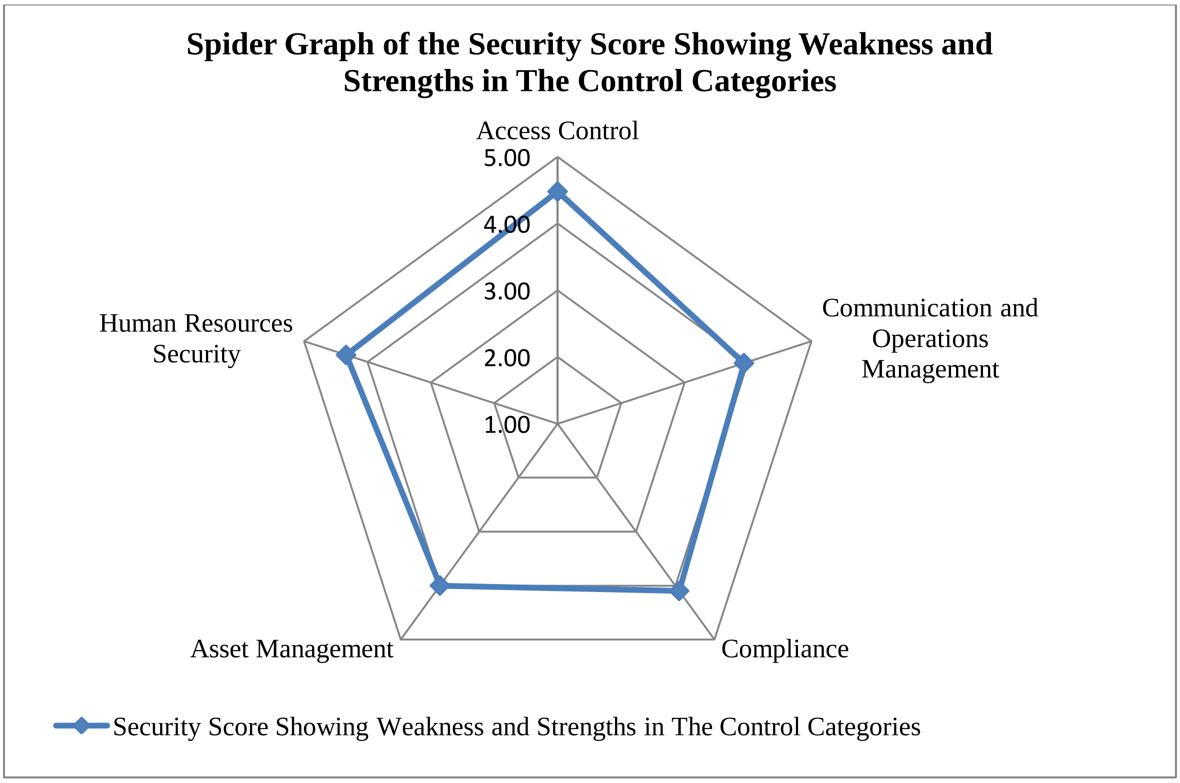


Figure 5.2 Spider Graph to Project Weaker and Stronger Areas of the Strategy at the Level of Control Category

At the next level, a spider graphs for the detailed control items within a control category is used to indicate the weaker controls. For example, nine detailed control items are placed within the control category of Human Resources Security. The description of the nine detailed control items in Figure 5.3 helps to identify the weaker control items. The scores for all nine control items are given in descending order in Table 5.5.

No	Detailed Control Items in Human Resources Security Category	Score (Descending)
1	Roles and responsibilities	5
2	Screening	5
3	Terms and conditions of employment	5
4	Disciplinary process	5
5	Termination responsibilities	5
6	Removal of access rights	4
7	Management responsibilities	4
8	Information security awareness, education and training	3
9	Return of assets	3

Table 5.5 Security Score in Descending Order for All Nine Detailed Control Items

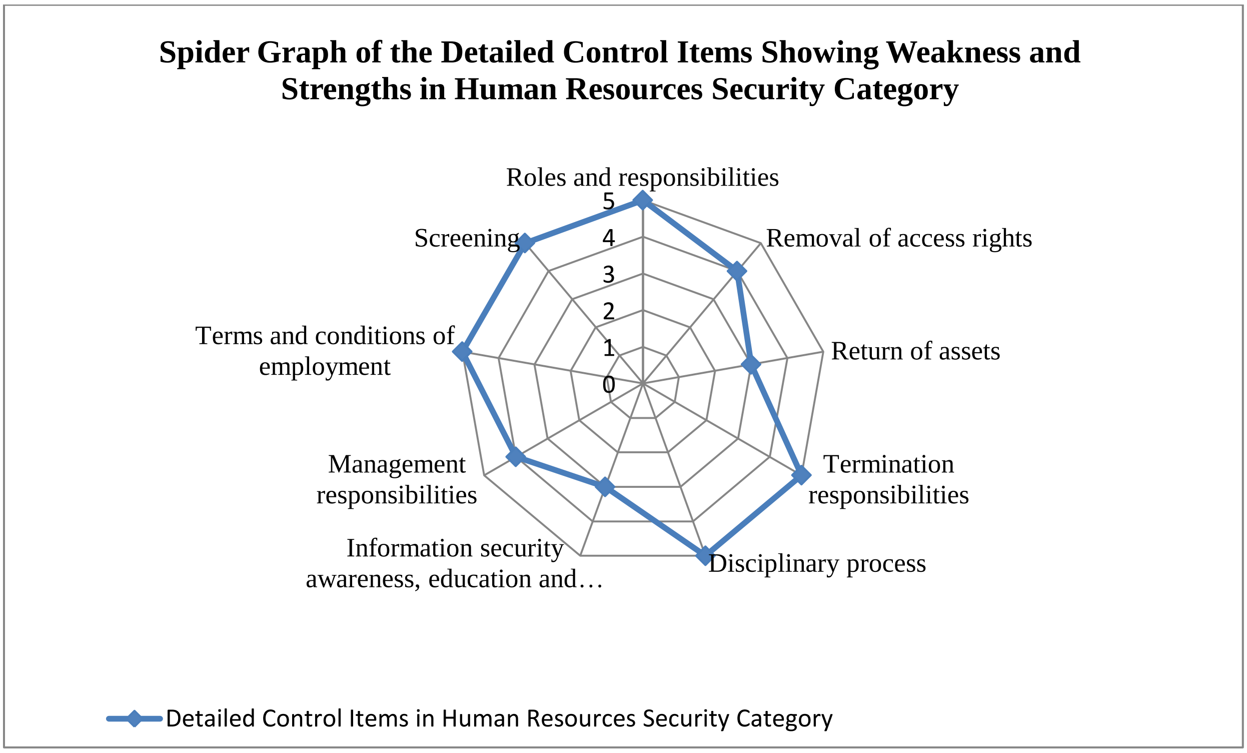


Figure 5.3 Spider Graph of the Detailed Control Items Showing Weakness and Strengths in Human Resources Security Category

5.3 Non-participant Observation of the Information Security Practices of a Hospital in Saudi Arabia

A 15-day observation was performed by the researcher at the OPD (Outdoor Patient Department) of the chosen case study hospital where healthcare professionals see outdoor patients while using the hospital’s information systems between 8 am and 3pm every day from Sunday to Thursday each week. The researcher noted down observations on information technology and security practices in a password protected personal laptop. A member of staff from the IT department was made available to assist in case of any questions or issues regarding the observed practices. The researcher was permitted by the hospital administration to see healthcare professionals entering, accessing, and editing data while performing their tasks.

On the OPD (Out-Patient Department) floor of the hospital where the direct non-participant observation was conducted, 20 specialist doctors, 30 nurses, and 5 support staff were working; the support staff were made up of two receptionists and 3 medical assistants, and 4 Security guards and 10 cleaning staff were also working there. Every day an average of 500 to 600 patients visit OPD.

When a patient arrived in OPD, he/she was directed to the relevant healthcare professional depending upon their appointment. Patients have to register themselves before their first ever appointment in the hospital. During the registration process, their personal details and previous medical history is recorded, and this data is updated every time they see a healthcare professional or receive treatment from the hospital, or undergo any lab tests.

The doctors working at OPD consist of GPs and specialist doctors, who have their clinics in their separate rooms. Every doctor is assisted by at least one nurse. Receptionists are situated close to the entrance of the hospital. Although the OPD clinics and the reception area formed the major site of observation in this research, at least two ethical and professional concerns were identified regarding observing the activities of healthcare professionals. First, some healthcare professionals may not wish to have someone observing their professional day-to-day work. Second, the patients may also object to observation. To resolve these potential issues, only doctors/clinics which were less sensitive with regard to privacy and confidentiality were considered for observation. For example, for social and legal reasons, gynaecology can be more sensitive than eye or orthopaedic departments. So, permission was requested from doctors of ophthalmology, orthopaedics, and ENT (Ear, Nose and Throat) for observation. In all, 4 out of 8 of those doctors agreed to allow the observation provided that their patients had no objection towards the activity. Each of these doctors was examining 20-28 patients per day. During the 15 days of observation, the researcher was able to observe the practices of healthcare professionals during 45 examination instances.

During the observations, the researcher was seated in a chair placed in one corner of the room and quietly observed the doctor and the nurses using their computers while performing their duties. The researcher took notes on his personal computer and discussed any queries with the doctors at the end of the day. No data relating to patients or their treatments were accessed or recorded by the researcher. The researcher focused on the way the healthcare professionals were using their IT equipment.

The observation practice was intended to record answers to the questions listed in Table 5.6 which was developed on the basis of findings of the RQ3 of the SLR helping to understand goals and nature of information security of healthcare data (table 3.5) and information security requirements of the same (table 3.6).

No	Questions	Notes/Remarks
1	How do healthcare professionals log in?	
2	How do healthcare professionals record data?	
3	How do healthcare professionals log off?	
4	Do they make any copies of the records?	

5	Do they use their personal devices to use healthcare records?	
6	Do they use portable or removable media to copy or use healthcare records?	
7	Do they ask someone else to record the data?	
8	Do they complete the healthcare records in a timely manner?	
9	Do they use paper-based records sometimes?	
10	Do they show any special commitment to the information security of the healthcare records? Or do they think that imparting health services is a more important job?	
11	Are they comfortable with using information technology and the available devices?	
12	Are IT devices and healthcare records facilitating the job of the healthcare professionals?	
13	Are the healthcare records available all the time without any delays or interruptions?	
14	What are the chances of data being stolen from their clinic?	
15	What are the chances of data being stolen or lost while they are on the move?	
16	What are the chances of data being stolen or lost while they are at home?	
17	What are the chances that healthcare professionals may maliciously compromise the information security in seeking some undue benefits?	
18	Are they using encrypted and password protected personal devices which may keep the data safe?	

Table 5.6 Observation Dimension

5.4 Comparing the Evaluation Results with the Observation Findings

The non-participant observation at the hospital, as stated above, disclosed some of practices at the hospital which could potentially threaten the information security of its healthcare data systems. The comparison of these practices with the evaluation results obtained through the application of the evaluation model developed in this study confirmed that the information security at the hospital has clear goals, and an understanding of the healthcare requirements at play. However, since the evaluation of the information security controls applied at the hospital is not a regular practice, several practices need to be checked with regard to whether they meet the information security requirements of healthcare data.

5.4.1 Communications and operations management

Segregation of duties is done to ensure that duties and areas of responsibility are separated to reduce the opportunities for the unauthorised modification or misuse of information or services. However, during the observation activity, it was noticed that doctors sometimes considered data entry to be boring and time-wasting, and that they therefore preferred to have another member of staff enter the data for them, e.g. an assistant or nurse. Although the information security policy segregates the duties of the healthcare officials, this control needs to be reviewed in terms of its implementation. Likewise, "monitoring system use" is performed to find out whether or not procedures have been developed and enforced to monitor system usage, the results of monitoring are reviewed regularly, and the level of monitoring required is determined through a risk assessment. However, the non-participant observation at the hospital revealed that healthcare professionals sometimes neglect to log off from their systems while going away for short periods, thus opening up a system vulnerability by which the information security of the healthcare data systems might be compromised.

Information handling procedures are developed and applied to ensure that a procedure is in place for handling information storage, in order to address issues such as information protection from unauthorised disclosure or misuse. It was observed during the non-participant observation at the hospital that not all records are transferred straight away into EHRs. Sometimes, staff maintain paper records and neglect to transfer the information to EHRs in a timely manner. Thus, the completeness of the EHRs can sometimes be compromised in addition to putting the confidentiality of the patients’ data at risk. Similarly, the electronic messaging control is intended to ensure that all information content of emails is well protected. It was observed that all staff have an official email account on the hospital system, and that the information contained in patients’ EHRs can be sent as attachments via email. The system does not have the capability to check attachments and email, which leaves another way open to breach the information security of EHRs.

Audit logging is done to maintain audit logs which record user activities, exceptions, and information security events, to assist in future investigations and access control monitoring. It was, however, observed that the hospital lacks mechanisms by which to certify the integrity of its data. The hospital believes its data to be secure as it is not linked to the internet or any external parties, and 24 hours after entering the data, no changes can be made to the information. However, the integrity of the data could still be checked and certified at regular intervals to ensure that the quality of the data matches healthcare requirements because someone could temper with it in the initial 24 hours.

Controls against malicious code are used to develop and implement user awareness procedures to detect, prevent, and recover from malicious code. The hospital believes that there is no way that external hackers can access the information system as the data systems are not connected with any external party through the internet. However, a program called *Teamviewer* is sometimes used to allow software maintenance vendors access to the system. During the temporary access granted through this maintenance program, the data systems are connected to the internet, a situation which constitutes a possible threat to information security. Likewise, Hospital also allows its staff to use email which means that external hackers may access the data systems. Therefore, information security staff must be conscious of that, and may wish to amend the strategy to mitigate these risks.

The backup of information and software is taken and tested regularly in line with the hospital's backup policy. This control is also responsible for ensuring that all essential information and software can be recovered following a disaster or media failure. However, it was observed in the hospital that although a backup of data is made every twenty-four hours, this backup is located on the same premises as the system itself. Therefore, in the case of any natural disaster such as a fire, earthquake, or flood, there is a possibility that the backup and the originally-stored data might be affected at the same time, somewhat defeating the purpose of making regular back-ups.

No	Detailed control items	Evaluation Results	Observation of practices related to security controls
1	Segregation of duties	3	Another member of staff enters the data on behalf of the authorised healthcare professional.
2	Monitoring system use	3	Healthcare professionals sometimes neglect to log off from their systems while going away for short periods.
3	Information handling procedures	3	Sometimes, staff maintain paper records and neglect to transfer such information to EHRs.
4	Electronic Messaging	3	The information in health records can be sent as attachments via email
5	Audit logging	3	The hospital lacks mechanisms to certify the integrity of data. Within 24 hours, if anyone makes changes, the record system cannot keep a record of the person making those changes.
6	Controls against malicious code	3	A program called Teamviewer is sometimes used to allow access to the system for software maintenance vendors. During the temporary access granted through the maintenance program the data systems are connected to the internet, a possible threat to information security.
7	Information backup	3	The backup is located on the same premises as the system

Table 5.7 Practices of the Case Study Hospital related to Communications and Operations Management

5.4.2 Compliance

Data protection and measures to ensure the privacy of personal information are meant to protect the privacy of health data in line with the relevant legislation, regulations and, if applicable, as per contractual clauses. The hospital’s position is that the data contained in EHRs is owned by the hospital and for that reason, it is not deleted or amended if a patient wishes to opt out or request amendments to their data. This information is not included in the consent/confidentiality agreements of the hospital. Some experts in the field (Mohammad 2010; Shoniregun et al. 2010; Sunyaev 2011; Aldajani 2012) believe that data is actually owned by patients, and that healthcare providers are simply entrusted to manage that data on behalf of their patients. Therefore, the hospital should either grant the right to opt out of the EHR system or offer to make changes to EHRs on request, or patients should at least be informed about this before they agree to enter and store their details in the hospital’s EHRs. Moreover, patients are not informed about what will happen to their data, in terms of how, why and where it might be used.

Health insurance companies require authorisation from their clients to access their medical information, for which the insurance company has paid. In practice, the observation found that hospital staff do not ask to see this authorisation or any evidence to prove that such authorisation has been granted to the insurance company, a failure which might be said to breach the privacy of patients. An authorisation process to grant access to third parties such as health insurance companies should therefore be implemented.

Compliance with security policies and standards requires managers to ensure that all security procedures within their area of responsibility are carried out correctly to ensure that all security policies and standards are being followed. It was observed that the policy, procedures, and guidelines in the hospital are generally circulated in Arabic, which international staff may find difficult to understand.

No	Detailed control items	Evaluation Results	Observation of Practices related to security controls
1	Data protection and the privacy of personal information	3	Data is not deleted or amended if a patient wishes to opt out or request amendments to their data. Patients are not informed what will happen to their data, in terms of how, why and where it might be used. Health insurance companies require authorisation from their clients to access their medical information, for which the insurance company has paid. In practice, the hospital staff do not ask to see this authorisation or any evidence to prove that such authorisation has been granted to the insurance company, a failure which might breach patients' privacy.
2	Compliance with security policies and standards	3	The policy, procedures, and guidelines are generally circulated in Arabic, which international staff may find it difficult to understand

Table 5.8 Compliance Practices in the Case Study Hospital

5.4.3 Human resources security

The process of a return of assets is developed and implemented to ensure that all employees, contractors, and third party users surrender all of the organisation's assets in their possession upon the termination of their employment, contract, or agreement. It is also the case that when doctors or other staff leave a job and join another healthcare provider, they can make copies of records to take with them. This should be prevented, as it might compromise patient confidentiality.

Information security awareness, education and training is a very important control as it can be used to establish whether or not all employees in the organisation are receiving appropriate security-related training, and regular updates on organisational policies and procedures to perform their essential job functions. However, the observation found that employees are trained when beginning their jobs or when new features of the software are to be used, but no periodic and regular training sessions are scheduled to keep them up-to-date on changing requirements in the healthcare sector.

No	Detailed control items	Evaluation Results	Observation of Practices related to security controls
1	Return of assets	3	Staff leaving a job and joining another healthcare provider can make copies of records and take those with them
2	Information security awareness, education and training	3	No periodic and regular training sessions are scheduled to keep staff up-to-date about changing requirements in the healthcare sector.

Table 5.9 Human Resources Security Practices in the Case Study Hospital

5.4.4 Asset management

Information labelling and handling is carried out to set appropriate procedures by which to label and handle data in line with the classification scheme adopted by the healthcare provider. The information stored in the EHRs of the hospital is classified as medical, personal, and financial, and is considered important to its operational needs. Medical data can be accessed by all doctors and other staff employees without any restriction, but some patients may not like their data to be accessible at any time by anyone working at the hospital. For example, a patient may wish to keep their medical information hidden from a particular doctor or nurse. Moreover, patients are not informed about what will happen to their data, in terms of how, why and where it might be used. Therefore, the relevant security controls need to be amended to meet the privacy and confidentiality requirements of healthcare.

Furthermore, the staff of the hospital, including doctors, nurses, assistants, receptionists, and management, are all able to access the personal information of patients, a practice that might be seen as contravening privacy requirements. However, the confidentiality agreements or consent forms given to patients do not inform the patients exactly who might access their personal information. Therefore, the hospital management could prefer to decide that in future, access to personal information should be partly or completely restricted, or that access may be granted only after the completion of an authorisation process. If the hospital is convinced that access to personal information is required by most of its staff, patients should be informed of this through confidentiality agreements or consent forms. Protecting the confidentiality of patients is a legal requirement for all healthcare organisations.

The acceptable use of assets is defined as regulating, identifying, documenting, and implementing the acceptable use of information and assets associated with an information processing facility. The data retention policy of the case study hospital in this research states that patient data is to be retained for a maximum of five years, and that every five years the data will be disposed of, along with backups. However, the observation disclosed that the hospital had not, in fact, deleted this data even after five years had elapsed, as they still considered it necessary for treatment purposes.

No	Detailed control items	Evaluation Results	Observation of Practices related to security controls
1	Information labelling and handling	3	The staff of the hospital, including doctors, nurses, assistants, receptionists, and management, are all able to access the personal information of patients, a practice that might be contrary to privacy requirements. Medical data can be accessed by all doctors and other staff members without restriction. Some patients may object to their data being accessed at any time by anyone working at the hospital.
2	Acceptable use of assets	3	Patients' data is retained for longer than the agreed time period, that is, beyond five years after collection.

Table 5.10 The Case Study Hospital's Asset Management Practices

5.4.5 Access Control

Password use is one of the important controls in the access control area of information security, and the security practices must be clearly articulated when put in place to guide users in selecting and maintaining secure passwords. However, the case study observation found no specific rules or guidelines in the hospital requiring staff to change their passwords regularly.

No	Detailed control items	Evaluation Results	Observation of Practices related to security controls
1	Password use	3	There are no specific rules or guidelines in the hospital requiring staff to change passwords regularly

Table 5.11 Case Study Hospital Access Control Practice

The controls mentioned above in Tables 5.7 to 5.11 are being implemented according to a plan and in consideration of the relevant healthcare requirements. However, the controls are not being reviewed and updated regularly, so some of the issues remain unresolved. The hospital needs to review and update their controls in these area to meet the healthcare information security requirements.

5.5 Summary of the Chapter

A case study of a hospital in Saudi Arabia was conducted to apply the evaluation model to a real life case and to perform non-participant observation to cross-check the evaluation results derived through the evaluation model. In order to understand the information security strategy, information security goals and information security requirements of the hospital in Saudi Arabia, the necessary documents, such as its information security policies, information security guidelines, and website, were accessed. The legal, statutory, and contractual requirements of Saudi Healthcare Organisations include: the Information Security Policies and Procedures Development Framework for Government Agencies; the Anti-Cyber Crime Law, 2007; and the Law of Practicing Healthcare Professions, 2005. Likewise, the business requirements of the hospital are to provide reliable, efficient and secure healthcare services to its patients. Further, its threat landscape is based on various factors, including: careless/negligent, ignorant, or malicious behaviour by employees resulting in the accidental exposure or disclosure of healthcare information; lost or stolen information devices, laptops or other removable and mobile media used by the employees of the organisation; third-party users such as other organisations or individuals providing auxiliary products or services such as pharmacies, insurance companies or teaching hospitals; hackers, viruses, and malicious codes; and a lack of staff training, inappropriate deployment, and inadequate monitoring.

Given the research constraints of limited time and access to information, this study performed an evaluation of five areas of information security at the hospital: Communications and Operations Management; Human Resource Security; Asset Management; Compliance; and Access Control. In the evaluation phase, based on the SLR findings, a questionnaire comprised of ten items was used to test healthcare specific information security requirements against the information security controls being evaluated. Further, all information security controls were assessed using a five-level set of evaluation criteria.

Non-participant observation at the hospital disclosed a few practices at the hospital which could potentially threaten the information security of its healthcare data systems. Comparison of these practices with the evaluation results obtained through the application of the evaluation model developed in the present study confirmed that information security at the hospital has clear goals which take into account healthcare requirements. However, some of the practices of the healthcare professionals were found to be contrary to the information security requirements of healthcare data systems. The evaluation results were updated accordingly.

Chapter Six:

Conclusion

This chapter draws together the findings of the present research. Section 6.1 gives an overview of the research. Section 6.2 summarises the research findings regarding the information security strategies in healthcare data systems and the evaluation models used in relation to those information security strategies. Section 6.3 provides some suggestions for future research.

6.1 Research Overview

This research was carried out in order to develop an evaluation model capable of more effectively highlighting the weaknesses of the information security strategies in healthcare data systems. The specific information security requirements in healthcare may differ from those of other sectors depending on the exact business requirements of privacy, availability, and integrity of data, and the threats posed to the systems, and may also vary with emergence of new threats, the introduction of new laws, and new innovations in technology.

One reason for information security strategies failing to restrict information security breaches in healthcare is that they have been evaluated with evaluation models which have not considered the most recent information security requirements of the sector. The existing evaluation models, though they can evaluate strategic weaknesses on the basis of threats common to different sectors, have no ability to consider the most recent specific requirements of healthcare emerging from the legal and professional requirements relating to privacy protection, patient consent for accessing medical and personal data, medical professional liability, managed care, and dealing with emergency situations. Thus, it was identified that an evaluation model for healthcare data systems was required to highlight weaknesses based on the distinctive current requirements of the sector. Consequently, this research has not only attempted to identify the information security requirements of healthcare data systems, but has also developed a new, more focused evaluation model which can highlight strategic weaknesses according to the most recent specific information security requirements of healthcare data systems.

The methodology used for this research included the deployment of a systematic literature review (SLR) and a case study. The SLR was used to analyse information security strategies and the existing evaluation models for healthcare in order to develop the required evaluation model. A case study then evaluated the information security strategy of a hospital in Saudi Arabia using the newly developed evaluation model. The evaluation results were compared with the findings of the non-participant observation of the practices of healthcare professionals at the hospital.

6.2 Research Findings

6.2.1 Information security strategy for healthcare data systems

Privacy, availability, integrity and non-repudiation are the basic goals of information security common to all organisations. However, the nature and priority of these goals may vary depending on the legal and business requirements and the existing threat landscape of the sector. Information security is provided by an organisation’s management through developing and applying strategies based on the information security requirements for its healthcare data systems. The purpose of information security is to protect the interests of the stakeholders of the healthcare data systems.

In order to meet their information security requirements, organisations develop and execute plans to apply technical and non-technical resources. Such a plan is known as an information security strategy. In healthcare, these strategies have some distinctive requirements that distinguish them from the equivalents in other sectors. Though privacy, availability, and the integrity of information are key areas of information security in the healthcare environment just like in any other sector, the level and nature of the goals in those areas is determined by the organisation's business requirements in terms of carrying out required work without unnecessary hindrance and trusting the quality of the data. A high level of privacy is also required in healthcare regarding patients' medical and personal information, due to patients' expectations and to meet the legal requirement for confidentiality.

Information security strategies in healthcare must also be developed to meet the expectations of diverse groups stakeholders other than patients, such as healthcare professionals, researchers, public authorities, and third parties like insurance companies, and software engineers. Other factors that might shape the requirements of the strategy are the availability of physical infrastructure, the contents and characteristics of the information to be secured, the required compliance in relation to standards, laws, and regulations, the organisational structure for the sharing of information and service provision, the level of information sharing, and the methods available for authentication and authorisation to grant access to permitted users.

While developing information security strategies for healthcare data systems, some aspects have to be given priority and must therefore be given special consideration. Those priorities include implementing data accreditation and encryption services to ensure the integrity of data in order to provide quality services and maintenance plans to deal with possible breakdowns and interruptions in service delivery; having training plans to equip staff to use the technology effectively while observing all information security requirements; determining and facilitating appropriate access rights for different roles in the organisation; developing appropriate consent models to meet legal and ethical requirements; determining minimum infrastructure requirements, adopting the recommended standards to ensure data sharing compatibility; facilitating data system audits, and ensuring stakeholder engagement.

6.2.2 Evaluation model for information security strategies in healthcare data systems

Information security strategies are developed to achieve the information security objectives of an organisation. They may need to be evaluated to highlight any weaknesses in order to develop them to meet the specific information security requirements. The evaluation process generally involves four stages: pre-evaluation preparation; evaluation; analysis; and reporting.

6.2.3 Evaluation model developed by this study

Information security is also required in the healthcare sector to ensure the required level of availability and integrity of information while also protecting the privacy of patients' data according to the expectations of stakeholders, while abiding by national and international laws. Therefore, healthcare data system strategies need to be evaluated in such a way that their weaknesses are highlighted while keeping in view the specific requirements of information security in healthcare, so that the strategies can be improved according to the most recent requirements of the sector.

Evaluation models can facilitate healthcare organisations to achieve this goal by determining the specific requirements of information security of the sector. However, the existing evaluation approaches utilise audit checklists based on the information security standards in order to evaluate the security controls selected and implemented by the healthcare providers. But existing approaches lack a criteria to determine effectively if a security control meets the specific requirements of information security in healthcare sector. This thesis has contributed into existing knowledge by devising such an evaluation criteria by developing a questionnaire to test healthcare specific information security requirements (table 4.1) which can help the evaluators to judge if a security control meets the information security requirements of healthcare sector. Thus, the existing approaches which currently use the audit checklists to merely see if a control is selected or implemented can be made more meaningful and useful by evaluating the controls according to specific information security requirements.

In order to validate the newly developed evaluation model, an evaluation of the information security strategy in a selected hospital in Saudi Arabia was carried out in the form of a case study. Firstly, the evaluation was done using the evaluation model. Secondly, a non-participant direct observation method was utilised to observe the information security practices of the healthcare professionals in order to finalise the evaluation results.

6.3 Future Research

This research has identified other research dimensions that could not be included in the current research due to its scope and limitations. The requirements of information security in other sectors such as banking, retail, and education, could also be examined in order to devise similar sector-specific evaluation criteria for each of those sectors. Similarly, this research was specifically focused on the information security strategy and its evaluation of the healthcare data systems. Future research may compare the information security strategies and evaluation practices of various sectors to highlight their similarities and differences.

Systematic Literature Review (SLR) is a useful and interesting methodology to pursue an evidence based research. This can be used by future researchers to understand certain phenomenon of interests in the field of information technology and information security and contribute into existing field of knowledge.

References

Abraham, C., Nishihara, E. & Akiyama, M., 2011. Transforming healthcare with information technology in Japan: A review of policy, people, and progress. *International Journal of Medical Informatics*, 80(3), pp.157–170. Available at: http://dx.doi.org/10.1016/j.ijmedinf.2011.01.002.

Afanasyev, M. et al., 2011. Privacy-preserving network forensics. *Communications of the ACM*, 54(5), pp.78–87.

Aldajani, M., 2012. *Electronic Patient Record Security Policy in Saudi Arabia National Health Services*. De Montfort University. Available at: http://hdl.handle.net/2086/6016.

Anderson, J.G., 2000. Security of the distributed electronic patient record: A case-based approach to identifying policy issues. *International Journal of Medical Informatics*, 60(2), pp.111–118. Available at: http://ac.els-cdn.com/S1386505600001106/1-s2.0-S1386505600001106-main.pdf?_tid=a5d594c2-fa65-11e4-9362-00000aacb35e&acdnat=1431627701_6a586b83c4e3360a6b894f23792f7fc4.

Andress, A., 2003. *Surviving Security: How to Integrate People, Process, and Technology* 2nd Editio., Auerbach Publications.

Anthes, G., 2010. Security in the cloud. *Communications of the ACM*, 53(11), pp.16–18.

Appari, A. & Johnson, E.M., 2008. Information Security and Privacy in Healthcare : Current State of Research., pp.1–39.

Atymtayeva, L.B. et al., 2012. Methodology and ontology of expert system for information security audit. In *Soft Computing and Intelligent Systems (SCIS) and 13th International Symposium on Advanced Intelligent Systems (ISIS)*. Japan: IEEE, pp.

238–243.

Bakker, A., 1998. Security in perspective; luxury or must? *International Journal of Medical Informatics*, 49(1), pp.31–37.

Barnard, L. & von Solms, R., 2000. A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Computers & Security*, 19(2), pp.185–194.

Biskup, J., 2009. *Security in Computing Systems*, Available at: http://www.amazon.co.uk/Security-Computing-Systems-Challenges-Approaches/dp/3540784411.

Blyth, A. & Kovacich, G., 2006. *Information Assurance* 2nd ed., London: Springer-Verlag London. Available at: http://www.springer.com/gb/book/9781846282669.

Booker, R., 2006. Re-engineering enterprise security. *Computers and Security*, 25(1), pp.13–17. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404805002051 [Accessed June 22, 2014].

Bottino, L.J., 2006. Security measures in a secure computer communications architecture. In *2006 ieee/aiaa 25TH Digital Avionics Systems Conference*. IEEE, pp. 1–18.

Brenner, J.F., 2010. Why isn't cyberspace more secure? *Communications of the ACM*, 53(11), p.33.

Brooks, W. & Warren, M., 2006. A methodology of health information security evaluation. *HIC 2006 and HINZ 2006*, 10(3), p.464. Available at: http://hcro.enigma.co.nz/website/results/20060926165844738025788.pdf%5Cnhttp://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed7&NEWS=N&AN=2

006474025.

Burke, G.I. & Jarratt, D.G., 2004. The influence of information and advice on competitive strategy definition in small- and medium-sized enterprises. *Qualitative Market Research: An International Journal*, 7(2), pp.126–138.

Calder, A., 2013. *ISO27001/ISO27002 A Pocket Guide* Second., Cambridgeshire: IT Governance.

Ceusters, W. & Smith, B., 2006. Strategies for referent tracking in electronic health records. *Journal of Biomedical Informatics*, 39(3), pp.362–378.

Chandler, A.D., 1962. *Strategy and Structure: Chapters in the History of the American Industrial Enterprise*, MIT Press.

Chi, H., Jones, E.L. & Zhao, L., 2008. Implementation of a security access control model for inter-organizational healthcare information systems. In *Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008*. Ieee, pp. 692–696. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4780754 [Accessed June 22, 2014].

Clarke, J. & Meiris, D., 2006. Electronic Personal Health Records Come of Age. *American Journal of Medical Quality*, 21(3), p.5S–5S.

Commonwealth of Australia, 2009. *Cyber Security Strategy*,

Data Protection Audit Manual, 2001. Data Protection Audit Manual., (June).

DH/Digital Information Policy, 2007. *Information Security Management: NHS Code of Practice*, Available at: http://svn.tools.ietf.org/html/rfc1158%5Cnhttp://www.connectingforhealth.nhs.uk/sys temsandservices/infogov/codes/securitycode.pdf.

Dogaheh, M.A., 2010. Introducing a framework for security measurements. In *Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010*. pp. 638–641.

Doherty, N.F., Anastasakis, L. & Fulford, H., 2009. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6), pp.449–457.

Dybå, T. & Dingsøyr, T., 2008. Empirical studies of agile software development: A systematic review. *Information and Software Technology*, 50(9–10), pp.833–859.

Ekelhart, A. et al., 2007. Ontological mapping of common criteria's security assurance requirements. In *IFIP International Federation for Information Processing*. Springer US, pp. 85–95.

Eminağaoğlu, M., Uçar, E. & Eren, Ş., 2009. The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*, 14(4), pp.223–229. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1363412710000099 [Accessed June 11, 2014].

Farn, K., Lin, S. & Fung, A.R., 2004. A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6), pp.501–513.

FFIEC, 1998. *A nnual R eport 1998*, Washington, DC.

Fraser, H.S. et al., 2005. Refereed papers Implementing electronic medical record systems in developing countries. *informatics in Primary Care*, 13, pp.83–95.

Fung, a. R.W., Farn, K.J. & Lin, A.C., 2003. Paper: A study on the certification of the information security management systems. *Computer Standards and Interfaces*, 25(5), pp.447–461. Available at: http://linkinghub.elsevier.com/retrieve/pii/S092054890300014X [Accessed June 22, 2014].

GAO, 2006. *NFORMATION SECURITY: Department of Health and Human Services Needs to Fully Implement Its Program*, US. Available at: http://www.gao.gov/products/GAO-06-267.

Gaunt, N., 1998. Installing an appropriate information security policy. *International Journal of Medical Informatics*, 49(1), pp.131–134.

Gerber, M. & von Solms, R., 2008. Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27(5–6), pp.124–135. Available at: http://dx.doi.org/10.1016/j.cose.2008.07.009.

Gerber, M., Von Solms, R. & Overbeek, P., 2001. Formalizing information security requirements. *Information Management & Computer Security*, 9(1), pp.32–37.

Goel, S. et al., 2007. Innovative Model for Information Assurance Curriculum : A Teaching Hospital The University at Albany, State University of New New York State Center for Information Forensics and Assurance. *ACM Journal of Educational Resources in Computing*, 6(3), pp.1–15.

Goel, S. & Chengalur-Smith, I.N., 2010. Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, 19(4), pp.281–295. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0963868710000521 [Accessed June 15, 2014].

Gong, G.Q., Qiang, S. & Wang, J., 2009. Information security measures and regulation research. In *2009 International Conference on Management Science and Engineering - 16th Annual Conference Proceedings, ICMSE 2009*. pp. 2184–2189.

Greenhalgh, T., 2010. *how to READ A PAPER the basics of evidence-basd medicine* Fourth Edi., UK: John Wiley & Sons Ltd. Available at: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:No+Title#0.

Gritzalis, D. & Lambrinoudakis, C., 2000. A data protection scheme for a remote vital signs monitoring healthcare service. *Medical informatics and the Internet in medicine*, 25(3), pp.207–224.

Gupta, M.G.M. et al., 2003. Intrusion countermeasures security model based on prioritization scheme for intranet access security (emerging concepts category). *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.*, pp.174–181. Available at: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=1232418.

Hamill, J.T., Deckro, R.F. & Kloeber, J.M., 2005. Evaluating information assurance strategies. *Decision Support Systems*, 39(3), pp.463–484. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167923604000284 [Accessed June 13, 2014].

Hart, B., 2001. Implementing a Successful Security Assessment Process. *SANS*, pp.1–10.

Hawkey, K. et al., 2008. Human, organizational, and technological factors of IT security. In *Proceedings of ACM CHI 2008 Conference on Human Factors in Computing Systems*. pp. 3639–3644. Available at: http://doi.acm.org/10.1145/1358628.1358905.

Häyrinen, K., Saranto, K. & Nykänen, P., 2008. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*, 77(5), pp.291–304.

Hoffmann, L., 2009. Implementing electronic medical records. *Communications of the ACM*, 52(11), p.18.

Höne, K. & Eloff, J.H.P., 2002. Information security policy — what do international information security standards say? *Computers & Security*, 21(5), pp.402–409.

HSCIC, 2014. *Code of practice on confidential information*, UK.

Humaidi, N. et al., 2011. Investigating the Relationship of Users ' Behavior and Internal Security Threat towards the Implementation of Total Health Information System (THIS) in Malaysian Medical Institutions. *Australian Journal of Basic and Applies Sciences*, 5(9), pp.291–297. Available at: http://connection.ebscohost.com/c/articles/69735084/investigating-relationship-users-behavior-internal-security-threat-towards-implementation-total-health-information-system-this-malaysian-medical-institutions.

ISO/IEC13335-1, 1996. *Information Technology -Guidelines for the Management of IT Security - Part 1: Concepts and Models for IT Security*, Geneva: International Standards Organization.

ISO/IEC17799, 2005. Information technology -- Security techniques -- Code of practice for information security management.

ISO/IEC 21827, B., 2008. Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM).

ISO/IEC 27001:2005, 2005. *Information technology — Security techniques — Information security management systems — Requirements*, ISO/IEC 27001:2013, 2013. *Information technology - Security techniques - Information security management systems - Requirements*,

ISO/IEC 27002:2013, 2013. *Information technology — Security Techniques — Code of practice for information security controls*,

ISO 27799:2008, 2008. *Health informatics — Information security management in health using ISO / IEC 27002*, London: British Standards Institution.

Jafari, S. et al., 2009. An approach for developing comparative security metrics for healthcare organizations. In *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*.

Jirasek, V., 2012. Practical application of information security models. *Information Security Technical Report*, 17(1–2), pp.1–8. Available at: http://dx.doi.org/10.1016/j.istr.2011.12.004.

Kankanhalli, A. et al., 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), pp.139–154. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0268401202001056 [Accessed May 26, 2014].

Kazemi, M., Khajouei, H. & Nasrabadi, H., 2012. Evaluation of information security management system success factors: Case study of Municipal organization. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, 6(14), pp.4982–4989. Available at: http://www.academicjournals.org/ajbm/abstracts/abstracts/abstracts2012/11Apr/Kazemi et al.htm [Accessed June 22, 2014].

Khan, S.U., 2011. *Software outsourcing vendors ' readiness model (SOVRM) Siffat Ullah Khan Doctor of Philosophy in Computer Science*. Keele University.

Kiely, M. et al., 2006. Macro-economic cyber security models. In *Proceedings of the 2006 IEEE Systems and Information Engineering Design Symposium, SIEDS'06*. IEEE, pp. 284–291.

Kitchenham, B., 2004. Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(TR/SE-0401), p.28. Available at: http://csnotes.upm.edu.my/kelasmaya/pgkm20910.nsf/0/715071a8011d4c2f482577a700386d3a/$FILE/10.1.1.122.3308[1].pdf%5Cnhttp://tests-zingarelli.googlecode.com/svn-history/r336/trunk/2-Disciplinas/MetodPesquisa/kitchenham_2004.pdf.

Kitchenham, B. a., Dyba, T. & Jorgensen, M., 2004. Evidence-based software engineering. In *Proceedings. 26th International Conference on Software Engineering*.

Kitchenham, B. & Charters, S., 2007. Guidelines for performing Systematic Literature Reviews in Software Engineering. *Engineering*, 2, p.1051.

Kluge, E.H.W., 2004. Informed consent and the security of the electronic health record (EHR): Some policy considerations. *International Journal of Medical Informatics*, 73(3), pp.229–234.

Knapp, K.J. et al., 2009. Information security policy: An organizational-level process model. *Computers & Security*, 28(7), pp.493–508.

Ko, I.S., Lee, G. & Na, Y.J., 2005. Development of an Intelligent Information Security Evaluation Indices System for an Enterprise Organization. *Springer Berlin Heidelberg*, 3682(2005), pp.1029–1035. Available at: http://link.springer.com/chapter/10.1007%2F11552451_142.

Kotulic, A.G. & Clark, J.G., 2004. Why there aren't more information security research studies. *Information & Management*, 41(5), pp.597–607.

Kuang, T. & Ibrahim, H., 2009. Security privacy access control for policy integration and conflict reconciliation in health care organizations collaborations. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS2009)*. New York: ACM, pp. 750–754. Available at: http://dl.acm.org/citation.cfm?id=1806480&dl=ACM&coll=DL&CFID=512023045&CFTOKEN=82822221.

Kulmala, P., 2007. *Evaluation of information service information security*,

Kumar, S. & Puri, A., 2012. A Framework for Evaluation and Validation of Information Security Policy Er. Satish Kumar Assistant Professor Dept. of Information Technology Mr. Amit Puri Assistant Professor Dept. of Computer Application GIMET, Amritsar. *International Journal of Computer and Distributed System*, 1(3), pp.19–31.

Lampson, B., 2009. Privacy and securityUsable security. *Communications of the ACM*, 52(11), p.25.

Linden, H. van der et al., 2009. Inter-organizational future proof EHR systems. A review of the security and privacy related issues. *International Journal of Medical Informatics*, 78(3), pp.141–160. Available at: http://www.ncbi.nlm.nih.gov/pubmed/18760661 [Accessed June 22, 2014].

Liu, M., Fu, G. & Jing, J., 2011. eHCBAC: Flexible column based access control for electronic healthcare systems. In *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*. Ieee, pp. 745–750. Available at:

http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120890 [Accessed June 22, 2014].

Loef, C., Mankovich, N.J. & Rosner, M., 2002. Standards and security for medical information technology. *MedicaMundi*, 26(2), pp.41–46. Available at: http://www.healthcare.philips.com/pwc_hc/main/about/assets/Docs/medicamundi/mm_vol46_no2/loef.pdf.

Lukasik, S.J., 2011. Protecting users of the cyber commons. *Communications of the ACM*, 54(9), pp.1–8.

McCann, E., 2014. HIPAA data breaches climb 138 percent. *HIMSS*, p.1. Available at: http://www.healthcareitnews.com/news/hipaa-data-breaches-climb-138-percent [Accessed May 10, 2015].

Meingast, M., Roosta, T. & Sastry, S., 2006. Security and privacy issues with health care information technology. In *28th Annual International Conference of the IEEE*. IEEE, pp. 5453–5458.

Mintzberg, H., 1978. Patterns in Strategy Formation. *Management Science,* 24(9), pp.934–948.

Mohammad, Y.M., 2010. *Information scurity strategy in telemedicine and e-Health systems [electronic resource] : A case of England's shared electronic health record system*. Brunel University.

Mohapatra, S. & Singh, R.P., 2012. *Information Strategy Design and Practices*, New York: Springer-Verlag. Available at: http://link.springer.com/10.1007/978-1-4614-2428-4.

NHS, 2010. NHS Summary Care Record - your emergency care record., (September).

Niazi, M., Cox, K.A. & Verner, J.M., 2006. An empirical study identifying high perceived value requirements engineering practices. In *Advances in Information Systems Development: Bridging the Gap Between Academia and Industry*. pp. 731–743.

Niazi, M., Wilson, D. & Zowghi, D., 2005. A framework for assisting the design of effective software process improvement implementation strategies. *Journal of Systems and Software*, 78(2), pp.204–222.

Norman, 2011. *Defense In Depth : A Comprehensive Strategy for Securing Health Care Networks*,

Otieno, G.O. et al., 2008. Measuring effectiveness of electronic medical records systems: Towards building a composite index for benchmarking hospitals. *International Journal of Medical Informatics*, 77(10), pp.657–669.

Papazafeiropoulou, A. & Gandecha, R., 2008. Interpretive flexibility along the innovation decision process of the UK NHS Care Records Service (NCRS): Insights from a local implementation case study. *IGI Global*, pp.2452–2462.

Park, S., Ahmad, A. & Ruighaver, A., 2010. Factors Influencing the Implementation of Information Systems Security Strategies in Organizations. In *Information Science and Applications (ICISA), 2010 International Conference on*. IEEE, p. 6.

Persusco, L., 2006. Using scenario planning in the evaluation of information security applications K. Michael & M. G. Michael, eds. *First Workshop on the Social Implications of National Security (Workshop on the Social Implications of Information Security Mesures on Citizens and Business, 2006)*, pp.105–117. Available at: http://www.secureaustralia.org/.

Pishva, D. et al., 2007. An initiative to improve the state of information security at local governments in Japan. In *Proceedings - International Carnahan Conference on Security Technology*.

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

Reni, G. et al., 2004. Chief medical officer actions on information security in an Italian rehabilitation centre. *International Journal of Medical Informatics*, 73(3), pp.271–279. Available at: http://www.ncbi.nlm.nih.gov/pubmed/15066558 [Accessed June 22, 2014].

Rosenthal, D.S.H., 2010. Keeping bits safe: How Hard Can It Be? *Communications of the ACM*, 53(11), pp.47–55.

Rugg, G. & Petre, M., 2007. *A Gentle Guide to Research Methods*, Open University Press. Available at: http://site.ebrary.com/www/lib/tralee/docDetail.action?docID=10197031.

Safran, C. et al., 2007. Toward a national framework for the secondary use of health data: an American Medical Informatics Association white paper. *Journal of the American Medical Informatics Association*, 14(1), p.1. Available at: http://jamia.bmj.com/content/14/1/1.short.

Sajko, M., Hadjina, N. & Pešut, D., 2010. Multi-criteria model for evaluation of information security risk assessment methods and tools. *MIPRO*, pp.1215–1220. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5533650&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5533650.

Saleh, M.S., Alrabiah, A. & Bakry, S.H., 2007. Using ISO 17799: 2005 information security management: A STOPE view with six sigma approach. *International Journal of Network Management*, 17(1), pp.85–97. Available at: http://onlinelibrary.wiley.com/doi/10.1002/nem.616/abstract.

Saydjari, O.S., 2006. Risk: A good system security measure. In *Proceedings - International Computer Software and Applications Conference*. pp. 37–38.

Schumacher, M. et al., 2006. *Security Patterns: Integrating security and systems engineering*, West Sussex: John Wiley & Sons Ltd. Available at: http://books.google.com/books?hl=en&lr=&id=T57rfpDko0YC&oi=fnd&pg=PR7&dq=Security+Patterns,+Integrating+Security+and+Systems+Engineering&ots=YJc3aw0jbL&sig=BTd_WIPUZ5y1fcGJyWjqk10DIJ0%5Cnhttp://books.google.com/books?hl=en&lr=&id=T57rfpDko0YC&oi=fnd&pg=PR7&.

Sheppard, N.P., Safavi-Naini, R. & Jafari, M., 2009. A Digital Rights Management Model for Healthcare. *2009 IEEE International Symposium on Policies for Distributed Systems and Networks*, pp.106–109. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5197393 [Accessed June 22, 2014].

Shoniregun, C.A., Dube, K. & Mtenzi, F., 2010. *Electronic healthcare information security*, London: Springer Science+Business Media.

Da Silva, F.Q.B. et al., 2011. Six years of systematic literature reviews in software engineering: An updated tertiary study. *Information and Software Technology*, 53(9), pp.899–913. Available at: http://dx.doi.org/10.1016/j.infsof.2011.04.004.

Siougle, E.S. & Zorkadis, V.C., 2002. A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls. *Springer-Version*, 2437, pp.104–114. Available at:

http://link.springer.com/chapter/10.1007%2F3-540-45831-X_8.

Smith, E. & Eloff, J.H., 1999. Security in health-care information systems--current trends. *International journal of medical informatics*, 54(1), pp.39–54.

Speed, T. & Ellis, J., 2003. Chapter 6: Authentication and Authorization. In *Internet Security: A Jumpstart for Systems Administrators and IT Managers*. USA: Digital Press Elsevier Science, p. 398.

Stahl, B., Doherty, N. & Shaw, M., 2012. Information Security Policies In The UK Healthcare Sector: A Critical Evaluation. *Information Systems Journal*, 22(1), pp.77–94. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1365-2575.2011.00378.x/full.

Staples, M. & Niazi, M., 2008. Systematic review of organizational motivations for adopting CMM-based SPI. *Information and Software Technology*, 50(7–8), pp.605–620.

Stewart, R., 2003. *A Case Study of Alberta Wellnet's Treatment of Privacy in Implementing Electronic Health Records*. DALHOUSIE UNIVERSITY.

Sunyaev, A., 2011. *Health-Care Telematics in Germany* 1st ed., Gabler Verlag. Available at: http://www.springerlink.com/index/10.1007/978-3-8349-6519-6.

Takeda, H. et al., 2000. Architecture for networked electronic patient record systems. In *International Journal of Medical Informatics*. pp. 161–167.

Tarwireyi, P., Flowerday, S. & Bayaga, A., 2011. Information security competence test with regards to password management. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*.

The Office of Cyber Security and Information Assurance, Cabinet Office, U.K., 2011. *The*

UK Cyber Security Strategy Protecting and promoting the UK in a digital world, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

Thigarajan, V., 2006. Information Security Management: SANS Audit Check List. *SANS*, pp.1–43. Available at: https://www.sans.org/media/score/checklists/ISO-17799-2005.pdf.

Tipton, H.F. & Krause, M., 2004. *Information Security Management Handbook, Sixth Edition*, Auerbach Publications. Available at: http://www.amazon.com/Information-Security-Management-Handbook-Sixth/dp/1420090925.

Tyson, B.K. & Slocum, R., 2012. Healthcare Information Security. *Journal Of Healthcare Information Management*, 26(4), pp.38–43. Available at: http://www.secureworks.com/assets/pdf-store/articles/JHIM-fall-2012.pdf.

Tzelepi, S., Pangalos, G. & Nikolacopoulou, G., 2002. Security of medical multimedia. *Medical informatics and the Internet in medicine*, 27(3), pp.169–184.

Vladimirov, A., Gavrilenko, K. & Michajlowski, A., 2010. *Assessing Information Security: Strategies, Tactics, Logic and Framework*, United Kingdom: IT Governance.

Von-Solms, R., 1996. Information security management: The second generation. *Computers & Security*, 15(4), pp.281–288.

Von-Solms, R., 1998. Information security management (2): guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*, 6(5), pp.221–223.

Wang, J., Xiao, N. & Rao, H.R., 2012. An exploration of risk information search via a search engine: Queries and clicks in healthcare and information security. *Decision Support Systems*, 52(2), pp.395–405. Available at: http://dx.doi.org/10.1016/j.dss.2011.09.006.

Wiant, T.L., 2005. Information security policy's impact on reporting security incidents. *Computers and Security*, 24(6), pp.448–459. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404805000490 [Accessed June 22, 2014].

Win, K.T. & Fulcher, J. a., 2007. Consent mechanisms for electronic health record systems: A simple yet unresolved issue. *Journal of Medical Systems*, 31(2), pp.91–96. Available at: http://link.springer.com/10.1007/s10916-006-9030-3 [Accessed June 22, 2014].

Wozak, F., Schabetsberger, T. & Ammmenwerth, E., 2007. End-to-end Security in Telemedical Networks - A Practical Guideline. *International Journal of Medical Informatics*, 76(5–6), pp.484–490. Available at: http://www.ncbi.nlm.nih.gov/pubmed/17097916 [Accessed June 22, 2014].

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

Yoo, D. et al., 2007. Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection). *Engineering and Technology*, 36(December), pp.162–166.

Appendix A:

A Systematic Literature Review Protocol for "An evaluation model for information security strategies in healthcare data systems"

Mutiq Almutiq

School of Computing and Mathematics,

Keele University,

Staffordshire, UK

m.m.a.almutiq@epsam.keele.ac.uk

April 2012

1. Change management

Document History	
Version 1.0	First draft of Protocol.
Version 1.1	Proofreading.
Version 1.2	Minor revisions made after expert review of Version 1.1 Protocol
Version 1.3	Final Version of Protocol

2. Background

Information security has an essential role in any organization. In the modern world, information is treated as power. To protect data security, measures taken need to be organized. Dedicated efforts to this end may be carried out by organizations such as banks, supermarkets, and airline companies. Educational institutions and the healthcare industry also have highly sensitive information to protect. Threats to this information can occur in many ways: natural disasters, accidents, or theft can have a significant impact on sensitive information. Software damage from viruses, hackers and intruders are also severe threats to information security.

Due to the expansion of information technology, the healthcare industry has embraced informatics. Healthcare data can influence many areas such as insurance policies, workplace contracts, family relationships, etc. In the hospital setting, information on doctors, medicines, vaccines, hospital locations and prescriptions are all vital. Laboratory activities, patient details, staff data and many other relevant data are now computerised instead of paper-based. As a result, patients can easily and quickly be routed to their doctors. Fast and efficient service is a benefit of engaging with information technology. It is also important to note the savings in cost and time such engagement brings (Buyukozkan et al., 2011).

Healthcare informatics aims to centralise patients' details in order to support the decision-making process with high-quality medical knowledge (Haux, 2002). Previously, patient information was recorded on paper as charts, tables, and files, which were difficult to analyse. Digitising this information has raised the efficiency of health care to a new level. Securing health information relates to patients' privacy as well. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in 1996 have been introduced in order to facilitate these requirements (Murray et al., 2011). As required by HIPAA, organizations are designated to collect information and store it in databases (Murray et al., 2011).

In implementing information security, lack of a policy structure may result in many issues which need to be addressed. Policy can be made in clusters. The security level of a medical institute may differ from department to department. Critical heath data for HIV and cancer patients requires more security than other patients' data. Employees involved in dealing with this information must be educated and have full confidence in their job. Clearly described tasks and responsibilities for staff make for more transparency when working with critical information. It is essential to bring sufficient understanding between third parties and the organization if there is any involvement from them (Janczewski et al., 2002). An information security structure must have data protection resources in use during operation (Grimson, 2001). Also, conducting a risk analysis is essential. Thorough knowledge of the above areas is necessary to design an effective security policy (Vaast, 2007). Further, an information security policy requires focusing management's attention in the proper direction (Knapp et al., 2009).

Once the information security policy has been created it is essential to assess whether the policy is effective or not. Review of an applied policy can help further develop information security systems. The effectiveness of the policy can be addressed from both sides: from the consumer's point of view and from the perspective of management. It can be compared with another policy, especially one from a different country (Abraham et al., 2011). The effectiveness of information security can be reviewed from many different angles. Cost effectiveness, time saving, quality and improved productivity are major components for measuring the usability of any information security policy. Key elements of effective policy are Plan, Do, Check and Act (NHS Code of Practice).

Despite the increase in general research on information security, which covers such areas as service institutions, industry and government, research on information security in the health sector, which is just as significant, is lacking. Nevertheless, it is important to take advantage of previous strategies used to study information security generally and the health sector, which are complementary.

Many computer-based techniques, non-computer-based measures and data access policies exist that aim to enforce data security, such as the Health Insurance Portability and Accountability Act (HIPAA), and Digital Imaging and Communication in Medicine (DICOM). However no integrated model for evaluating the effectiveness of information security measures exists, and the same is true for healthcare systems (Knapp et al., 2009, Abraham et al., 2011, Park et al., 2010 and Mohammad and Stergioulas, 2010). Therefore, this study aims to develop an evaluation model for measuring the effectiveness of information security strategies in healthcare data systems. It starts by analysing the current state of existing healthcare data system strategies, and then uses the results to design an information security strategy that will help the health sector provide better privacy and confidentiality for patients. It finds that a model that appraises the strengths and weaknesses of security strategies in healthcare data systems may benefit the health sector.

3. Research Questions:

There are many of objectives for the application of a systematic literature review in this research. Firstly, the review is used to identify many of the previous studies of information security strategy in health care systems. In addition, it examines the potential application and its benefits through the collection and analysis of evidence from these studies, as well as seeking to provide a picture of the current state of information security strategy in health care systems. Finally, the overall aim of this

SLR is the possibility of measuring the effectiveness of information security strategies in healthcare data systems.

In order to accomplish these objectives, and to ensure the collection of all pertinent data, numerous research questions have been produced. These questions will guarantee a comprehensive study in the research area, at the same time as providing a deep analysis of the past use of information security strategy in healthcare data systems.

The research questions are:

RQ1. What is information security?

RQ2. What is an information security strategy?

RQ3. What is an information security strategy for healthcare data systems?

RQ4. How can the effectiveness of an information security strategy be measured?

RQ5. How can the effectiveness of an information security strategy in healthcare data systems be measured?

4. Search Strategy

4.1 Identifying Search Terms

According to Kitchenham and Charters (2007), the following search strategy is used for the construction of search terms.

a. Use the Research Questions for the derivation of major terms, by identifying population, intervention and outcome;

b. For these major terms, find the alternative spellings and synonyms;

c. Verify the key words in any relevant paper;

d. Use of Boolean Operators for conjunction if the database allows, in such a way as to use the 'OR' operator for the concatenation of alternative spellings and synonyms whereas 'AND' is for the concatenation of major terms.

Results for (a)

The following details assist in designing a search term related to the research questions.

Population: Information security strategy in healthcare data systems

Intervention: Measure the effectiveness of the strategy

Outcomes of relevance: Trust, meeting the information security requirements.

Experimental Design: Theoretical studies, empirical studies, case studies.

Results for (b)

Key word	Alternatives or Synonyms
Information	Data, records
Security	Safety, Protection, Assurance
Strategy	Policy, Approach, Plan, Model, Framework
Healthcare	Patient care, Health, Hospital, Medical, Clinical
Systems	Database, Data Systems
Measure	Evaluate, Assess, Monitor, Appraise, Audit
Effectiveness	Success

Results for (c)

- Information
- Security

- Strategy
- Healthcare
- Systems
- Measure
- Effectiveness

Results for (d)

RQ1 and RQ2: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”)).

RQ3: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Patient care” OR “Healthcare” OR “Hospital” OR “Clinical” OR “Health” OR “Medical”)).

RQ4: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Measure” OR “Evaluate” OR “Assess” OR “Monitor” OR "Appraise" OR "Audit") AND (“Database” OR “Data Systems” OR “Systems” OR “Effectiveness” OR “Success”)).

RQ5: ((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Patient care” OR “Healthcare” OR “Hospital” OR “Clinical” OR “Health” OR “Medical”) AND (“Measure” OR

“Evaluate” OR “Assess” OR “Monitor” OR "Appraise" OR "Audit") AND (Database” OR “Data Systems” OR “Systems” OR “Effectiveness” OR “Success)).

4.2 Resources to be searched:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- Cite Seer Digital Library
- EBSCOhost
- Google Scholar

4.3 Search Documentation

Search results will be documented in the format shown in the following table.

Name of database	Search strategy	Search string no.	Date of search	Years covered by search	Total Results Found	Initial selection	Final selection
Science Direct	((“Information” OR “Data” OR “Records”) AND (“Security” OR “Safety” OR “Protection” OR "Assurance") AND (“Strategy” OR “Policy” OR “Approach” OR “Plan” OR “Model” OR “Framework”) AND (“Patient care” OR “Healthcare” OR “Hospital” OR “Clinical” OR “Health” OR “Medical”) AND (“Measure” OR “Evaluate” OR “Assess” OR “Monitor” OR "Appraise" OR "Audit") AND (Database” OR “Data Systems” OR “Systems” OR “Effectiveness” OR “Success)).	Trial search	30 of March 2012	All years			

5. Selection Criteria

5.1 Inclusion Criteria

In inclusion criteria, a set of literature which will be discovered in the research conducted on papers or articles will be created. This review will be used for data extraction. The criteria are listed below:

- Studies that identify information security in general and health care systems in particular.
- Studies that identify the models which can be used to measure the level of information security in healthcare data systems.
- Studies that identify factors which affect information security in healthcare data systems.
- Studies regarding the constraints and limitations affecting information security strategies in healthcare data systems.
- Studies that identify strategies and guidelines relating to information security in healthcare systems.

5.2 Exclusion Criteria

Exclusion criteria describe which pieces of literature uncovered in the research will be excluded. The criteria are,

- Studies that are not related to the research questions.
- Studies that do not describe information security in general or healthcare data systems in particular.
- Studies that are only related to healthcare without information security.

- Studies where only the abstract but not the full text is available.
- Studies which are not written in English.
- Studies which are not peer reviewed.

5.3 Selection Process

Initial selection will be by reviewing the title, keywords and abstract. In order to exclude the results that no related with research questions.

Final selection will be verified from primary sources selected in the initial selection process according to the criteria for inclusion / exclusion by reviewing carefully the full text of the studies.

5.4 Publication Quality Assessment

The assessment of quality in publications and data extraction will be completed concurrently, and measurement of quality will be achieved after the final selection of publications. The quality checklist comprises the following questions:

1. Is the paper based on research or is it a "lessons learned" report based on expert opinion?
2. Is there a clear statement of the aims of the research?
3. Is there an adequate description of the context in which the research was carried out?
4. Was the research design appropriate to address the aims of the research?
5. Was the recruitment strategy appropriate to the aims of the research?
6. Was there a control group with which to compare treatments?

7. Was the data collected in a way that addressed the research issue?
8. Was the data analysis sufficiently rigorous?
9. Has the relationship between researcher and participants been considered to an adequate degree?
10. Is there a clear statement of findings?
11. Is the study of value for research and practice?

A spreadsheet will be created and each study assigned a value of either 1 (Yes), or 0 (No). The first three of the above criteria will be used to exclude from the review non-research items and studies without clarity of aims. This factor represents the minimum quality threshold.

6 Data Extraction Strategy

6.1 Primary Study Data

The aim of the study is to gather data for review from publications which focus on the given research questions. The following data will be extracted from each publication (Kitchenham and Charters, 2007).

- Publication details (Title, Authors, Journal/Conference title, etc.)
- Data that address the research questions.

The following table presents the data to be captured and the extraction form.

Data to be extracted
✓ Reference ✓ Goals and Requirements of Information Security and Information Security Strategy. ✓ Goals and Requirements for Healthcare Information Security Strategy. ✓ Evaluation Models Used to Assess the Effectiveness of Information Security Strategy. ✓ Evaluation Models Used to Assess the Effectiveness of Information Security Strategies of Healthcare Data Systems.

The review will be carried out by the researcher, who will be responsible for the data extraction. A secondary reviewer will be looked to for guidance in case of any issues arising regarding the data extraction.

6.2 Data Storage

The list of publications found by the search string will be reserved as a Microsoft Word/SPSS document and will be stored on the researcher’s PC and also on the Keele University server.

6.3 Data Synthesis

As there are five research questions, the synthesis will be divided into five divisions. For Research Question 1, the data will be synthesized by creating one summary table with the columns No, Strategies, Frequency, and Percentages. The complete details of every strategy mentioned in the Summary table will be recorded in a separate table which will hold the following columns: Strategy group name, No of references, Strategies subgroups, Paper reference/Paper title. For Research Questions 2, 3, 4 and 5, the same process will be presented as for the RQ1 described above. For details, see the following table.

No	Strategies	Frequency	Percentages
01			
02			
03			
04			

7 Validation of the Review Protocol

A preliminary version protocol will be submitted for comments to Professor Pearl Brereton, Dr. Mahmood Niazi and Dr. Siffat Ullah Khan. The protocol will then be updated and presented (Kitchenham and Charters, 2007).

8 Schedule:

Task	Required Completion Date	Completion Date
Submission of the Protocol for Review	19-Mar-2012	05-Apr-2012
Protocol Construction	26-Mar-2012	09-Apr-2012
Test and finalize search strings	02-Apr-2012	12-Apr-2012
Primary Study Selection	09-Apr-2012	18-Apr-2012
Final Selection	23-Apr-2012	02-May-2012
Data Extraction	14-May-2012	21-May-2012
Analysis	21-May-2012	28-May-2012
Review Report	15-Oct-2012	

9 Divergences

In case of any divergence from the protocol, which may occur during the study, will proof any amend in a new Appendix to this document.

10 References:

R. Haux, "Health care in the information society: what should be the role of medical informatics?," *Methods Inf Med*, vol. 41, PP. 31-35., 2002.

J. Grimson, "Delivering the electronic healthcare records for 21st century," *International Journal of Medical Informatics,* vol. 64, PP. 111-127., 2001.

L. Janczewski and F. Shi, "Development of Information security baselines for healthcare information systems in New Zealand," *Computer & Security*, vol. 21(2), PP. 172-192., 2002.

E. Vaast, "Danger is in the eye of the beholders: social representations of information systems security in healthcare," *Journal of Strategic Information Systems*, vol.16, PP. 130-152., 2007.

K. Knapp, R. Morris, T. Marshall and T. Byrd, "Information security policy: An organizational-level process model," *Computer & Security,* vol. 28, PP. 493-508., 2009.

DH/Digital Information Police. "Information security management: NHS code of practice," *DH Department of Health*, 2007.

C. Abraham, E. Nishihara, and M. Akiyama, "Transforming healthcare with information technology in Japan: A review of policy, people, and progress," *International journal of medical informatics*, vol. 80(3), PP. 157-170., 2011.

B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," *Keele University and Durham University Joint Report*, vol. 2 (EBSE 2007-001), 2007.

G. Buyukozkan, G. Çifçi, and S. Guleryuz, "Strategic analysis of healthcare service quality using fuzzy AHP methodology," *Expert Systems with Applications*, vol. 38 (8), PP. 9407-9424., 2011.

T. Murray, M. Calhoun and N. Philipsen, "Privacy, Confidentiality, HIPAA, and HITECH: Implications for the Health Care Practitioner," *The Journal for Nurse Practitioners*, vol. 7(9), PP. 747-752., 2011.

Y. Mohammad and L. Stergioulas, "Building an information security strategy for EHR: guidelines for assessing the current Situation," *Engineering in Medicine and Biology Society*, vol. 32, PP. 3919-3922., 2010.

S. Park, A. Ahmad and A. Ruighaver, "Factors influencing the Implementation of Information Systems Security Strategies in Organizations," *Information Science and Applications,* PP.1-6., 2010.

Appendix B:

Data Extraction Strategy

01	Data extracted from (Tarwireyi et al. 2011)
Reference	Tarwireyi, P., Flowerday, S. & Bayaga, A., 2011. Information security competence test with regards to password management. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Holistic Approach to Information Security** "An information system is composed of **technology, people, and processes**. It therefore follows that any effort to secure this system should regard all the system components as equally important and should also identify how these components are intertwined. This means that a holistic approach to security, which integrates technology, people, and processes needs to be taken." **Structured Measurement Approach to Monitor Security Practices of Users** "**Security awareness programmes** employ mechanisms that focus on reinforcing good security practices and changing employee security behaviour. However, the implementation of such programmes does not mean that all employees will automatically become security competent… It is therefore necessary to have a way of measuring the extent to which good security practices can be reinforced. With a structured measurement approach, it becomes easy to monitor the security practices of users."
Additional note.	Information security needs a holistic approach to include people, technology, and processes in order to address all dimensions of information security. The authors are of the view that generally technological dimensions of information security are over emphasised whereas the social aspect which is about people related to information systems is generally ignored.
02	**Data extracted from (Goel & Chengalur-Smith 2010)**
Reference	Goel, S. & Chengalur-Smith, I.N., 2010. Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, 19(4), pp.281–295. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0963868710000521 [Accessed June 15, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Security as a Function of the Interaction between *People and Technology*** "Security (or lack thereof) in an organization, is a function of the interaction between people and technology. In order to manage security effectively, both social and technical factors need to be considered concurrently. Security policies integrate these elements into a cohesive plan that organizations use for enforcing security. Security policies are at the core of the security strategy in an organization but little attention has been devoted to understanding them." **Policy and Strategy** "The term security policy is used primarily in two different contexts: (1) computer/network security, and (2) information security management in organizations. Security policy in the context of computer/network security is most commonly used for formally describing access control rules in a computer system/network. Organizational information security policy describes the overall strategy and plan for ensuring

	information security in an organization." **Effectiveness of Strategy Depends upon Breadth, Clarity and Brevity** [as it helps better understanding on the part of concerned people] "Thus, three recurring themes emerge from the literature as vital characteristics of effective policies. The first is the breadth or scope of the coverage of the policy. In addition, the policy must be clear, i.e. written in language that is user friendly, non-technical and easy to understand. Concurrent with that is the necessity that the policy document be short, to the point, and not unnecessarily verbose, otherwise the user will not read it."
Additional note.	Information security involves both people and technology. Information security is applied through development and implementation of strategy. However, this strategy is to be applied by the people interacting with the information systems. Therefore, the strategy to be more effective has to be at higher levels of clarity, brevity, and breadth. So that the strategy is well read, understood, and applied with trust by the people.
03	**Data extracted from (Goel et al. 2007)**
Reference	Goel, S. et al., 2007. Innovative Model for Information Assurance Curriculum : A Teaching Hospital The University at Albany, State University of New New York State Center for Information Forensics and Assurance. *ACM Journal of Educational Resources in Computing*, 6(3), pp.1–15.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Education** "The need for widespread dissemination of information assurance (IA) education is clearly understood, and several researchers have elegantly elucidated these concerns." **Security is a Socio-Technical Problem** "In the past, most efforts to improve security have focused on technological innovations, and substantial improvements have been made with basic security tools such as the use of intrusion detection systems and firewalls. By themselves, such improvements have been inadequate in controlling the worsening security environment. Security is a socio-technical problem that requires active user participation and technology development to control the proliferation of attacks as well as to prevent human errors."
Additional note.	The education of information security at universities need to be improved on the model of "teaching hospitals" in order to enhance the information security skills of the information security students.
04	**Data extracted from (Doherty et al. 2009)**
Reference	Doherty, N.F., Anastasakis, L. & Fulford, H., 2009. The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, 29(6), pp.449–457.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Importance of Information** "Given the growing importance of information, it is often viewed as being analogous to an organisation's '*lifeblood*': should the flow of information become seriously restricted or compromised then the organisation may wither and die." **Increasing Severity of Information Security Breaches Supported by Empirical Evidence** "Although the modern enterprise is increasingly dependent upon high quality information, in practice, information resources are often incomplete or compromised, because of the unacceptably high levels of security breaches experienced. For example, in the UK, it has recently been found that '*the number of security incidents continues to rise*', with 74% of businesses reporting a security breach in 2004, as compared with only 44% in 2000… [and] in the United States '*security breaches affect 90% of all businesses every year, and cost some $17 billion*'… One increasingly important mechanism for protecting corporate information, and in so doing helping to safeguard organizational

	knowledge assets, is through the formulation and application of a formal information security policy [strategy]." **Definition of Information Security Strategy** "The broad consensus within the literature is that the information security [strategy] is a high level document, which defines the organization's goals, intentions and priorities, with respect to the management of information security, as well as highlighting the roles, rights and responsibilities of individual members of staff, with respect to the attainment of the security objectives." **Aim of the Study** "[T]he broad aim of the study … [is] empirically examining the content and structure of actual information security policies." **Objectives of Information Security and Information Security Strategy** "… the information security policy [strategy] is an increasingly important business document, which is uniquely well placed to proactively safeguard the availability, confidentiality and integrity of corporate information resources." **Coverage of Polices is Modest** "The study has demonstrated that the coverage of information security policies, in terms of the numbers of issues explicitly addressed, is typically rather modest, particularly when judged against the prescriptions from the literature and the international standards." **Policies are Highly Techno-Centric** "It was not perhaps greatly surprising to find that our sample of policies still reflect a high techno-centric view of information security management, given the technical orientation of the majority of security standards." The study "highlights some worrying deficiencies in terms of explicit coverage of policy issues and the ability of organizations to effectively cross-reference and integrate their portfolios of information security documentation."
Additional note.	The study examines the structure and content of the security policies and concludes that the coverage of those policies is limited as compared to the recommendations from literature and international standards. The study also concludes that policies are more techno-centric and ignore the social dimension of information security.
05	**Data extracted from (Jafari et al. 2009)**
Reference	Jafari, S. et al., 2009. An approach for developing comparative security metrics for healthcare organizations. In *2009 International Conference for Internet Technology and Secured Transactions, (ICITST).*
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Issue of Interoperability among Healthcare's Isolated Information Systems** "Security and Privacy of patients' information are concerns of all healthcare organizations. These concerns do not only hamper the adoption of e-healthcare deployment but also the desire to interconnect isolated e-healthcare systems belonging to different organizations. The later case increases exposure to risks of damage, loss and fraud. Intuitively, if organization A is said to have certain security posture, and organization B is said to possess a certain security posture different from A, connecting A and B will result into a more vulnerable system than the individual systems. That is, weakness from each of the systems are aggregated thus increasing the channels for attacks." **Security Metrics** "Security metrics are collections of several measurements taken at different points in time, compared against baselines and interpreted to reveal an understanding. They provide insight, improve performance and accountability, and can reveal the overall security posture of an organization." "Security metrics are numbers computed to facilitate decision making in order to improve performance and accountability through collection, analysis, and reporting of relevant performance-related data…" **Security Posture** "the actual state of a system, entity, or process regarding security, that is, what the

system security assessment aims to describe…"

Current Security Assessment Practices

"The current security assessment practices focus either on measuring security programme effectiveness (e.g. using National Institute of Standard and Technology (NIST) metrics approach); auditing (e.g. using ISO/IEC 27002; or measuring specific IS components like networks (e.g. using vulnerability scanning, intrusion detection) and software (e.g. using defects counts, complexity measure, attack surfaces)."

Information Security

"A classical definition of security requires maintaining three attributes; confidentiality, integrity and availability. In some recent studies, authenticity, accountability and non-repudiation attributes are considered."

Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"

Availability

"Ensuring timely and reliable access to and use of information …"

Authenticity

"Verifying the identity of a user, process or device, prerequisite to allowing access to resources in an information system."

Non-Repudiation

"Ensuring no false denial of an entity of having participated in all or part of a communication."

Issues of Security in Healthcare Information Systems

"Healthcare organizations are vulnerable to security attacks due to the fact that they contain sensitive patient information. The nature of work require collaboration among multi-occupations communities (e.g. physicians, nurses, technicians, and administrative staff). These groups of users may have different understanding of security. In some cases, the urgency of work may necessitate bypassing security rules. In totality, ensuring an organizational impression that perceive security with an appreciation and attentiveness that encourages persistent responsible behavior becomes difficult. This environment make security and privacy issues more challenging to address.

New technologies like senor networks for remote patient monitoring introduces other risks. A stringent protection is required for any organization processing health information regardless of size, location, or mode of delivery."

Security Assessment and Metrics for Healthcare

"As far as we are aware, there are no security metrics publicly available for assessing security posture of healthcare organizations. A few security metrics for overall security assessment not tailored to any specific domain have been found.

Security Metrics based on Risk Management Approach Found in Literature and Suggested by Weiss et al

Weiss et al proposed security metrics that build on a risk management approach. In this study, security is quantified and measured in terms of incidents as a result of asset loss by organization in a defined time interval. Total security is reached if nothing is lost. In comparison, an organization is considered more secure than the other if it possesses the same set of assets but lost less than a competitor. It is also regarded as more secure if its possesses more assets but has lost the same. The metric has a number of limitations; among them is a notation of security and selection of security performance indicator. There is vague relationship between security incident counts and assets loss expressed in monetary value. The indicator *S* for security of an organization is given by the formula:

S = 100% - [percentage of lost asset]

Lucky of not being attacked may play its part. The countermeasures may not have the capability to know that you have been attacked. Also security is multidimensional, its overall measurements results cannot meaningfully be aggregated into a single value. The proposed security equation by itself does not tell much about security, but could be used to supplement other security metrics results.

Security Assessment Approach Proposed by ISO/IEC 17799 Predecessor of ISO/IEC 27002

	The approach described in proposed security programme maturity model using ISO/IEC 17799 standard, a predecessor of ISO/IEC 27002, by incorporating separately the notion of existence and quality. It defines security posture as an improvement to the maturity model which essentially modify maturity model based on the quality of implementation of each element. Existence of quality factor in the programme is an attempt to alter security assessment from existence to effectiveness of the process. The proposed programme permits the adoption of security standard with little or no customization. This is generally useful in ensuring uniform deployment of controls and generally can improve the process of auditing. It suffers from ensuring the reproducible assessment results due to lack of formula in reaching the results. **Security Assessment Approach Based on ISO/IEC 27002** The standard ISO/IEC 27002, contains eleven security controls with a total of 39 security categories. The recommended controls are to be implemented based on requirements identified from a risk assessment. The standard is intended to ensure uniform security management practices and help build confidence in inter-organizational activities. As extended to healthcare, BS EN ISO 27799 standard provides general guidance for implementation of ISO/IEC 27002 in healthcare domain. This standard specifies a set o detailed controls for managing health information security and provides a minimum requisite level of security appropriate for each individual healthcare organization. Both standards contain guidelines for security controls for organizations to adopt. These guidelines presented in generic-technology neutral fashion. They lack interpretation details of the suggested controls, put much focus on requirement enumeration and no account on measurement of its quality and applicability. It also becomes difficult to ensure reproducible objective results. **Metrics Development Criteria**
Additional note.	Interoperability among healthcare organisations is problematic and challenging due to privacy and security concerns. Information security becomes a bigger challenge due to the fact that there are no information security metrics which can be used to evaluate the information security to compare the overall security posture of two or more healthcare organisations. This study attempts to develop metrics which can be used to compare the security postures of different healthcare organisations so that they can interconnect.
06	**Data extracted from (Kuang & Ibrahim 2009)**
Reference	Kuang, T. & Ibrahim, H., 2009. Security privacy access control for policy integration and conflict reconciliation in health care organizations collaborations. In *Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS2009)*. New York: ACM, pp. 750–754. Available at: http://dl.acm.org/citation.cfm?id=1806480&dl=ACM&coll=DL&CFID=512023045&CFTOKEN=82822221.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Issues in Data Sharing among Healthcare Organisations** "Nowadays healthcare domains need to be collaborative and to support dynamic architectures in order to share data among different cross-organisations. Often such data sharing contains personal confidential information about a patient, such as family composition and DNA. Challenging security and privacy risk issues have arisen during sharing sensitive patient data in different large distributed and heterogeneous organizations. **Information Security in Healthcare** "Security concerns on confidentiality, integrity and availability of patient data. Privacy typically concerns the patient right to keep their personal medical records. Thus, security can be seen as a key to privacy, as a necessary condition to assure it."
Additional note.	The study is about developing an access control model which can facilitate integration and conflict reconciliation of security policies of different healthcare organisations.
07	**Data extracted from (Sheppard et al. 2009)**

Reference	Sheppard, N.P., Safavi-Naini, R. & Jafari, M., 2009. A Digital Rights Management Model for Healthcare. *2009 IEEE International Symposium on Policies for Distributed Systems and Networks*, pp.106–109. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5197393 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Electronic Healthcare Records** "Electronic healthcare record systems promise to increase the efficiency and effectiveness of healthcare systems by ensuring that healthcare workers can get timely access to the correct and complete information that they require in order to provide good health services to their patients. Electronic healthcare systems have been investigated in many countries, and numerous research journals and conferences are devoted to their design and evaluation. **Risks Attached with Use and Information Security of Electronic Healthcare Records** "Distribution of information through electronic healthcare system, however, carries a risk that patients' information will be misused, resulting in invasions of privacy and/or unfair discrimination on the basis of patients' medical histories. Security and privacy therefore forms an important of any electronic healthcare system." **Electronic Healthcare Records' Issue of Privacy and Consent** "In particular, the principle of *consent* is widely used in privacy law to restrict the disclosure of sensitive information according to the wishes of the subject of the information. *Electronic Consent Systems* allow the subject of some electronic information to permit or deny the disclosure of the information to the particular people in particular circumstances. Electronic consent systems have been proposed as a method of controlling the disclosure of healthcare records as well as other kinds of personal information. Electronic consent systems bear some resemblance to *digital rights management systems* ("DRMs"). Digital rights management is best known for its use in the protection of intellectual property, but can also be applied to the protection of personal information."
Additional note.	The Study suggests a model for a secure electronic healthcare record system on the basis of digital rights management approach to privacy protection and workflow-based access control.
08	**Data extracted from (Win & Fulcher 2007)**
Reference	Win, K.T. & Fulcher, J. a., 2007. Consent mechanisms for electronic health record systems: A simple yet unresolved issue. *Journal of Medical Systems*, 31(2), pp.91–96. Available at: http://link.springer.com/10.1007/s10916-006-9030-3 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Security Concerns regarding Electronic Healthcare Records** "EHRs include sensitive health information and if they are integrated among healthcare providers, data can be accessible from many different sources. This leads to increased concern regarding invasion of privacy and confidentiality. Incorporating consent mechanisms into EHRs has potential to enhance confidentiality. However there are both positive and negative effects from employing such mechanisms- they need to balance privacy, safety, consumer and public interest." **Benefits of Electronic Healthcare Records** "Integrated EHRs have the potential for enhanced sharing of information among healthcare providers as well as enhancing communications between healthcare providers and patients/consumers." **Issue of Consent and Privacy** "In recent times, the focus in healthcare has changed from healthcare providers' paternalistic approach to a consumer focused approach, with the importance of obtaining

consumer's consent for use of health information being emphasised in the latter [EHRs]. Nevertheless, since EHRs include patients' health information and this raises concerns over privacy and confidentiality of such information."

Privacy and Confidentiality

"To maintain privacy and confidentiality, a system needs to be secure. Issues of confidentiality and abuse of data cause many healthcare providers to oppose the integration of medical databases despite the potential benefits. Therefore EHR implementations need to ensure privacy and confidentiality. Healthcare providers and other stakeholders have a duty to maintain the confidentiality of data, and systems need to prohibit access by unauthorized users.

Patients' medical data can be revealed only with the patients' consent, except in emergencies or when the law obliges the healthcare providers to do otherwise. In certain serious medical situations, the principle of implied consent assumes that patient would provide consent if they were competent, even though patient is incapable of communicating such consent, unless the patient has *explicitly* refused even in emergencies."

Consent

"Consent in medicine - in the context of both therapy and research - has been debated since the Second World War. More specifically, there is a need for informed consent and the necessary flexibility of its application. However, in earlier times consent was primarily focused on treatment and procedures."

"Consent should be informed, voluntary and competent. The degree of informed consent may vary according to interpretation. It can be a "subjective standard of disclosure," where the patient has been informed of all the information that she has asked for, or a "professional standard of disclosure," where the patient has been given all the information that a reasonable professional would convey.

There is increasing emphasis on patient autonomy and patients' rights. Patients need to know how information will be kept, who is able to access their records, and for what purpose."

"Many organisations with access to health information do not obtain an individual's consent for disclosing personal information. Effective notification and truly informed consent requires that individuals know and understand the contents of the record in question; it is unethical to use implied consent when the patient is not fully aware of the information disclosure."

"**The data protection act of 1998, UK** states that:

"Sensitive health data cannot be processed in the absence of explicit consent unless they are needed for medical purposes or undertaken by professional who in a circumstance owes a duty of confidentiality."

"To protect patient's privacy, integrated EHRs must be access controlled. AS EHRs become more integrated between healthcare organizations, system access levels become increasingly more important. There can be a role based access mechanism among the healthcare providers with an organization (such as doctors, nurses, and administrative staff). In addition each clinical record can be marked with a list of authorized personnel."

"Consent mechanisms need to balance privacy and safety against both consumer and public interest. In New Zealand in 1983, a general practitioner was charged because he had disclosed a patient's heart condition, which can be dangerous for driving children's school buses, with the result that the patient sued him. Although cases are dealt with differently in different countries, it is advisable that the need to disclose sensitive information to the governing authority should be discussed with the patient and the patient's permission sought *beforehand.* Several countries have enacted legislation to enhance information privacy of personal health information. The USA HIPAA (Health Insurance Portability and Accountability Act), PIPEDA (Personal Information Protection and Document Act) in Canada, and HRIPA (Health Records and Information Privacy Act 2002) of NSW, Australia are some typical examples."

"It is undeniable that properly integrated EHRs have potential for enhancing the sharing of information among healthcare providers, healthcare institutions and patients. Obtaining appropriate consent for use of health information would enhance patients' privacy. However, consent mechanisms need to be practical and applicable to healthcare processes without impeding the workflows of healthcare providers. So that use of EHRs is able to assist in the healthcare delivery process. Physicians need to be better informed

	about the health status of patients in order to improve their healthcare decision making. Moreover, obtaining consent should not undermine medical/health services research. There should be appropriate mechanism or legislation to obtain high quality research data as health service research is important in the prevention and treatment - indeed, the very future of healthcare process." **Information Security in Healthcare** Privacy, confidentiality, and access are important considerations in the successful implementation of EHR systems. Therefore incorporating consent mechanism is essential. Healthcare institutions and authorities need to implement appropriate consent mechanism in order to maintain consumer privacy. Finally, such a consent mechanism need to maintain privacy without impeding the healthcare process in order to achieve the best healthcare outcomes for consumers."
Additional note.	Maintaining confidentiality of patients' data is the responsibility of healthcare providers. Therefore, healthcare organisations need to develop and implement appropriate consent mechanism to ensure patients' privacy.
09	**Data extracted from (Hamill et al. 2005)**
Reference	Hamill, J.T., Deckro, R.F. & Kloeber, J.M., 2005. Evaluating information assurance strategies. *Decision Support Systems*, 39(3), pp.463–484. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167923604000284 [Accessed June 13, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Information Technology** "The tremendous worldwide increase in reliance upon information technologies (IT) reaps huge benefits for their users but also threatens significant drawbacks. These technologies afford decision-makers with the capability to quickly fuse data from multiple sources, make informed decisions, and disseminate those decisions at nearly the speed of light. IT capabilities have become essential for day-to-day operations in today's global economy." **Importance of Information Security** Increasing trends in cyber attacks on information systems imply that information security will continue to be of vital importance. **Balanced Information Security** "To provide information assurance, the level of assurance attained must often be balanced with potential reductions in operations capability and the consumption of valuable resources (e.g. time, money and people)." **Information Security** "IA protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access control, secure network servers, and intrusion detection software."
Additional note.	The study offers an evaluation model to compare different strategies in order to select a better strategy in order to create a balance between information security, operational capability, and resource cost. A good strategy should provide with higher levels of information security while not compromising on required level of operational capability. Such a strategy however must be less costly as compared to other strategies.
10	**Data extracted from (Wiant 2005)**
Reference	Wiant, T.L., 2005. Information security policy’s impact on reporting security incidents. *Computers and Security*, 24(6), pp.448–459. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404805000490 [Accessed June 22, 2014].
Study type Journal/ Conference/	Journal

book	
Data that address the research questions	**Risks Attached with Use of Electronic Healthcare Records** "Modern computer applications in the healthcare industry threaten individual information security despite offering significant benefits to patients and practitioners. In any industry compared to paper based records, computer databases of personally identifiable information may be accessed, changed, viewed, copied, used, disclosed, deleted more easily and by more individuals regardless of their official access restrictions. Private or commercial parties can assemble medical profiles by using only a minimum amount of personal data." **Health Privacy Rules/Laws** "The New Health Privacy Rule, effective April 14, 2003 has made it illegal for healthcare providers and insurers to release a patient's medical records without the individual's consent. Rule provisions dictate that healthcare providers and insurers must have a written information security policy and present it to patients." **Computer Abuse** "Computer abuse is defined as the unauthorized, deliberate, and internally recognizable misuse of computers of any organization's information system by individuals. Possible violations include: (1) The unauthorized access of a computer to obtain information relating to hospital operations, to obtain information relating to hospital financial records, or to manipulate information on a computer that would adversely affect the hospital's operation of the computer. (2) Accessing a hospital computer without, or in excess of, authorization and with intent to defraud or obtain anything of value, to include medical record information. (3) The intentional access of a hospital computer without authorization, where such access alters, damages, or destroys information, to include medical records, or prevents "authorized use" of the computer. (4) Certain types of reckless conduct in addition to intentional acts. This may include the transmission of malevolent software, such as computer viruses, if such actions are sufficiently reckless. (5) Knowingly, and with intent to defraud, trafficking in passwords, which would permit unauthorized access to a hospital computer." **Information Security** Information security has been defined as encompassing systems and procedures designed to protect an organization's information assets from disclosure to any person or entity not authorized to have access to that information, especially information that is considered sensitive, proprietary, confidential, or classified, as in national defense." **Causes of Security Incidents** "Security incidents are largely due to operating system vulnerabilities, abuse of valid user account or permissions, and unintentional user error. The perpetrators of such attacks are believed to be internal users to per 31% of survey respondents." **Means of Security Incidents** "There are four principal means by which sensitive information is exposed. Those means are: intentional theft by unauthorized agents outside the organizations; theft or sabotage by former employees or disgruntled current staff; accidental exposure by employees entrusted with the information for use in their particular jobs; various types of disclosures by members of the healthcare industry as exemplified by the availability of Nicole Brown Simpson's medical records within one week of her murder in 1994, and from uncontrolled use of information among secondary users. **The Accidental Exposure of Information** Of the avenues of information loss, the accidental exposure of information by an employee is the most common problem. The accidental exposure of information is usually due to employee negligence, ignorance, or carelessness. However, in the healthcare industry the uncontrolled use of information by secondary users is the greatest threat. These secondary users include insurers, pharmaceutical payers, some employers, and other players in the emerging health information service industries. Some of these secondary users such as employers who are self-insured, are highly conflicted. Due to the passage of the Employment Retirement Income Security Act (ERISA), self insuring

	employers are entitled to receive fully identified patient information for employees being covered. The purpose of these disclosures is to allow the employer/insurer to make sound benefit management decisions. However, this information could be used to terminate employment if the medical information reveals medical condition to the employer/insurer that would not have been accessible to an employer under normal employer/employee relations.
Additional note.	The study has attempted to establish that formal security policy helps to increase the reporting of security incidents and decreasing the number of security incidents. Security policy is an important tool which increases the level of information security in an organisation.
11	**Data extracted from (Loef et al. 2002)**
Reference	Loef, C., Mankovich, N.J. & Rosner, M., 2002. Standards and security for medical information technology. *MedicaMundi*, 26(2), pp.41–46. Available at: http://www.healthcare.philips.com/pwc_hc/main/about/assets/Docs/medicamundi/mm_vol46_no2/loef.pdf.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Information Technology** "IT in healthcare provides a set of tools intended to organize the enterprise and improve efficiency, thus serving more people with better outcomes." **Standards** "Standards allow the systems to operate and interoperate in a smooth and seamless manner. Shared definitions of healthcare terminology, and information exchange protocols, allow a smooth flow of care-critical and business data." **Information Security** "Security allows the system to protect the privacy and integrity of both the enterprise and the patient. Part of the promise of IT is that information is accessible wherever it is needed. The dark side of this improved accessibility is that, unlike its paper counterpart, the information can be duplicated, distributed, changed or destroyed instantaneously, electronically, and en masse." For information security in healthcare "security policies, procedures and technology are needed to ensure the continuing confidentiality, integrity and availability of a patient's health information." "Security in healthcare enterprise is concerned with protection from: • physical injury to health and property • invasion of privacy • theft or destruction of vital information • compromises in operational integrity. **Issues arising from Lack of Information Security in Healthcare** "If [information security] not properly implemented, securing information access could not only lead to legal problems, but could also become an impediment to integration and interoperability and, in the worst case, could adversely affect clinical workflow and efficiency."
Additional note.	The study discusses the requirements of standards and security in healthcare.
12	**Data extracted from (Humaidi et al. 2011)**
Reference	Humaidi, N. et al., 2011. Investigating the Relationship of Users ' Behavior and Internal Security Threat towards the Implementation of Total Health Information System (THIS) in Malaysian Medical Institutions. *Australian Journal of Basic and Applies Sciences*, 5(9), pp.291–297. Available at: http://connection.ebscohost.com/c/articles/69735084/investigating-relationship-users-behavior-internal-security-threat-towards-implementation-total-health-information-system-this-malaysian-medical-institutions.
Study type Journal/ Conference/	Journal

book	
Data that address the research questions	**Information Security in Healthcare Databases** "Health information System require three aspects of security, which are confidentiality, integrity and availability (CIA) … the system require strong confidentiality as the health information is an important in medical. Integrity is essential since incorrect treatment based on erroneous medical data might be fatal. Moreover, availability is also as important as integrity because the information in health information system might be necessary for adequate treatment." **Motivations to Breach Information Security of Healthcare** "Problem can be arising if patient medical information can be accessed through internet or the use of secondary storage by non-healthcare providers. Those data will be used by third party payers to process claims and to manage pharmacy benefits programs … [D]isclosure of personal health information may result in discrimination by employers insurance agencies if they get access to such information and could manipulate the information in the systems. The systems provide more cost effective healthcare and to support the information needs of integrated delivery systems. However, these systems are vulnerable to inappropriate use, both within and without the medical institution that provides care. "*The systematic use of patient-identifiable health information by insurers, employers, drug companies, and commercial marketing firms poses major threats to the privacy and security of health information"* (Anderson 2000, p.116 cited in Humaidi et. al.) "Hackers are also one of health information security threat as hackers could access health information if the provider lacks adequate data security. Threats to information security have been studied for many years. Most of the studies examined in the related fields were categorized as studies of computer abuse or computer ethics… Viruses, worms, hackers, and employee abuse and misuse have created a dramatic need for understanding and implementing quality information security."
Additional note.	
13	**Data extracted from (Kumar & Puri 2012)**
Reference	Kumar, S. & Puri, A., 2012. A Framework for Evaluation and Validation of Information Security Policy Er. Satish Kumar Assistant Professor Dept. of Information Technology Mr. Amit Puri Assistant Professor Dept. of Computer Application GIMET, Amritsar. *International Journal of Computer and Distributed System*, 1(3), pp.19–31.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security** "Effective information security systems incorporate a range of policies, security products, technologies and procedures." "Information security means protecting information and information systems from unauthorized access, unauthorized use, disclosure, disruption, modification or destruction." "In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information (Parkerian hexad). The elements are confidentiality, possession, integrity, authentication, availability, and utility."
Additional note.	
14	**Data extracted from (Kazemi et al. 2012)**
Reference	Kazemi, M., Khajouei, H. & Nasrabadi, H., 2012. Evaluation of information security management system success factors: Case study of Municipal organization. *AFRICAN JOURNAL OF BUSINESS MANAGEMENT*, 6(14), pp.4982–4989. Available at: http://www.academicjournals.org/ajbm/abstracts/abstracts/abstracts2012/11Apr/Kazemi et al.htm [Accessed June 22, 2014].

Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Key Success Factors for Information Security** On the basis of empirical evidence, the study has found top management's support, Information security policy and training and awareness programs as the most effective success factors for information security.
Additional note.	
15	**Data extracted from (GAO 2006)**
Reference	GAO, 2006. *NFORMATION SECURITY: Department of Health and Human Services Needs to Fully Implement Its Program*, US. Available at: http://www.gao.gov/products/GAO-06-267.
Study type Journal/ Conference/ book	Report
Data that address the research questions	**Information Security** Information security means "protecting the confidentiality, integrity, and availability of its information and information systems."
Additional note.	
16	**Data extracted from (Jirasek 2012)**
Reference	Jirasek, V., 2012. Practical application of information security models. *Information Security Technical Report*, 17(1-2), pp.1–8. Available at: http://dx.doi.org/10.1016/j.istr.2011.12.004.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security** "The information security is a part of information risk management, which in turn has a place in the business risk management. This shift in approach enables clever information security professionals talk similar language as business people; those who actually bring money to the company." "It [Information Security] is all about People, Process,…, Technology." **A. Security Drivers** "Clearly, if there were no drivers then we would not need to do any security. There are three major drivers for security work: 1. **Laws & Regulations** - These are something than a company must comply with or face legal action or a fine. For example, complying with the Data Protection Law or the Company Act Law is an example of the legal drivers. Complying with the PCI DSS is an example of regulation drivers. 2. **Business Objectives** - The company typically wants to generate profit and defines a set of business objectives. Security supports these business objectives by protecting systems and information that is used in the business processes. Think of protecting Microsoft Windows source code: if the source code was not protected I could have compiled my own operating system without paying Microsoft any licence fee. Hence Microsoft business objecting "Sell Software" is supported by "Protect Source Code" security objective. Amazon's business objective is to sell product in their online shop. The business objective is to have on-line shop up 24/7. Security objective is to keep system up and running, be it by keeping them free of malware that could disrupt or slow IT systems, or keeping attackers at bay. 3. **Security Threats -** a trick one in this context. Security threats work against laws &

	regulations and business objectives. However, they are driving information security as well and company needs to respond to threats in order to satisfy first two drivers." B. **Security Management** In this area we have three frameworks that enable company to achieve objectives defined in the drivers section. 1. **Policy Framework** [Definition of Strategy] This is a set of policies, standards and guidelines that describe how the company addresses information security drivers. All together these define security controls that are available for a company to implement. There are also International Standards which can be source of information and controls for the Policy framework. i. **Policies -** describe high level to deal policy statements, and Security Control Objectives (typically using words should and must). The key objective of the security policy document is the alignment with the business objectives and drivers. I have seen security policy being a simple copy of ISO27001 Annex A document without actually describing why individual control objectives have been selected. It is then very difficult to justify investment into something which "is compliant with a policy" but does not support business objectives. ii. **Standards -** detailed security controls that should be implemented to support individual policy statements. I see the relationship and 1:N here, i.e. one policy statement can be supported by multiple security controls. Again without a link to a policy the security professionals will hardly justify why the password needs to be 12 characters and change every 45 days. The controls should be selected from an internationally accepted catalogue of controls. iii. **Artefacts** - It is all very well to have statements like "must be authenticated" but how is that done in practice by an engineer that actually needs to configure the system? I have learnt that architecture standardisation is the key to success of any company. Same applies to security. If I find a solution to implement a security control from the "Standard" I will put it into a "Security Architecture Repository". That way someone else can benefit from my experience, and more importantly achieve consistent security. Far too many security professionals do not document these into a shared library, which results in problems when they leave the company. 2. **Process Framework** This section in the Security Management implements what is stated in the policy framework. Any security control in a policy or a standard is a process, no exceptions. This is where people and technology come into play. Each process is supported by people and most are supported by technology. However, there needs to be link between any technology the company has, its process, corresponding controls in the policy framework up to the business objective. This enables traceability of the security investments and allows security professionals to justify the security budgets. 3. **Security Metrics Framework** This is rather, in my view still developing area of information security management. A proliferated statement "What you cannot measure, you cannot manage" can be applied in security as well. Security professionals should be able to measure the state of security controls, compliance with own policies and effectiveness of security processes. My key metrics here is to take a security policy statements and measure each team against them; this turns into a nice balanced scorecard for security. The metrics framework provides feedback to the process framework with the necessary metrics information to run the security processes as designed. **C- Stakeholders** Stakeholders, for example classified using TOGAF methodology, are the recipients of the security metrics framework results. The stakeholders need to know that what has been promised is being delivered. More importantly, the security professional needs to show the value of security to business. This is the area where security professionals need to enhance their skills. Talk to your stakeholders, ask them what their concerns are and show them how your are addressing the concerns. Then send a report to them that relates to their area and concerns. Get them on your side.
Additional note.	Security drivers are the factors that determine the requirements of information security for an organisation. There these are also the factors which distinguish the requirements of information security of one organisation from the other. Healthcare has its own unique security drivers which make it different from other sectors in terms of information

	security requirements. Therefore information security strategies for healthcare should be developed and evaluated according to the security drivers for healthcare.
17	**Data extracted from (Bakker 1998)**
Reference	Bakker, A., 1998. Security in perspective; luxury or must? *International Journal of Medical Informatics*, 49(1), pp.31–37.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Information Technology for Healthcare [Clinical Requirements]** "Information is of ever increasing importance in the delivery of modern healthcare. Because of evolution of medicine, there is more to know and more to remember. Data on each case is collected by healthcare providers and recorded, until now mostly on paper, but increasingly in digital form. This is because it is not realistic to except care providers to remember patient data, the more because they in general have to deal with many patients. In their contacts with a patient, the recorded data are used to be able to realise continuity of care. Because of the increase in medical knowledge, we see an ever progressing specialisation in healthcare. No longer can one person treat a complex case, but several specialists work together in the 'care team'. Data have to be communicated between team members, another reason for recording the data. Some of the specialists work in dedicated departments like laboratories or radiology. They need patient data to carry out their specialised job, so data must be communicated throughout the institution. With the increasing complexity of the healthcare system (transmural care) the need for the data exchange between healthcare providers in different institutions is also increasing. Data are not only needed for the care/cure process; healthcare institutions, in particular hospitals, are complex organisations and to run them efficiently data are needed to support logistics, administration and management. Last but not least, patient data are needed as fuel for medical research, in this way advancing in the long term medical knowledge and quality of care. The handling of information by pencil and paper has serious limitations, such as: • information is available only at one location at a time. • fixed structure (difficult to sort); • can hardly be analysed systematically; • difficult to read These limitations can in principle to a large extent be overcome by using information and communication technology (ICT). With the rapid evolution of this technology we see increasingly successful use in healthcare. Initially, in isolated departments such as laboratories, radiology or the medical records office, later institution-wide with 'integrated hospital information systems,' initially mainly supporting logistics and information supply, these days we see as major trends: 1. Direct support of the primary care/cure process by means of electronic patient records (EPR) and nursing applications being used by the healthcare professionals through workstations/terminals at their working locations. 2. Information exchange beyond the borders of institutions, e.g. sending of patient information to general practitioners or pharmacies through EDI or a regional EPR share by all healthcare professionals dealing with the patient, at different location. 3. Handling of multimedia data by the information systems. **Problems of Information Technology in Healthcare** It is not surprising that the idea of applying ICT in healthcare was received with great enthusiasm, even in the early days of computers; a welcome aid was expected for institutions suffering from inadequate information supply. Many project were launched, but most of them did not meet the expectations because of, among other thing: • limitations in the technology (storage capacity, processing speed, operating systems, programming techniques, networks); • limitations in the user interface (healthcare professionals are not used to typing); • the complexity of the processes in healthcare institution;

- the significant role of improvisation in healthcare;
- the limited experience in developing such complex software systems.

It was already recognised at the end of the 1970s that ICT in healthcare also can have negative side effects:

- access to patient data by unauthorised persons;
- linking of datasets;
- systematic analysis of the datasets;
- loss or inaccuracy of the data.

In view of the benefits to be expected from application of ICT in healthcare, it would be a serious error not to use it, because it can improve both the care/cure process and the efficiency. On the other hand, it would be a serious error not to protect against the negative side effects.

Drawbacks of Paper Based Medical Records

- the access to the record is hardly restricted, a white coat is often sufficient;
- reports are often distributed in an insecure way, data and even complete files get lost;
- data are difficult to read, so may be misinterpreted;
- data are not at the place where they are needed.

However, damage in the paper and pencil system is in general incidental, whereas in computer systems the effects may be massive and systemic.

Information Security

"Fortunately, a standard terminology has emerged, dividing the field of security in three domains:" confidentiality, Integrity, and availability.

Confidentiality

"The prevention of the unauthorised disclosure of information."

"The aspect of confidentiality has until now received most attention, both from public opinion and the government. In most western countries, legislation sets rules for the systematic registration of personal data in computer systems and the communication/processing of such data. Important principles are the rights of the data subjects for:

- information (that the register exists and which data are stored for how long a period);
- inspection (access to personal data);
- modification (in case the data recorded is incorrect);
- deletion.

In most regulations and laws special attention is given to medical data. The legislation differs significantly between countries. The Directive of the European Union aims at harmonisation at least in its member states, however in several points it leaves freedom for national preferences, e.g. the question of whether the patient can have direct access to his/her own data or if such access is only possible through a healthcare professional.

Violations of confidentiality may occur through, for example:

- lack of authentication of users;
- poorly defined access rights, giving access to data not needed;
- inadequate rules for the use of patient data for research purposes. In general such use should only be allowed with explicit consent of the patient;
- unsupervised distribution of computer output;
- unauthorised access to the computer centre.

Integrity - the prevention of unauthorised modification of information.

Integrity attracts much less attention from the public opinion and politics, nevertheless it is an issue to be taken seriously. Data should be presented to the authorised user without modification, deletion, or addition. The integrity of data might be damaged by, for example:

- program errors;
- hardware failures (e.g. head crashes of magnetic disks);
- communication failure;
- human errors in the handling in the technical structure;
- malicious alteration of the data by either authorised or unauthorised users."

Availability - the prevention of unauthorised withholding of information or resources.

Availability is especially important in healthcare where often the care has to be

	continuous (24 hours a day, 7 days a week). With the further increase in the role of ICT in healthcare, healthcare providers will more and more rely on the data in their work. Of particular importance is the EPR. Non-availability may be caused by, for example: • failure of the computer system; • failure of the network/inconsistencies in the data bank; • program errors; • environmental conditions (fire, flooding); • human errors.
Additional note.	Healthcare has its own benefits and challenges in adoption of information technologies. Information security is one of the biggest challenges.
18	**Data extracted from** (Yoo et al. 2007)
Reference	Yoo, D. et al., 2007. Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection). *Engineering and Technology*, 36(December), pp.162–166.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	The study has developed a methodology for assessing the information protection level which can be used to establish the quantitative object setting method required for the improvement of the information protection level. This paper intends to check the current security status and establish security measures accordingly to protect infrastructures effectively, and will propose a methodology of evaluation for the information security level for Critical Information Infrastructure Protection (CIIP), which can enhance the security level of critical information infrastructure. The Information Security Evaluation Method will provide specific assessment schemes and methods that can be used for constant and active enhancement of security level. (For further data refer to the paper)
Additional note.	
19	**Data extracted from (Schumacher et al. 2006)**
Reference	Schumacher, M. et al., 2006. *Security Patterns: Integrating security and systems engineering*, West Sussex: John Wiley & Sons Ltd. Available at: http://books.google.com/books?hl=en&lr=&id=T57rfpDko0YC&oi=fnd&pg=PR7&dq=Security+Patterns,+Integrating+Security+and+Systems+Engineering&ots=YJc3aw0jbL&sig=BTd_WIPUZ5y1fcGJyWjqk10DIJ0\nhttp://books.google.com/books?hl=en&lr=&id=T57rfpDko0YC&oi=fnd&pg=PR7&.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Information Security** An asset's information security properties include confidentiality, integrity, availability and accountability. (p.104) **Information Security Requirements** "The information security requirements are normally provided by the asset owner. Otherwise, the security needs of the asset can be identified by applying Security Needs Identification for Enterprise Assets."(p.106)
Additional note.	
20	**Data extracted from (Biskup 2009)**
Reference	Biskup, J., 2009. *Security in Computing Systems,* Available at: http://www.amazon.co.uk/Security-Computing-Systems-Challenges-Approaches/dp/3540784411.

Study type Journal/ Conference/ book	Book
Data that address the research questions	**Information Security** Mainly but not exclusively, threats might be directed against following security goals, interpreted as interests: - availability of data and activities; - confidentiality of information and actions; - integrity of the computing system i.e., correctness of data concerning contents and the unmodified state of the data, programs and processes; - authenticity of actors, including later - non-repudiation of their actions. (p.6)
Additional note.	
21	**Data extracted from (Blyth & Kovacich 2006)**
Reference	Blyth, A. & Kovacich, G., 2006. *Information Assurance* 2nd ed., London: Springer-Verlag London. Available at: http://www.springer.com/gb/book/9781846282669.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Information Security** Information security means protection against unintended exposure which "is a form of possible loss or harm against an information asset… Examples of exposure include unauthorised disclosure of data, modification of data or denial or legitimate access to the information asset." Information security can be defined as *"The protection of information against unauthorised disclosure, transfer, modification, or destruction, whether accidental or intentional."*
Additional note.	
22	**Data extracted from (Pishva et al. 2007)**
Reference	Pishva, D. et al., 2007. An initiative to improve the state of information security at local governments in Japan. In *Proceedings - International Carnahan Conference on Security Technology*.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Information Technology** "Today's business activities depend highly on information systems and every enterprise has its own information for its business. In an industrialised country like Japan, most enterprises use information technology to establish their management governance. This helps them improve their efficiency and cost performance. As it is called 'IT governance' information systems have significant impact on the operations. Information assets have thus become valuable commodities for business and information systems are the key factors to ensure the growths of enterprises."
Additional note.	
23	**Data extracted from (Speed & Ellis 2003)**
Reference	Speed, T. & Ellis, J., 2003. Chapter 6: Authentication and Authorization. In *Internet Security: A Jumpstart for Systems Administrators and IT Managers*. USA: Digital Press Elsevier Science, p. 398.

Study type Journal/ Conference/ book	Chapter
Data that address the research questions	**Authentication** "Authentication is a process where a user (via any type of physical access - PC, network, remote) establishes a right to an identity. I log in to a system with my user name and password, and the system now knows who I am." **Authorisation** "Authorisation is the process of determining whether a user is permitted to perform some action or access to a resource. I log in to a system with my user name and password, and the system knows who I am and now can grant or deny access to certain databases."
Additional note.	
24	**Data extracted from (Gerber & von Solms 2008)**
Reference	Gerber, M. & von Solms, R., 2008. Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27(5-6), pp.124–135. Available at: http://dx.doi.org/10.1016/j.cose.2008.07.009.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Requirements** Information security requirements are directly related to the unique need for information security that an organisation has. A methodical assessment of security risks is used to identify the requirements. Once the information security requirements have been identified, controls should be identified and implemented to ensure that risks are reduced to an acceptable level. These distinctive requirements for organisations, irrespective of their size and, are derived from three sources: 1. **Assessing Security Risks:** Assessing the unique set of security risks to an organisation, which could lead to significant losses in business if they occur. This assessment normally takes the form of some risk analysis that is used for the identification of threats to assets, the evaluation of vulnerabilities to and likelihood of occurrence and an estimation of the potential impact. 2. **Information Processing of Unique Requirements** The second source is the unique organisational principles, objectives and business requirements, developed by an organisation for processing information, to support its business operations. "It is important, e.g., for a competitive edge, cash flow and/or profitability, that the ISMS supports these requirements, and vital that the implementation, or absence, of security controls in each of the information systems do not impede efficient business operations." 3. **Legal Compliance** The third source relates to the legal, statutory, regulatory and contractual requirements to which an organisation, its trading partners, contractors and service providers have to comply. Examples of these include the data protection legislation, copyright restrictions and organisational record preservation. Additionally, an organisation may have to adhere to certain contractual requirements, based on the agreement that exists between parties when serving as a customer or supplier of products and services. **ISO 27002: The Standard** A revised and improved version of the joint ISO/IEC 17799 standard, which has become the growing e-commerce community's international benchmark for information security management, was published and released in June 2005. During April 2007 it was replaced and emerged under the series of 27,000 numbers of the new numbering scheme as ISO/IEC 27002. The Standard has 133 controls under 11 headings. The consideration of other security controls, not listed in ISO 27002, may be assets or to counter exceptionally high level of security threats. **Specific Security Requirements and The Standard ISO 27002** To ensure that the appropriate controls are identified and selected, it is essential that an organisation first establishes the security requirements for its information systems, to be

	included in an Information Security Management System (ISMS), in the context of its business and business environment. Thus, when dealing with ISO 27002, the most effective way of achieving information security is to use a structured approach, based upon an organisation's specific security requirements. Adhering to this recommendation will ensure that all the most important areas are considered. **The Legal Aspects of Information Security Requirements** "ISO 27002 mentions four requirements of the legal source with which an organisation, its trading partners, contractors and service providers have to comply, namely legal, statutory, regulatory and contractual … the terms legal, statutory, regulatory and contractual all share the commonality of being legally binding, resulting in some form of penalty, regardless of whether it is of civil or criminal nature, if violated." **Legal** A rule is a legal rule when it is recognised by the State, being an authoritative body, as binding upon its subjects (Chetty 2004, p.4. cited in). The purpose of law is, therefore, is to preserve order and to promote justice. **Statutory** The adjective 'statutory' is defined as "required, permitted or enacted by statute". A statute is, "a written law passed by a legislative body" or "a rule of an organisation or institution". Statutes are legislation passed by Parliament, which is normally the highest law-making body in a country, and once they are passed, they are known as Acts of Parliament. **Regulatory** The word 'regulatory' means "control or supervise by means of rules and regulations". A regulation is "a rule or directive made and maintained by an authority", "in accordance with regulations" or "the action or process of regulating or being regulated. **Contractual** "relating to or agreed by a contract". "A written or spoken agreement intended to be enforceable by law". **Model to Determine Specific Information Security Legal Requirements of an Industry** Four Legal Categories proposed: 1. Intellectual Property Rights 2. Legislation (statutes & regulations) 3. Contractual obligations 4. International Laws (treaties) **The Legal Mapping Matrix** The main aim of this model is to assist in ensuring compliance to most, if not all, the legal requirements related to a specific organisation's unique needs and circumstances. "***Compliance cannot be attained by an organisation unless it is specified what it want to comply with and to what extent (Casper 2004 cited in)."*** **(**The study offers a method to determine specific information security requirements of an organisation)
Additional note.	
25	**Data extracted from (Knapp et al. 2009)**
Reference	Knapp, K.J. et al., 2009. Information security policy: An organizational-level process model. *Computers & Security*, 28(7), pp.493–508.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Policy (Strategy)** "The development of information security policy is the first step toward preparing an organisation against attacks from internal and external sources… Information security policy addresses the integrity, availability, and confidentiality of electronic data held within and transmitted between information systems and is the precondition to implementing effective deterrents. Policies act as clear statements of management intent and demonstrate that employees should pay attention to information security. Without an

	approved policy document, overall guidance may be lacking and managerial support called into question."
Additional note.	
26	**Data extracted from (Anderson 2000)**
Reference	Anderson, J.G., 2000. Security of the distributed electronic patient record: A case-based approach to identifying policy issues. *International Journal of Medical Informatics*, 60(2), pp.111–118. Available at: http://ac.els-cdn.com/S1386505600001106/1-s2.0-S1386505600001106-main.pdf?_tid=a5d594c2-fa65-11e4-9362-00000aacb35e&acdnat=1431627701_6a586b83c4e3360a6b894f23792f7fc4.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Importance of Information Technology for Healthcare** The growth of managed care and integrated delivery systems has created a new commodity, health information and the technology it requires… the importance of collecting, electronically storing, and using the information is undisputed. This information is needed by consumers to make informed choices; by physicians to provide appropriate quality clinical care; and by health plans to assess outcomes, control costs and monitor quality. **Information Security Concerns for Electronic Healthcare Records** The collection, storage and communication of a large variety of personal patient data, however, present a major dilemma. How can we provide the data required by the new forms of healthcare delivery and at the same time protect the personal privacy of patients? Recent debates concerning medical privacy legislation, software regulation, and telemedicine suggest that this dilemma will not be easily resolved. The problem is systematic and arises out of routine use and flow of information throughout the health industry. Healthcare information is primarily transferred among authorised users. Not only is the information used for patients care and financial reimbursement, secondary users of the information include medical, nursing, and allied health education, research, social services, public health, regulation, litigation, and commercial purposes such as the development of new medical technology and marketing. The main threats to privacy and confidentiality arise from within the institutions that provide patient care as well as institutions that have access to patient data for secondary purposes."
Additional note.	The study discusses important issues related to public policy on information security of electronic healthcare records.
27	**Data extracted from (Booker 2006)**
Reference	Booker, R., 2006. Re-engineering enterprise security. *Computers and Security*, 25(1), pp.13–17. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167404805002051 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security** "Enterprise security and compliance are becoming increasingly important to organisations of all sizes, and it is more vital than ever that these businesses need to have an organised, efficient, and proactive approach to information security."
Additional note.	
28	**Data extracted from (Eminağaoğlu et al. 2009)**
Reference	Eminağaoğlu, M., Uçar, E. & Eren, Ş., 2009. The positive outcomes of information security awareness training in companies - A case study. *Information Security Technical Report*, 14(4), pp.223–229. Available at:

	http://linkinghub.elsevier.com/retrieve/pii/S1363412710000099 [Accessed June 11, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Management** One of the key factors in successful information security management is the effective compliance of security policies and proper integration of "people", "processes" and "technology". When it comes to the issue of "people", this effectiveness can be achieved through several mechanisms, one of which is the security awareness training of employees." "Effective countermeasures, technologies, solutions usually exist for many of these breaches and related threats, but in most of cases they are neither correctly nor effectively deployed. This is due to the fact that technology alone cannot deal with all information security risks, and the people in the organisations are actually the primary and the most critical line of defence."
Additional note.	
29	**Data extracted from (Kankanhalli et al. 2003)**
Reference	Kankanhalli, A. et al., 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), pp.139–154. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0268401202001056 [Accessed May 26, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Information Technology** "Organisations are increasingly relying on information systems (IS) to enhance business operations, facilitate management decision-making, and deploy business strategies. The dependence has increased in current business environments where a variety of transactions involving trading of goods and services are accomplished electronically." **Effectiveness of Information Security** "By offering a theoretical basis for empirical results, this study advances a theory on IS security effectiveness that informs IS managers about what kinds of IS security measures may be more effective and what types of organisations need to pay more attention on IS security."
Additional note.	
30	**Data extracted from (Fung et al. 2003)**
Reference	Fung, a. R.W., Farn, K.J. & Lin, A.C., 2003. Paper: A study on the certification of the information security management systems. *Computer Standards and Interfaces*, 25(5), pp.447–461. Available at: http://linkinghub.elsevier.com/retrieve/pii/S092054890300014X [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Standards and Issue of Incomplete Information** "Current reliable strategies for information security are all chosen using incomplete information. With standards, problems resulting from incomplete information can be reduced, since the standards, we can decrease the choices and simplify the process for reliable supply and demand decision making."

Additional note.	The study discusses evaluation of information security.
31	**Data extracted from (Park et al. 2010)**
Reference	Park, S., Ahmad, A. & Ruighaver, A., 2010. Factors Influencing the Implementation of Information Systems Security Strategies in Organizations. In *Information Science and Applications (ICISA), 2010 International Conference on*. IEEE, p. 6.
Study type Journal/ Conference/ book	Conference
Data that address the research questions	**Information Security is not Techno-Centric** "Recent surveys report that over 97% of the users of various organisations have installed anti-virus software, and more than 80% are using firewalls. According to the same survey, over 60% of users employ intrusion detection systems, encryption mechanisms, anti-spyware software, and patch management systems. Despite these measures, reports also point out that organisations have experienced (targeted) attacks continuously and that threats are increasing, and security is getting harder to manage… Information systems security (ISS) in the real world is believed to have a high tendency of failure when approached from a technology-centric perspective and is strongly influenced by organisational imperatives and constraints within which security measures have to be implemented." **Factors Influencing the Selection of Information Security Strategy** A. Economic Factors and Requirements 1. Cost 2. Time B. Organisational Factors and Requirements 1. Alignment 2. Balance 3. Effectiveness C. Structural Factors and Requirements 1. Multiplicity 2. Modularity 3. Coupling D. Operational Factors and Requirements 1. Dynamic Nature and Agility E. Technological Factors and Requirements 1. Ease of implementation F. Environmental factors and Requirements 1. Situation change and speed of change
Additional note.	This paper addresses the identification and classification of factors that influence implementation of security strategies in organisations.
32	**Data extracted from (Mohapatra & Singh 2012)**
Reference	Mohapatra, S. & Singh, R.P., 2012. *Information Strategy Design and Practices*, New York: Springer-Verlag. Available at: http://link.springer.com/10.1007/978-1-4614-2428-4.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Benefits of Information Technology (pp.4-8)** Speed and distance, data storage and manipulation, communication, control and scalability, cost benefit, record keeping and analysis, multimedia and animation, research and simulation, integration and collaboration, regulatory compliance, knowledge management and learning. **Security and Privacy (pp.45-46)** "This is vital function. Right strategy and implementation only can control and release information access. CIOs must create infrastructure, structure and policies to manage it,

as lapses could lead to information leakage, misinterpretation, loss of confidence and some embarrassing moment for the government. There are many federal as well as local acts such as Federal Information Security Management Act (FISMA), The Privacy Act of 1974, E-Government Act of 2002, Health Insurance Portability and Accountability Act (HIPAA), Data Accountability and Trust Act (DATA) - HR 221 in USA that are to be aided by. Every government has somewhat similar acts, which govern the data access and control practices."

Security Strategy (pp.103-107)

Growth of Information Technology and Growing Information Security Concerns

"IT facilitates more collaboration and reach to users, customers, and partners. More we reach to people and more we promote "anywhere - anytime" information, more we need security. As businesses are capitalising internet and collaboration across organisational boundaries for mission-critical communications and business operations, serious security risks are proliferating. The information network grows porous and need structured approach to manage security risk. The technology and its components have not only increased features for improved business services but also made the security management more complex. In today's context Security has become even more relevant because of the following, which have increased vulnerability.

- Business data may be hosted out of premises
- Business systems are being developed and implemented by external parties
- System access and connectivity is required to and from outside
- System administration are being performed remotely
- Disaster data backup or fall-back sites are out locations
- Working environment and miniaturised data storages have increase chances of data leakage
- presence of malware such as VIRUS, Phishing, Trojan, SPAM
- Motivated Hackers

Security breaches do not happen always from external interface and external parties. Many a time, the threat is generated inside, when the business internal people leak and sell the information. Earlier, the disposal of printed reports and documents also used to be hazardous practice. Applying security with these authorised users is more difficult than the outsiders. The explosion of information network, messaging systems such as email, Blogs, and IM, and wireless networking, usage of common equipment such as laptop and mobiles inside organisation and outside, and USB storage devices have made the protection of critical enterprise data even more difficult.

Information Security Strategy

"Security does not mean hiding information from everyone, rather it means access to authorised person, process, and business entities only. The entity covers person, process, and other inter and intra-business actors such as web-services and soft connections which take out information with no further control. To achieve security objective, the entity looking for access must be identified and authenticated to be true to its introduction and then as per the organisation policy its authorisation and entitlement are enforced. No resource should be accessible beyond the authorised limit. This requires well defined security policy, which must categorise the entities likely to access the resource and accordingly the policy is defined and implemented. Since entities represent at individual level, group level, class and category level; and each can have varying access permission, a security policy could have layered structure with clear guidance on order of precedence. Even permissions for an entity can differ based on time, location, assignments, access mode and other dimensions, the policy guidance must address different possibilities and respective authorisations.

The strategy for security need to be designed at the following three levels

- Network Communication
- Application and Data centre
- Administrator and Users

and they must be made compatible and complimenting to each other. These must be validated with respect to information at rest, in use, in motion and in archive.

… The security solution cannot be just by technology. The security framework has multi-layered approach. The layered approach to address security need is applied to information, application and technology components. One must consider people, process

	and technology to have comprehensive and cost-effective security. … Some of the good aspects for an effective strategy are: • Maintaining good physical security • Auditing of service providers' processes, practices and installations • Keeping record of all the accesses to vital information and tracking the privileged users such as server, system and database administrators • Tracking mass data transfers and attempts to unauthorised commands • Disabling local copy devices in user machines • Implementing and enforcing regular update of malware control application in network and on such machines and devices entrusted for such malefic access An effective strategy demands good policy, information classification, setting right infrastructure, having intelligent workflow for discovery, monitoring, reviewing & auditing, reporting and demonstrating severe punishments to culprits. Therefore, security strategy influences technology, bill of material and overall technology architecture, hence, need attention of the organization as well as CIO." **Metrics and Measurement 151** **Goals of Information Technology in UK (p.274)** "The goal of the project is to improve the quality and reduce the cost of healthcare in the UK through an integrated patient health record on a national scale. To achieve this goal, the NHS has begun a process to install a comprehensive, integrated, and standardised portfolio of clinical and administrative IT systems for the NHS-affiliated healthcare providers (hospitals, clinics, primary care practices, and other allied healthcare delivery organisations) in each of five health regions (or "clusters") into which the NHS divides its services." **Challenges to Achieve Healthcare IT Objectives** Healthcare industry is faced with challenges such as increased government regulations, E-Business challenges rising patient expectations and demand for lower healthcare costs. All of these factors must be taken into account while developing the IT Strategy."
Additional note.	
33	**Data extracted from (Höne & Eloff 2002)**
Reference	Höne, K. & Eloff, J.H.P., 2002. Information security policy — what do international information security standards say? *Computers & Security*, 21(5), pp.402–409.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Elements of an Information Security Policy/Strategy** • Need for and Scope of Information Security • Objectives of Information Security • Definition of Information Security • Management Commitment to Information Security • Approval of Information Security Policy (Signature) • Purpose or Objective of the Information Security Policy • Information Security Principles • Roles and Responsibilities • Information Security Policy Violations and Disciplinary Action • Monitoring and Review • User Declaration and Acknowledgement • Cross References • General Elements (the authors, date of policy, review date of policy)
Additional note.	
34	**Data extracted from (Andress 2003)**

Reference	Andress, A., 2003. *Surviving Security: How to Integrate People, Process, and Technology* 2nd Editio., Auerbach Publications.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Information Security** • The Importance of an effective security infrastructure • People, processes, and technology • Types of Attacks (denial of service, buffer overflows, SYN attack, teardrop attack, intrusion attacks, information theft attacks) • Types of attackers (Hackers, crackers, script kiddies, malicious insiders, industrial espionage) **Security Policies and Procedures Development, Enforcement and Monitoring Security Audits (pp.373-387)**
Additional note.	The study analyses different aspects of information security and information security strategy.
35	**Data extracted from (Tipton & Krause 2004)**
Reference	Tipton, H.F. & Krause, M., 2004. *Information Security Management Handbook, Sixth Edition*, Auerbach Publications. Available at: http://www.amazon.com/Information-Security-Management-Handbook-Sixth/dp/1420090925.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Methods of Attacks (pp.162-240)** **Information Law (pp.2321-2380)**
Additional note.	
36	**Data extracted from (Mintzberg 1978)**
Reference	Mintzberg, H., 1978. Patterns in Strategy Formation. *Management Science*, 24(9), pp.934–948.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Strategy** "A deliberate conscious set of guidelines that determines decisions into the future."
Additional note.	
37	**Data extracted from (Lukasik 2011)**
Reference	Lukasik, S.J., 2011. Protecting users of the cyber commons. *Communications of the ACM*, 54(9), pp.1–8.
Study type Journal/ Conference/ book	Journal
Data that address the research	**Information Security - Social Side** "Are computer vulnerabilities growing faster than measures to reduce them? Perhaps the problem is not purely a technical matter, but more to do with users. Carelessness in

questions	protecting oneself, tolerance of bug-filled software, vendors selling inadequately tested products, or the unappreciated complexity of network connectivity have led today's abuse of the common [people]."
Additional note.	
38	**Data extracted from (Kulmala 2007)**
Reference	Kulmala, P., 2007. *Evaluation of information service information security*,
Study type Journal/ Conference/ book	Report
Data that address the research questions	**Evaluation of requirements and implementation** The evaluations of the information security requirements and implementation of information services is carried out by inspections and analyses of the design and implementation documents and code. The evaluations check that all identified and essential threats are observed both in the requirement definitions and in implementation. Evaluations can also utilise existing directives and reference check lists. The ISO 17799 (BS 7799) standard [11] defines the directive for the management of total information security. The standard consists of ten sub-areas: 1. Security policy 2. Security organization 3. Assets classification and control 4. Personnel security 5. Physical and environmental security 6. Computer and network management 7. System access control 8. Systems development and maintenance 9. Business continuity planning 10. Compliance Other information security management evaluation standards are: • SSE-CMM (Systems Security Engineering Capability Maturity Model, ISO/IEC 21827) standard defines and specifies the evaluation of information security process maturity. • INFOSEC IA-CMM • IS Program Maturity Grid • Murine-Carpenter SW Security Metrics
Additional note.	The study offers best practices and methods for information security evaluation.
39	**Data extracted from (Mohammad 2010)**
Reference	Mohammad, Y.M., 2010. *Information scurity strategy in telemedicine and e-Health systems [electronic resource] : A case of England's shared electronic health record system*. Brunel University.
Study type Journal/ Conference/ book	PhD Thesis
Data that address the research questions	**Benefits of Electronic Healthcare Records** The electronic patient record system offers an improved access to patient-specific information and provides a major benefit for the quality of healthcare and for the quality of life of clinicians in practice. The new communication technologies offer clinicians creative ways to interact with their patients and to provide higher quality care. **Concerns of Information Security for Electronic Healthcare Records** "With shared health records, the accuracy and accessibility do increase, but potential

	threats to confidentiality and patient privacy are more controversial." "… 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." (According to Shortliffe and Fagan 2000, citied in Mohammad 2010) Standards are needed in the area of clinical terminology, there are concerns about data privacy, confidentiality, and security, challenge of data entry by physicians, and difficulties related to integration of record systems with other information and data in healthcare settings. **Consent Mechanisms and Privacy** is also a challenge for EHRs. Some kinds of consent include informed, implied, express, general consent with specific denials, and general denial with specific consent. Other challenges/concerns include right access control and data accuracy. **Information Security Requirements of Electronic Healthcare Records** "From patient's perspective, confidentiality is essential to the patient-physician relationship. 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 part of the record they need or are allowed to access. [quality and efficiency are also expected and therefore required by the patients]… 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." **Information Security** "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 (Laden et. al., 2006 cited in Mohammad 2010). Information security involves the use of physical and logical data access controls to ensure the proper use of data and to prevent unauthorised 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 cited in Mohammad 2010)." **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. **Confidentiality:** is the privacy interests that arise from specific relationship (e.g. doctor/patient, researcher/subject) and corresponding legal and ethical duties (Boulos et. al., 2009 and US CDC Public Health Law 101 cited in Mohammad 2010). It refers to the property that information is not made available or disclosed to unauthorised individuals, entities, or processes (Gerber et. al., 2001 cited in Mohammad 2010) ensuring that information is accessible only to those authorised to have access (Laden et. al., 2006). **Integrity** is the property that data have not been altered or destroyed in an unauthorised manner (Gerber et. al., 2001 cited in Mohammad 2010) ensuring that information is accurate and complete in storage and transport; that is correctly processed. **Availability** is "the property of being accessible and usable upon demand by an authorised entity" (ISO/IEC TR 13335-1, 1996, p.5 cited in Mohammad 2010) ensuring that information is available to those who are authorised to have it, when and where they should have it." **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… Privacy in health sector is the individual's right to control the acquisition, use, and disclosure of their identifiable health information. **Audit-ability** (usually called accountability), it is the ability of investigation, which ensures that the actions of an entity may be traced uniquely to the entity (Gerber et. at. 2001 cited in Mohammad 2010). **Authenticity** is the property that ensures that the identity of a subject or resource is the one claimed.

	Strategy 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 organisations as instruments for collective perception and action. **Policy** 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 provide overall direction to the organisation. **Standard** 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. **Information Security Strategy** Information security strategy is the roadmap for the foreseeable future and details how the organisation intends to progress along the path of maturity. It is a plan to prevent or minimise risks while complying with legal, statutory, contractual, and internally developed requirements (FFIEC 1998 and Wylder 2004 cited in Mohammad 2010). **Information Security Policy** Information security strategy 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. **Baseline** 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. **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 systms and procedures. **Guideline** 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.
Additional note.	
40	**Data extracted from (Saleh et al. 2007)**
Reference	Saleh, M.S., Alrabiah, A. & Bakry, S.H., 2007. Using ISO 17799: 2005 information security management: A STOPE view with six sigma approach. *International Journal of Network Management*, 17(1), pp.85–97. Available at: http://onlinelibrary.wiley.com/doi/10.1002/nem.616/abstract.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**STOPE** (strategy, technology, organisation, people, and environment) Approach **DMAIC** (define, measure, analyse, improve, and control) approach **Strategy and Strategic Objectives** The strategic objective of ISO/IEC 17799: 2005 is stated as follows: 'to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations'. The required response to this main objective is expressed in terms of the following two controls:

	- 'An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.' - 'The information security policy should be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness.' **Requirements of a strategy** The strategy must consider: relevant laws and regulations, business requirements, employees of the organisation, external parties, continuous attention. **Strategy** includes information security policy **Technology** includes Communications and operations management, access control, information systems acquisition, and development and maintenance. **Organisation** includes Organisation of information security, asset management, information security incident management, and Business continuity management. **People** comprise human resources security **Environment** Physical and environmental security, and compliance.
Additional note.	
41	**Data extracted from (Linden et al. 2009)**
Reference	Linden, H. van der et al., 2009. Inter-organizational future proof EHR systems. A review of the security and privacy related issues. *International Journal of Medical Informatics*, 78(3), pp.141–160. Available at: http://www.ncbi.nlm.nih.gov/pubmed/18760661 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security/ Privacy Concerns of Electronic Healthcare Records** Electronic healthcare records are generally develop and used for local usage. Information in healthcare has to be generally stored and needed for a very long time i.e. lifetime of a patient and with an intention to integrate EHRs to communicate with external partners such as other healthcare organisations. Information security and privacy concerns may increase due to the increase in total number of users, increase in the need for record sharing, and evolution of clinical structure, organisation and structure. "These challenges require a generic interface that can comply with these changes, and mechanisms to find the location of the requested data. "Security and privacy related issues are more important in such an environment than in the current systems. For example, in the current situation access rights are defined locally, based on formal or less formal rules of the house. When dealing with access from outside the situation may ask for different requirements. In the current situation, outsiders can only have access to patient data through human intermediation, often the treating physician; she may act as a filter on what is communicated taking the patient wishes [and interests] into account. In a fully digital communication patient's wishes regarding disclosure of information have to be respected as well."
Additional note.	
42	**Data extracted from (Reni et al. 2004)**
Reference	Reni, G. et al., 2004. Chief medical officer actions on information security in an Italian rehabilitation centre. *International Journal of Medical Informatics*, 73(3), pp.271–279. Available at: http://www.ncbi.nlm.nih.gov/pubmed/15066558 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research	**Information Security/Privacy Concerns of Electronic Healthcare Records** "Local push to high priority [security] arose from several concurrent forces, like privacy both on the patient and on doctor side, legal and ethical aspects. Recommendations on

questions	the protection of medical data require appropriate technical and organisational measures to be taken to protect personal data against unauthorised access, alterations, or any other form of inappropriate processing. In the same time quick and easy access to patient information should be granted to authorised personnel to ensure proper and in time treatment of patients."
Additional note.	
43	**Data extracted from (Chi et al. 2008)**
Reference	Chi, H., Jones, E.L. & Zhao, L., 2008. Implementation of a security access control model for inter-organizational healthcare information systems. In *Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008*. Ieee, pp. 692–696. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4780754 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Conference
Data that address the research questions	**Concerns about Electronic Healthcare Records** "The inability to share information across systems is just one of the major impediments in the healthcare business that hinders progress towards efficiency and cost effectiveness."
Additional note.	
44	**Data extracted from (Liu et al. 2011)**
Reference	Liu, M., Fu, G. & Jing, J., 2011. eHCBAC: Flexible column based access control for electronic healthcare systems. In *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*. Ieee, pp. 745–750. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120890 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Conference
Data that address the research questions	**Benefits of Electronic Healthcare Records** "An electronic healthcare (e-Health) system is a database system that collects patients' medical data from participating organisations such as hospitals, clinics and insurance companies, and facilitate services for these organisations." "E-Health system provides electronic medical data sharing between different providers, in order to satisfy their diverse medical needs. It remedies the inconvenience of conventional healthcare data sharing, and makes great savings in terms of efficiency and cost." **Concerns about Electronic Healthcare Records** Though e-Health system transforms healthcare services with great savings in terms of efficiency and cost, it also triggers great privacy concerns as all patients' data are maintained in a centralised system which may be accessed and misused by unauthorised parties." "A major concern over patient's privacy is how to protect electronic health data when the data are increasingly passed around and accessed by a large number of people such as doctors, nurses, technicians, and researchers." "One countermeasure is access control which requires that only authorised entities or users with a legitimate request satisfying related policies or laws can access sensitive information."
Additional note.	

45	Data extracted from (Tzelepi et al. 2002)
Reference	Tzelepi, S., Pangalos, G. & Nikolacopoulou, G., 2002. Security of medical multimedia. *Medical informatics and the Internet in medicine*, 27(3), pp.169–184.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Concerns of IT in Healthcare** "The application of information technology to healthcare has generated growing concern about the privacy and security of medical information. As healthcare organisations collect, process, and store more health information in computerised form and use both private and public telecommunications systems to transmit this information between different entities, they must ensure that adequate mechanisms are in place to protect the information." **General Information Security Requirements for Medical Data** • Limited access to multimedia medical data is indicated for several reasons. Patient privacy, medical ethics, and simple good business sense. Patients have an expectation that their medical records and information will be, in general kept in confidence. This expectation may, in some jurisdictions, be codified in law; in any case, lawsuits for failure to preserve the confidentiality of medical information are a real threat. Moreover, even if there are no legal ramifications, a hospital or clinic that gains a reputation of having a cavalier attitude towards, or being careless with the personal information of its patients runs the real risk of losing business to competitors. • Protection of Data against Unauthorised disclosure is also required for several reasons. As is with the case with limiting access to medical data, issues of privacy, medical ethics, and good business sense are all considerations in this case. • Positive detection of data corruption is required for reasons of patients' safety. If a medical image or a stored patient information has been corrected, either by chance, accident, or malicious alteration, it must be detectable. Otherwise, it is possible that a patient will receive inappropriate and potentially fatal medical treatment. • Positive Binding Between Patient Data and Other Data is also required for reasons of patient safety. Medical images and related consultations are often the basis for decisions regarding surgery or other potentially health - or - life threatening medical procedures. There must be a mechanism to ensure a positive, detectable binding between patient identification information and the other information stored on the system. Otherwise the potential exists for patients to receive medical care that is based on the medical image/information of someone else, with potentially fatal or serious results. • Protection against data corruption is required for both economic and patient health and safety reasons. While it is preferable to re-image a patient if an image has become corrupted, this should be avoided if possible. Re-imaging a patient is costly, occupies diagnostic equipment, and is inconvenient for the patient. • Protection of information against unauthorised distribution and illegal copies is required to protect intellectual property and content continuity from unauthorised use, misappropriation and misrepresentation. • The desirability of an audit trail is essentially an internal multimedia medical data base system issues. A positive audit trail of system resource usage, patient information access, etc. is a key element in providing the other requirements detailed above. It is also invaluable in determining the extent of possible damage and the critical details (how, what, who) in the event that a security incident occurs.
Additional note.	
46	**Data extracted from (Gritzalis & Lambrinoudakis 2000)**
Reference	Gritzalis, D. & Lambrinoudakis, C., 2000. A data protection scheme for a remote vital signs monitoring healthcare service. *Medical informatics and the Internet in medicine*, 25(3), pp.207–224.

Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security in Healthcare** Personal and medical data processed by Healthcare Information Systems must be protected against unauthorised access, modification, and withholding. Security measures should be selected to provide the required level of protection in a cost-efficient manner.
Additional note.	The study offers an evaluation approach for healthcare.
47	**Data extracted from (Stewart 2003)**
Reference	Stewart, R., 2003. *A Case Study of Alberta Wellnet's Treatment of Privacy in Implementing Electronic Health Records*. DALHOUSIE UNIVERSITY.
Study type Journal/ Conference/ book	Thesis
Data that address the research questions	**Benefits of Electronic Healthcare Record** • Efficient treatment of patients, • Helping patients to make informed choices by giving them control over their own health information to limit or grant access to their medical information which is perceived as private and personal. • Helping Doctors to make informed/better decisions • Doctors can share X-rays, blood test and other diagnostic tools quickly and efficiently - eliminating the need to repeat tests. • Doctors can consult with one another with more ease thus saving time and cost for patient's treatment. • Public health officials can more effectively track and manage "population health" issues. • Health administrators can make better decisions about how to manage the health system
Additional note.	
48	**Data extracted from (Abraham et al. 2011)**
Reference	Abraham, C., Nishihara, E. & Akiyama, M., 2011. Transforming healthcare with information technology in Japan: A review of policy, people, and progress. *International Journal of Medical Informatics*, 80(3), pp.157–170. Available at: http://dx.doi.org/10.1016/j.ijmedinf.2011.01.002.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Issues/Concerns about Electronic Healthcare Records** "Transforming healthcare with HIT requires committed governmental policy, a willingness of providers and patients to adopt the technology, and the promotion of progress towards meeting societal challenges in healthcare delivery."
Additional note.	
49	**Data extracted from (Safran et al. 2007)**
Reference	Safran, C. et al., 2007. Toward a national framework for the secondary use of health data: an American Medical Informatics Association white paper. *Journal of the American Medical Informatics Association*, 14(1), p.1. Available at: http://jamia.bmj.com/content/14/1/1.short.

Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Use of Secondary Health Data** Secondary use of health data applies personal health information (PHI) for uses outside of direct healthcare delivery. It includes such activities as analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, marketing, and other business applications, including strictly commercial activities. Secondary use of health data can enhance healthcare experiences for individuals, expand knowledge about disease and appropriate treatments, strengthen understanding about effectiveness and efficiency of healthcare systems, support public health and security goals and aid business in meeting customers' needs.
Additional note.	
50	**Data extracted from (Shoniregun et al. 2010)**
Reference	Shoniregun, C.A., Dube, K. & Mtenzi, F., 2010. *Electronic healthcare information security*, London: Springer Science+Business Media.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Concerns Regarding Information Security of Electronic Healthcare Records** "The adoption of Information and Communication Technologies (ICT) in healthcare is driven by the need to contain costs while maximising quality and efficiency. However, ICT adoption for healthcare information management has brought far reaching effects and implications on the spirit of the Hippocratic Oath, patient privacy and confidentiality." **The Approach to Securing e-Healthcare Information [pp.135-137]** **The Framework for Securing e-Healthcare Information Security and Privacy [pp.137]** • **The Key Drivers to the Security and Privacy of e-Healthcare Information Security [pp.138-139]** • **The Model for the e-Healthcare Information Control and Security and Privacy Risk Level Over Time [pp.140-143]:** period 1: The immediate past - absolute control by the clinician or healthcare organisation. Period 2 and 3A: The present - transition to patient control. Periods 3B and 4: The immediate future - balancing professional requirements with patient privacy. • **The Conceptual Framework for Secure e-Health Information [pp.144-146]** • **The Conceptual Architecture [pp.146-148]**
Additional note.	The study also offers an evaluation approach.
51	**Data extracted from (Häyrinen et al. 2008)**
Reference	Häyrinen, K., Saranto, K. & Nykänen, P., 2008. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*, 77(5), pp.291–304.
Study type Journal/ Conference/ book	Journal
Data that address the research question	**Definition, Structure, Content, Use and Impacts of Electronic Health Records** Where is the EHR used? Health services are organised in different ways in different countries, but most typically they are divided between primary, secondary and tertiary care. Primary care is health care provided in the community by the staff of a general practice. Secondary care is medical attention provided by a specialist facility upon referral by a primary care physician, and tertiary care is provided by a team of specialists in a major hospital [110].

	The context of the studies is represented. A few of the studies were concerned with self-monitoring. The patients in their homes (n=5). Nine of the studies were con- ducted in more than one organisation, for example in two hospitals in one context. Users of the EHR system The EHR is used by different health care professionals and also by administrative staff. Among the various health care professionals who use different components of the EHR are physicians, nurses, radiologists, pharmacists, laboratory technicians and radiographers. Furthermore, EHRs are also used by patients or their parents
Additional note.	
52	**Data extracted from (NHS 2010)**
Reference	NHS, 2010. NHS Summary Care Record - your emergency care record., (September).
Study type Journal/ Conference/ book	Leaflet
Data that address the research questions	**Benefits of Electronic Healthcare Records** "Today, records are kept in all the places where you receive care. These places can usually only share information from your records by letter, email, fax or phone. At, times this can slowdown treatment and sometimes information can be hard to access. "We are introducing Summary Care Records to improve the safety and quality of patient care. Because the Summary Care Record is an electronic record it will give healthcare staff faster, easier access to essential information about you, to help provide you with safe treatment when you need care in an emergency or when your GP practice is closed." • "Healthcare staff will have quicker access to information about any medicines you are taking, allergies you suffer from and any bad reactions to medicines you have had". • "This means they can provide you with safer care during an emergency, when your GP practice is closed or when you are away from home in another part of England." • Patients will have more control on their medical information as healthcare staff directly involved with patient's treatment can see the Summary Care Records, but only after authorised through NHS Smartcard with a chip and passcode. Staff will look at only the information which they need to do their job and will record their information. • "Healthcare staff will ask your permission every time they need to look at your Summary Care Record. If they cannot ask you, for example if you are unconscious … healthcare staff may look at your record without asking you. If they have to do this, they will make a note on your record." **Protection of Confidentiality and Informed Consent** "By law, everyone working with us or on our behalf must respect your confidentiality and keep all information about you secure. We publish the NHS Care Record Guarantee for England. This says how the NHS will collect, store, and allow access to your electronic records and your choices for how your information is stored and looked at." **Consent and Choices** • "You can choose to have a Summary Care Record: you do not need to do anything. This will happen automatically. • You can choose not to have a Summary Care Record: you need to let your GP practice know by filling in and returning an opt-out-form."
Additional note.	
53	**Data extracted from (Takeda et al. 2000)**
Reference	Takeda, H. et al., 2000. Architecture for networked electronic patient record systems. In *International Journal of Medical Informatics*. pp. 161–167.

Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of Electronic Healthcare Records** "A networked electronic patient record (EPR) system should ensure that such information can be used, shared, and exchanged between clinicians of all disciplines, across all sectors of healthcare, different countries and different models of healthcare and healthcare delivery. It should also support secondary uses such as clinical research, population health, health administration, financing, and health service planning."
Additional note.	
54	**Data extracted from (ISO 27799:2008 2008)**
Reference	ISO 27799:2008, 2008. *Health informatics — Information security management in health using ISO / IEC 27002*, London: British Standards Institution.
Study type Journal/ Conference/ book	Standard
Data that address the research questions	**Health Information Security Goals** "Maintaining information confidentiality, availability, and integrity (including authenticity, accountability, and auditability) are the overarching goals of information security. In healthcare, privacy of subjects or care dependents upon maintaining the confidentiality of personal health information. To maintain confidentiality, measures must also be taken to maintain the integrity of data, if for no other reason then it is possible to corrupt the integrity of access control data, audit trails, and other system data in ways that allow breaches in confidentiality to take place or to go unnoticed. In addition, patient safety depends upon maintaining the integrity of personal health information; failure to do this can also result in illness, injury, or even death. Likewise, a high level of availability is essentially important attribute of health systems, where treatment is often time-critical. Indeed, disasters that could lead to outages in other non-health related IT systems may be they very times when the information contained in health systems is most critically needed. Moreover, denial of service attacks against networked systems are increasingly common. The controls discussed in Clause 7 are those identified as appropriate in healthcare to protect confidentiality, integrity and availability of personal health information and to ensure the access to such information can be audited and accounted for. These controls help to prevent errors in medical practice that might ensue from failure to maintain the integrity of health information. In addition, they help to ensure that the continuity of medical services is maintained. There are additional considerations that shape goals of health information security. They include: a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care's right to privacy. b) maintaining established privacy and security best practices in health informatics. c) maintaining individual and organisational accountability among health organisations and health professionals. d) Supporting the implementation of systematic risk management within health organisations. e) meeting the security needs identified in common healthcare situations f) reducing operating cost by facilitating the increased use of technology in a safe, secure, and well managed manner that supports - but does not constrain - current health activities. g) maintaining public trust in health organisations and the information systems these organisations rely upon; h) maintaining professional standards and ethics as established by health-related professional organisations (insofar as information security maintains the confidentiality and integrity of health information).

	i) operating electronic health information systems in an environment appropriately secured against threats. j) facilitating interoperability among health systems, since health information increasingly flows among organisations and across jurisdictional boundaries (especially as such interoperability enhances the proper handling of health information to ensure its continued confidentiality, integrity, and availability)." **Health Information to be Protected** a) personal health information b) pseudonymized data derived from personal health information via some methodology for pseudonymous identification. c) statistical and research data, including anonymized data derived from personal health information my removal of personality identifying data; d) clinical/medical knowledge not related to any specific subjects of care, including clinical decision support data (e.g. data on adverse drug reactions). e) data on health professionals, staff and volunteers f) information related to public health surveillance; g) audit trail data, produced by health information systems that contain personal health information, pseudonymous data derived from personal health information, or that, contain data about the actions of users with regard to personal health information. h) system security data for health information systems, including access control data and other security-related system configuration dta for health information systems. The extent to which confidentiality, integrity, and availability need to be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed. For example, statistical data [c)above] may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data [g) above may not require high availability (frequent archiving with a retrieval time measured in hours rather than seconds might suffice in a given application) but its content might be highly confidential. Risk assessment can properly determine the level of effort needed to protect confidentiality, integrity, and availability (see 6.4.4). The result of regular risk assessment must be fitted to the priorities and resources of the implementing organisation.
Additional note.	
55	**Data extracted from (DH/Digital Information Policy 2007)**
Reference	DH/Digital Information Policy, 2007. *Information Security Management: NHS Code of Practice*, Available at: http://svn.tools.ietf.org/html/rfc1158\nhttp://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/securitycode.pdf.
Study type Journal/ Conference/ book	Code of Practice
Data that address the research questions	**Legal and Professional Obligations (Requirements)** 17. "The statutory requirements for NHS compliance with information security management principles is the Data Protection Act 1998, and in particular its seventh principle. The Act provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer. It applies to personal information generally, not just to health records, and therefore the same principles apply to record of employees held by employers, for example in finance, human resources and occupational health departments. 18. Other applicable legislation relating to information and the information security management function shall be contained within additional guidance to be provided under separate cover and that shall relate to the NHS Information Governance function generally. Additionally, clinicians are under a duty to meet information security management standards set by their professional regulatory bodies."

Additional note.	
56	**Data extracted from (Gaunt 1998)**
Reference	Gaunt, N., 1998. Installing an appropriate information security policy. *International Journal of Medical Informatics*, 49(1), pp.131–134.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Issues related to Information Security of Healthcare** "Security of personal healthcare is of concern to patients, healthcare staff, and informaticians. Nevertheless, their awareness of the appropriate measures for protection of such data have been found wanting. The development and implementation of an information and security policy in the healthcare environment must therefore take into account the attitudes of staff and their educational needs."
Additional note.	The study details the process, development, and implementation of Information security policy/strategy for a healthcare organisation in UK. The study finds that relevant **training and awareness** programs are required to promote the security culture within healthcare organisations.
57	**Data extracted from (Meingast et al. 2006)**
Reference	Meingast, M., Roosta, T. & Sastry, S., 2006. Security and privacy issues with health care information technology. In *28th Annual International Conference of the IEEE*. IEEE, pp. 5453–5458.
Study type Journal/ Conference/ book	
Data that address the research questions	**Issues/Concerns Related to Information Security in Healthcare** "While there are benefits to technologies, associated privacy and security issues need to be analysed to make these systems socially acceptable." **Problems of Paper Based Records/ Benefits of IT and Electronic Healthcare Records** "The healthcare system has long been plagued by problems such as diagnosis being written illegibly on paper, doctors not being able to easily access patient information, and limitations on time, space, and personnel for monitoring patients. With advancements in technology, opportunities exist to improve the current state of healthcare to minimise some of these problems and provide more personalised service." "… With healthcare organisations transitioning to EPRs, information that was once stored in paper format will now be stored electronically allowing for easy accessibility and use." … After having appropriate level of standardisation "medical records can be stored electronically and be instantly sent anywhere in the world." … Some advanced healthcare sites in the USA "provide a set of individualised services to allow patients access to their clinical laboratory results and other components of the electronic patient records. These services have previously been available only to physicians and other healthcare providers." "Sensor network is another technology that is being adopted." "Electronic patient records take the current paper-based documents and convert them to a digital format so they are available electronically. The records include different types of data, such as physician's notes, MRIs, and clinical lab results. Using EPRs allows real-time access to healthcare records independent of the physical location of the user. Physicians, nurses, insurance companies, and patients can all access the records over the internet. EPRs reduce the number of errors due to illegibility and inconsistency of terms. In addition, electronic records can be backed up more easily than paper-based records which prevents data loss. **Privacy and Security Issues** "…Both industry and academic institutions are developing sensor systems for remote patient monitoring. … these technologies will provide many benefits for healthcare

	delivery, yet there are number of security and privacy implications that must be explored in order to promote and maintain fundamental **medical ethical principles** and **social expectations**. These issues include access rights to data, how and when data is stored, security of data transfer, data analysis rights, and the governing policies. While there are current regulations for medical data, these must be re-evaluated as an adaption of new technology changes how healthcare delivery is done." "While the [new IT technologies] can help improve overall quality of healthcare delivery, the benefits of these technologies must be balanced with the privacy and security concerns of the user." **a. Data access and storage**: "There has long been concern over a patient's health record privacy and confidentiality. Connecting personal health information to the internet exposes this data to more hostile attacks compared to the paper based medical records." … "Once this information is available electronically, it opens the door for hackers and other malicious attackers to access the records as well as those who are authorised. • **Who owns the data?** • **What type of data, and how much data should be stored?** • **Where should the health data be stored?** • **Who can view a patient's medical record?** • **To whom this information be disclosed to without the patient's consent?** **B. Data Mining:** "From mining on medical data, one may be able to categorise and profile patients based on numerous factors such as age, gender, or disease. This may lead to discriminatory and exclusionary effects. As this data becomes a more of a "commodity" that can be passed over the Internet and collected, it is important that anonymity of data happens before any data mining takes place. The question of what anonymity entails and regulations for data disclosures to users, such as managed care evaluators and insurance companies, all must be answered in terms of data mining." **C. Conflicting Regulatory Framework:** "There are currently many different regulations and rules surrounding healthcare including the Federal Regulations of The American Health Insurance Portability and Accountability Act (HIPAA) as well as various state regulations. … HIPAA is a set of rules to be followed by doctors, hospitals, and other healthcare providers. HIPAA's goal is to ensure that all medical records, medical billing, and patient accounts meet certain consistent standards with regards to documentation, handling, and privacy. Moreover, HIPAA requires that all patients be able to access their own medical records, correct errors or omissions, and be informed how their personal information is shared or used. Other provisions of HIPAA include notification of privacy procedures to the patients. **D. Solutions** • **Role-based access control or role-based security** • **Encryption** • **Authentication mechanisms**
Additional note.	
58	**Data extracted from (Otieno et al. 2008)**
Reference	Otieno, G.O. et al., 2008. Measuring effectiveness of electronic medical records systems: Towards building a composite index for benchmarking hospitals. *International Journal of Medical Informatics*, 77(10), pp.657–669.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Benefits of EHRs** "These [EHR] systems offer extraordinary opportunities to achieve the six aims of improved care including safety, effectiveness, patient centeredness, timeliness, efficiency and equity."
Additional note.	
59	**Data extracted from (Smith & Eloff 1999)**

Reference	Smith, E. & Eloff, J.H., 1999. Security in health-care information systems--current trends. *International journal of medical informatics*, 54(1), pp.39–54.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Concerns regarding EHRs** "The prospect of storing health information in electronic form raises concerns about patient privacy and data security. Any attempt to introduce computerised healthcare information systems should, therefore, guarantee adequate protection of the confidentiality and integrity of patient information. At the same time, the patient information also needs to be readily available to all authorised healthcare providers, in order to ensure the proper treatment of the patient. " "As [EHR] systems are more closely connected with clinical matters, life threatening situations may arise when and if they fail, be it owing to an accident or a deliberate attempt to compromise the system. Healthcare professionals are, therefore, increasingly dependent on the availability of computer systems, as well as reliant upon the accuracy of the data they store. While healthcare records may contain information of the utmost sensitivity, for example the HIV status of a patient, this information is only useful to the patient when shared with the healthcare providers and system under which the patient gets his/her care. The dilemma of obtaining, using, and sharing healthcare information to provide care while not breaching patient privacy, is therefore a serious concern." "The latter trend marks an ever-growing and clamant need for protecting the confidentiality and integrity of healthcare information, whilst at the same time ensuring it availability to authorised healthcare providers. However, one has to acknowledge the fact that complete protection of data is, in practice, neither feasible nor possible." "A key concern in this changed environment is that fact that enormous chunks of data will be generated electronically. It is critical, therefore, that the information thus captured be stored and maintained in a database in such a way that its integrity could be guaranteed. From a provider perspective, healthcare information is needed to analyse the outcomes and costs of different treatment plans. Simultaneously, in today's information-intensive society consumers of healthcare want to be better informed of their health options, which, in turn, necessitates ready access to all relevant healthcare information. The possibility that the user could compromise the integrity of such data, be it intentionally, inadvertently or from sheer negligence, becomes all the more real. If systems on which healthcare professionals relied in the execution of their clinical work were to fail in terms of their integrity, patients may even be incorrectly treated, with obvious and dire consequences for all parties concerned." "Securing information is shown to be more difficult to accomplish in a distributed environment than in a centralised system. On the other hand, total failure of a centralised system has by far more serious consequences than a failure in one or more elements of distributed systems. Similarly greater masses of data are in danger of abuse in a centralised system if an unauthorised person manages to break the security measures. The concept of distributed processing necessarily results in decentralisation and spread of data security concerns. Furthermore, the necessary transfer of data between the diverse elements of a distributed system also presents problems to data security. The storage of data at distributed sites causes further difficulties concerning security. In this context, the integrity of data and its protection against partial or total destruction is of major importance. there is a further problem concerning the update of data in distributed storage. This holds especially whenever data are constantly being augmented or altered - as in the case of patient data." **[Also see page 43-50 of the research paper for different information security requirements of healthcare]**
Additional note.	
60	**Data extracted from (Stahl et al. 2012)**
Reference	Stahl, B., Doherty, N. & Shaw, M., 2012. Information Security Policies In The UK Healthcare Sector: A Critical Evaluation. *Information Systems Journal*, 22(1), pp.77–94. Available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1365-2575.2011.00378.x/full.

Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Information Security Policy/Strategy** "The information security policy is viewed as an increasingly important business document which covers a broad set of security concerns."
Additional note.	
61	**Data extracted from (Tyson & Slocum 2012)**
Reference	Tyson, B.K. & Slocum, R., 2012. Healthcare Information Security. *Journal Of Healthcare Information Management*, 26(4), pp.38–43. Available at: http://www.secureworks.com/assets/pdf-store/articles/JHIM-fall-2012.pdf.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Healthcare Information Security** "Between 2009 and 2011, more than 18 million patients' Protected Health Information (PHI) was compromised. Over the past year alone, healthcare breaches in the United States have increased by 32 percent. As these numbers clearly show, securing medical information is one of the most pressing issues facing hospitals and other healthcare organisations. However, a 2012 report from the American National Standards Institute notes, a lack of resources and leadership support have made it hard for many organisations to effectively protect such data." **Internal Vs. External Threats** "Internal threats have historically been the most common, with a reported 49 percent of breaches occurring due to lost or stolen devices and laptops. The prominent media image of a healthcare breach often evokes the occasional rogue employee who steals information and sells it on the black market. In fact, most healthcare security incidents result from more mundane and unintended causes, such as the accidental loss or theft of laptop computers or mobile devices: a clinician or employee leaves a laptop or mobile device on a train during their evening commute; or a thief steal an employee's computer bag from the backseat of her car." External threats such as hackers are no less dangerous and are considered to be more systematic and intended as compared to internal threats. **Responding to the Threats** "Organisations can protect against both common and advanced threats by gaining situational awareness, and forming defensive strategies around the risk posture that exists. Although a foundation for this awareness starts with risk assessments, implementing effective network architecture, along with penetration testing and continuous monitoring are also necessary components of a security program. Planning for these events and the organisation's anticipated response on a continual basis makes it much more difficult for malware actors to conceal their actions and will make incident response efforts more effective, both for internally and externally based threats." **Data Visibility and Risk Assessments** **Mobile Device Security** **Endpoint Access and Encryption** **Data Centre and Networking Security** **Continuous monitoring**
Additional note.	
62	**Data extracted from (Thigarajan 2006)**
Reference	Thigarajan, V., 2006. Information Security Management: SANS Audit Check List. *SANS*, pp.1–43. Available at: https://www.sans.org/media/score/checklists/ISO-17799-2005.pdf.

Study type Journal/ Conference/ book	Audit Check List
Data that address the research questions	
Additional note.	SANS Audit Check List based on BS ISO/IEC 27001:2005)
63	**Data extracted from (Sunyaev 2011)**
Reference	Sunyaev, A., 2011. *Health-Care Telematics in Germany* 1st ed., Gabler Verlag. Available at: http://www.springerlink.com/index/10.1007/978-3-8349-6519-6.
Study type Journal/ Conference/ book	Book
Data that address the research questions	**Catalogue of IS Healthcare Security Characteristics [pp.53-81]** • **Legal Frame Work:** Privacy and Legal Requirements • **Protection Goals of Healthcare Information Systems:** Dependable Healthcare Information Systems (Confidentiality, Integrity, Availability) and Controllability of Healthcare Information Systems (Authenticity, Liability, Use Regulation, Accuracy, Utility, Possession, Revisability, Legal Certainty, Enforceability, Suitability for Daily Use, and Anonymity). • **Characteristics of IS Security Approaches with Respect to Healthcare:** Security Requirements for the appropriate use of information and communication technology (ICT) in public health systems on both technical and organisational level
Additional note.	
64	**Data extracted from (Papazafeiropoulou & Gandecha 2008)**
Reference	Papazafeiropoulou, A. & Gandecha, R., 2008. Interpretive flexibility along the innovation decision process of the UK NHS Care Records Service (NCRS): Insights from a local implementation case study. *IGI Global*, pp.2452–2462.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Concerns about Healthcare Information Security** "With medical errors becoming a cruel reality in the provision of healthcare worldwide, the role of information technology in preventing those errors becomes predominant. It is recognised that more people die every year due to medical errors than from vehicle accidents, breast cancer or AIDS. The American Hospital Association CDER (2004) relates the vast majority of medication errors occurring to lack of appropriate information and processes such as: • Incomplete patient information • unavailable drug information • miscommunication of drug orders due to poor handwriting, similar name drugs, misuse of zeroes and decimal points, confusion of metric and other dosing units, and inappropriate abbreviations • lack of appropriate labelling • environmental factors, such as lighting, heat, noise, and interruptions that can distract health professionals from their medical tasks. One way to reduce medical errors is to make efficient, accurate, reliable medical decisions based on reliable and up-to-date information or patient record. "
Additional note.	

65	Data extracted from (Siougle & Zorkadis 2002)
Reference	Siougle, E.S. & Zorkadis, V.C., 2002. A Model Enabling Law Compliant Privacy Protection through the Selection and Evaluation of Appropriate Security Controls. *Springer-Version*, 2437, pp.104–114. Available at: http://link.springer.com/chapter/10.1007/3-540-45831-X_8.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Legal Requirements of Information Security** Rapid adoption of information technologies by organisations has lead to "creation, collection, and processing of enormous amount of personal data. Responding to this development, international bodies, the European Union and various countries established personal data protection laws and Authorities to regulate and control their application. The legal framework imposes the taking of appropriate security measures, that may be different compared with those specified by data controllers based on their business needs, since personal data are assets with, possibly, different values for the data subjects and the controllers." Therefore, this study offers "a security control selection model, that can support data controllers to methodologically choose security controls/measures compliant to the legal requirements of privacy. The paper also offers a methodological way to assess the privacy protection requirements according to the related legal provisions and the selected and implemented security controls. **Privacy Protection Requirements** "Data subjects (users, consumers, etc) **expect** their personal data to be protected and their privacy to be respected by the organisations (data controllers) they conduct business with. On the other hand, data controllers have realised that protecting personal data and developing data subject's trust promise to become **a competitive advantage**. Thus protecting privacy has become a new business imperative. Privacy protection laws were enacted in many countries in the last three decades. They have been introduced **to regulate** the processing of personal data and to prevent what are considered to be privacy violations, such as unlawful storage or storage of inaccurate personal data and abuse and unauthorised disclosure of personal data. In addition to national data protection laws, several legal instruments related to privacy protection have been adopted at **an international level**. Among the most influential are the European Union's Directives 95/46/EC and 97/66/EC, the Council of Europe's Convention of the protection of individuals with regard to Automatic processing of Personal Data, and the OECD's guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data." "The data protection laws are based on **the principles** of lawfulness and fairness, minimality, purpose specification, accuracy, anonymity, security, individual participation, and accountability." **Security Principal Requirements** "The main security obligations are outlined in the security principle. This principle clearly defines that appropriate security measures, both technical and organisational, should be taken by the data controller for the protection of personal data against **accidental or unauthorised destruction** or accidental loss as well as against **unauthorised access**, **alteration** or dissemination." According to data protection laws based on the Directive 95/46/EC, the obligations of the data controller regarding the secure processing of personal data are: 1. Establishment of appropriate security standards and procedures. 2. Selection of personnel based on their skills and ethics and the provision of appropriate training in security issues. 3. Management of outsourcing contracts and the selection of a processor according the technical and organisational security measures governing the processing. 4. Whenever personal data are transferred outside Europe, the data controller must consider the security measures taken and the legislation concerning data protection in the country or territory where the data are transferred. **Security Control Selection Process** Baseline security based on international standards such as ISO 17799, provides "good

	protection against most threats and under most circumstances. However, baseline manuals provide little guidance on how to determine the set of controls to provide adequate security for the particular business situation or according to legal, regulatory requirements." This study suggests "a model for the selection of the most appropriate set of security controls that will satisfy the privacy protection requirements regarding the secure processing of the personal data." • **Purpose Specification:** identity the purposes for which data is collected and processed. i.e. to provide healthcare services, to facilitate medical research etc. • **Identification of the Personal Data or Categories of Personal Data:** Required to Fulfil the Basic Purpose of Data Collection and Processing. The principles of lawfulness and fairness and the principle of minimality are taken into account while personal data is identified as necessary for each data processing purpose. i.e. Does clinical procedures need personal data? What type of personal data is required to perform clinical procedures? Does medical research needs personal data? What type of personal data is required for the medical research. • **The Protection Degree of Personal Data:** corresponding to each data purpose is identified based on the privacy protection legal requirements. • **Application of the Security Principle:** for the selection of the appropriate security controls from one or a combination of baseline manuals, the CC standards, sample security plans and the findings of the risk assessment exercises. "The security controls are selected according to the concrete privacy protection requirements. The security principle is specifically applied in this step so that the security controls selected are the appropriate ones to assure the law provisions regarding data disclosure, destruction, and modification, both in technical and organisational domain. The computational and telecommunication infrastructure of the organisation is taken into consideration in this step." "The technical control requirements of the security principle range from authentication, integrity, access control mechanisms, confidentiality, accountability and digital signature creation and verification to privacy enhancing requirements such as anonymity, pseudonymity, unlinkability, and unobservability. To organisational control requirements belong among others security and privacy protection planning and strategy, security and privacy policy creation and maintenance and disaster recovery and business continuity planning." "Additionally, the selection of appropriate controls is base on the requirements regarding staff selection and security and privacy related training and the possible outsourcing contracts, in case the data controller involves third entities for the collection and processing of personal data. Finally, possible transfers of personal data outside European Union should be considered with respect to the security measures taken and the legislation concerning data protection in the country or territory where the data are transferred." • **Periodical Monitoring:** of the security publications and vulnerability analysis and generally of technological solutions and advances that should be considered so that privacy protection profiles and implementations are adjusted properly. **Example to Clarify the Model:** "The data processing **purposes** of a hospital may include, among others, the provision of health services, the administration of personnel, and the notification of the infectious diseases to the authorities responsible for monitoring such diseases." "Each of these purposes has certain **privacy protection requirements** regarding the secure processing of personal data, which dictate the adoption of different security controls. To the personal data for the purpose of administration less strict security controls may be applied in comparison to the personal data for the purpose of providing health services." [Refer to study for the diagram of Privacy Protection Model and Evaluation Model].
Additional note.	
66	**Data extracted from (Kluge 2004)**

Reference	Kluge, E.H.W., 2004. Informed consent and the security of the electronic health record (EHR): Some policy considerations. *International Journal of Medical Informatics*, 73(3), pp.229–234.
Study type Journal/ Conference/ book	
Data that address the research questions	**Issue of Informed Consent** "This paper examines the ethical basis of this position [informed consent], outlines its implications for professionals, institutions and society in general, and identifies its limits." Modern health care delivery is a complex affair and EHRs play different roles in different settings. However, the factor that unifies them is the patient who migrates from one domain to another and whose EHR provides the epistemic tool that makes the delivery of health care possible. These different technical domains present different security problems, which in turn may call for distinct security architectures and protocols. This is not the place to detail why these architectures and protocols should have a unifying underlying logic. Suffice it to say that if this is not the case, then the operational frameworks in which the EHRs have to function may well be logically inconsistent which will make it likely that the distinct HIS in which the EHRs are embedded will not mesh. This may have disastrous consequences for patients. However, even if different security architectures and protocols are mandated for different technical modalities, whether these be web-based approaches, smart cards, intranet usage, stand-alone systems, etc. this does not affect the logic of the consent process that should surround the development and processing of EHRs. The set of fundamental informatic patient rights is logically the same for all of these settings. Therefore, the logic of the informed consent process must be the same for all of these domains. The content of the processes may differ insofar as they may have to be adjusted to accommodate distinct material possibilities of security compromise. In other words, differences in operational execution should only occur in the contents of the fields that are demarcated by the categories of the rights themselves. Further, it is important that this process will alert the subjects of the EHRs (or their duly empowered proxies) to these informatic rights as well as to their limitations, and that they be given all the information that the reasonable person in the subject's position would want to know before making a decision, and that s/he be allowed to make a competent and voluntary decision.
Additional note.	
67	**Data extracted from (Rosenthal 2010)**
Reference	Rosenthal, D.S.H., 2010. Keeping bits safe: How Hard Can It Be? *Communications of the ACM*, 53(11), pp.47–55.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Measuring Failures** It wasn't until 2007 that researchers started publishing studies of the reliability that actual large-scale storage systems were delivering in practice.
Additional note.	
68	**Data extracted from (Afanasyev et al. 2011)**
Reference	Afanasyev, M. et al., 2011. Privacy-preserving network forensics. *Communications of the ACM*, 54(5), pp.78–87.

Study type Journal/ Conference/ book	Journal
Data that address the research questions	Related to research question one and for more detail check the study.
Additional note.	
69	**Data extracted from (Kotulic & Clark 2004)**
Reference	Kotulic, A.G. & Clark, J.G., 2004. Why there aren't more information security research studies. *Information & Management*, 41(5), pp.597–607.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Noting a serious lack of empirical research in the area of security risk management (SRM), we proposed a conceptual model based on the study of SRM at the firm level. Although considerable time and effort were expended in attempting to validate the usefulness of the proposed model, we were not successful. We provide here a description of our conceptual model, the methodology designed to test this model, the problems we faced while attempting to test the model, and our suggestions for those who attempt to conduct work in highly sensitive areas.
Additional note.	
70	**Data extracted from (Von-Solms 1998)**
Reference	Von-Solms, R., 1998. Information security management (2): guidelines to the management of information technology security (GMITS). *Information Management & Computer Security*, 6(5), pp.221–223.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Information security has become very important in most organizations. To introduce, manage and maintain a high level of information security in an organization calls for a proper management methodology. International Standards Organization/International Electro technical Commission has drafted a multi-part technical report to provide guidelines to organizations to effectively manage the process of IT security. This paper provides a brief description of the first three parts of this technical report.
Additional note.	The study offers a guideline to plan and implement information security policies in an information security management framework.
71	**Data extracted from (Gupta et al. 2003)**
Reference	Gupta, M.G.M. et al., 2003. Intrusion countermeasures security model based on prioritization scheme for intranet access security (emerging concepts category). *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.*, pp.174–181. Available at: http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=1232418.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Generally, an organizational network is partitioned into the un-trusted Internet and the trusted internal network to design and delegate security responsibilities. The security issues that surround any Intranet: are Authentication and Authorization. Authorization entails an access

	control mechanism for resources on Intranet. The traditional security model for Intranet is designed on philosophy that what is not expressly permitted is denied. An Intranet’s internal security perimeters must be dynamic. Depending on the application accessed, the enterprise’s definition of communities of trusted users will be different. Its challenge will be to create strong identity and centrally configurable access control. The tools used to implement an Intranet security program must be less intrusive than those used by organizations to safeguard access to and from the Internet.
Additional note.	
72	**Data extracted from (Kiely et al. 2006)**
Reference	Kiely, M. et al., 2006. Macro-economic cyber security models. In *Proceedings of the 2006 IEEE Systems and Information Engineering Design Symposium, SIEDS’06*. IEEE, pp. 284–291.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	This paper quantitatively addresses two issues concerning cyber security economics that prior efforts have not. The first involves cyber security and its effect on a company's reputation. In this case, we focus on the levels of investment companies make related to reputation and how they implicitly reveal their views on cyber security risks. The second involves cyber security regulations. This analysis compares different strategies for choosing companies to regulate and the corresponding levels of risk reduction. This analysis can be used by companies and government policy makers to address cyber security investments decisions.
Additional note.	
73	**Data extracted from (FFIEC 1998)**
Reference	FFIEC, 1998. *A nnual R eport 1998*, Washington, DC.
Study type Journal/ Conference/ book	Report
Data that address the research questions	
Additional note.	
74	**Data extracted from (Burke & Jarratt 2004)**
Reference	Burke, G.I. & Jarratt, D.G., 2004. The influence of information and advice on competitive strategy definition in small- and medium-sized enterprises. *Qualitative Market Research: An International Journal*, 7(2), pp.126–138.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Although strategy development in large corporations has been well documented, the process of formulating strategy in small firms has not been extensively investigated by researchers. The process in small firms does not reflect exhaustive strategic analysis, but rather, a personality driven, opportunistic or instinctive approach, channelled through an emergent planning process. This study builds on recent work examining the planning patterns and approaches of small firms by integrating an understanding of the nature and

	extent of information and advice sought and received by the firm, and how that interaction influences the formation of competitive strategy.
Additional note.	
75	**Data extracted from (Gong et al. 2009)**
Reference	Gong, G.Q., Qiang, S. & Wang, J., 2009. Information security measures and regulation research. In *2009 International Conference on Management Science and Engineering - 16th Annual Conference Proceedings, ICMSE 2009*. pp. 2184–2189.
Study type Journal/ Conference/ book	Conference
Data that address the research questions	In order to analyze the online enterprises Information Security optimal management measures quantitatively, a information security decision model is constructed. Based on the online firms information security decision analysis, found that the information security measures investment is proportioned to firm online business scale, Lots of online small-and-medium-enterprises become huge threads to internet because they are without incentive investment in security measures. When firms are attacked by independent threads, the enterprises can deploy security measures optimization respectively, but net attacks are contagious threats, the enterprises will loss enormous profits in spite of deployed security measures. Then government regulation is necessary. Government takes taxes and subsidy strategy to realize social optimal welfare, the comparing difference regulation results with complete and incomplete information are proposed in the model.
Additional note.	
76	**Data extracted from (Ekelhart et al. 2007)**
Reference	Ekelhart, A. et al., 2007. Ontological mapping of common criteria’s security assurance requirements. In *IFIP International Federation for Information Processing*. Springer US, pp. 85–95.
Study type Journal/ Conference/ book	Conference
Data that address the research questions	The Common Criteria (CC) for Information Technology Security Evaluation provides comprehensive guidelines for the evaluation and certification of IT security regarding data security and data privacy. Due to the very complex and time-consuming certification process a lot of companies abstain from a CC certification. We created the CC Ontology tool, which is based on an ontological representation of the CC catalog, to support the evaluator at the certification process. Tasks such as the planning of an evaluation process, the review of relevant documents or the creating of reports are supported by the CC Ontology tool. With the development of this tool we reduce the time and costs needed to complete a certification.
Additional note.	The study offers ontological mapping of Common Criteria's security assurance requirements for IT products.
77	**Data extracted from (Bottino 2006)**
Reference	Bottino, L.J., 2006. Security measures in a secure computer communications architecture. In *2006 ieee/aiaa 25TH Digital Avionics Systems Conference*. IEEE, pp. 1–18.
Study type Journal/ Conference/ book	Conference

Data that address the research questions	The Architecture of a Computer Communication System has evolved with advances in technology. Changes to satisfy telecommunication needs within the technical community have surfaced gradually through the efforts of international computer standards organizations, technical panels, and guidance committees. The design of a secure Computer Communications Architecture to protect the integrity of information exchange is pursued by the aerospace industry, the commercial and financial sectors, and at all levels of government agencies. Banking institutions, the insurance and medical professions, goods and commodity exchanges, the airline industry, and local, state, and federal government agencies have all sought increased computer security and confidence in their computer communications.
Additional note.	
78	**Data extracted from (Barnard & von Solms 2000)**
Reference	Barnard, L. & von Solms, R., 2000. A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Computers & Security*, 19(2), pp.185–194.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Current Evaluation and Certification Efforts in Information Security against BS 7799** Control selection goes hand in hand with evaluation and certification schemes. The Dutch Scheme The British Scheme **Security Aspects that Need to be Evaluated** • **Functionality:** the functionality aspect should indicate that all the proposed controls are in fact present in the IT environment being evaluated. • **Assurance of Correctness:** this aspect will prove that all controls are correctly installed and fully operational. • **Assurance of Effectiveness:** effectiveness will ensure that the set of proposed and installed controls are indeed adequate to satisfy the level of security envisaged in the security policy. • **Assurance of Operation:** assurance of operation will ensure that all the operational procedures that support the installed controls are indeed being followed by the information users. **An Evaluation Model for Information Security Against a Baseline Manual** The model is based on a two-stage evaluation process, namely an off-site evaluation and an on-site evaluation. The offsite evaluation will evaluate the functionality, correctness, and effectiveness of the proposed set of security controls. The on-site evaluation will evaluate the operational procedures associated with each security control. It should include all the required refinements to enable any organisation to effectively define, implement, evaluate and maintain a specified level of information security. **Figure 4: Evaluation model for BS 7799** **Steps of Evaluation Model** • Information security policy • Identify target of evaluation • identify security target • Evaluation (functionality, correctness, effectiveness, and operation assurance) • Certification (or reporting) **Evaluation Process** • Evaluation for functionality • Evaluation for correctness • Evaluation for effectiveness Evaluation for operation
Additional note.	

79	Data extracted from (Atymtayeva et al. 2012)
Reference	Atymtayeva, L.B. et al., 2012. Methodology and ontology of expert system for information security audit. In *Soft Computing and Intelligent Systems (SCIS) and 13th International Symposium on Advanced Intelligent Systems (ISIS)*. Japan: IEEE, pp. 238–243.
Study type Journal/ Conference/ book	Conference
Data that address the research questions	Information security auditing plays key role in providing any organization's good security level. By reason of high expenses of the audit process implementation, the automation of it through the development of the software may lead to a creation of a good alternative that will reduce costs, speed up the process of audit and improve its quality by the bringing it to compliance with international standards in information security. We suggest that fuzzy expert systems techniques can offer significant benefits when applied to this area. This paper presents some issues of the development of methodology and ontology for expert systems application concerning Information Security Audit (Expert System in Information Security Audit – ESISA)
Additional note.	The study offers an automated solution for risk analysis.
80	**Data extracted from (Commonwealth of Australia 2009)**
Reference	Commonwealth of Australia, 2009. *Cyber Security Strategy*
Study type Journal/ Conference/ book	Report
Data that address the research questions	**Strategic priorities** To achieve these objectives the Australian Government applies the following strategic priorities to its programs: • Improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest. • Educate and empower all Australians with the information, confidence and practical tools to protect themselves online. • Partner with business to promote security and resilience in infrastructure, networks, products and services. • Model best practice in the protection of government ICT systems, including the systems of those transacting with government online. • Promote a secure, resilient and trusted global electronic operating environment that supports Australia's national interests. • Maintain an effective legal framework and enforcement capabilities to target and prosecute cyber crime. • Promote the development of a skilled cyber security workforce with access to research and development to develop innovative solutions.
Additional note.	
81	**Data extracted from (Farn et al. 2004)**
Reference	Farn, K., Lin, S. & Fung, A.R., 2004. A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6), pp.501–513.
Study type Journal/ Conference/ book	Journal

Data that address the research questions	The security of information system is like a chain. Its strength is affected by the weakest knot. Since we can achieve 100% Information Security Management System (ISMS) security, we must cautiously fulfil the certification and accreditation of information security. In this paper, we analyzed, studied the evaluation knowledge and skills required for auditing the certification procedures for the three aspects of ISMS asset, threat, and vulnerability. **ISMS evaluation** Reducing risks is the target of ISMS protection mechanism as shown in Fig. 3.1 [15]. In order to achieve the ISMS, as early as in 1998, NIACAP started a Pilot Project, which accomplished the ISMS assurance ranging from national defence telecommunication, to finance infrastructure et al. as shown in Fig. 2.2. Table 3.1 illustrates the input and output for each stage. The telecommunication infrastructure of the U.S. is a good example. Federal Aviation Administration (FAA) was founded in 1958, and was incorporated into Department of Transportation (DoT) in 1967. On February 21, 1996, FAA according to the Guideline for Computer Security Certification and Accreditation developed by NIST on September 29, 1983, announced the FAA automatic information system and communication security function requirement, and also demanded the information assurance as described in Fig. 3.2.
Additional note.	The study offers a model for risk analysis
82	**Data extracted from (Vladimirov et al. 2010)**
Reference	Vladimirov, A., Gavrilenko, K. & Michajlowski, A., 2010. *Assessing Information Security: Strategies, Tactics, Logic and Framework*, United Kingdom: IT Governance.
Study type Journal/ Conference/ book	Book
Data that address the research questions	"Information security assessments are a practical way of improving the information security state." There are passive and active security incidents. Passive security incidents happen due to error Active security incidents happen due to combination of error and a hostile act. Security assessments must evaluate probabilities and the potential impacts of passive and active security incidents. Process of evaluation • Define goals and conditions of evaluation • Plan the appropriate actions • Select the corresponding methodologies and tools • Check and test everything you can within the limits of budget, requirements, time and means • pull the results together • measure and analyse risks • consider realistic remedies • generate an impressive report • work with the client on any follow-up acts if needed Why Organisations need to Evaluate their strategies? 1. Compliance and regulations demand it 2. A security incident has happened 3. Higher priority for security 4. the company and its information assets are lucrative target for cybercriminals 5. Internal security auditing team in the company needs justification for their presence Important Principles of Evaluation 1. Information security assessment must shape information security systems of its targets. 2. Information security assessment is never complete 3. Information security assessment must be a part of a continuous process 4. Information security assessment should maintain a proper balance between tempo and

	depth. 5. Information security assessment must always exceed its perceived scope. 6. Information security assessment always targets corporate or organisational ISMS. 7. Information security assessment (ISA) should aspire to establish the roots of all discovered vulnerabilities, weaknesses and gaps. 8. ISA should aspire to discover strategic problems through tactical means. 9. ISA must be endorsed, controlled and debriefed at the top. 10. ISA should be understood and appreciated at the bottom 11. ISA must produce transferable results. 12. ISA must decrease the friction of the auditee. (typical elements of internal friction figure 1 p. 46) 13. ISA should promote security awareness and initiative. 14. ISA always operates with probabilities 15. ISA is mainly a proactive countermeasure. 16 ISA must be impartial 17 ISA must be disassociated from the checked system. 18 ISA results must be strictly confidential. Categories of Audit Black, Grey, and White Box assessments The human, Technical, and ISMS (intervention) chain examples (pp. 119-121) Types of ISMS Audit • Documentation reviews • Process reviews • Overall security management reviews Human Related Audits • Social engineering Premises and Physical Checks • Overall premises security audit • Physical systems security audit • Social engineering Technical Security Audits • External penetration testing • External vulnerability scanning • Internal Penetration testing • Internal vulnerability scanning • Application security testing • Source code review • Wireless security testing "We operate in a fluid, rapidly changing, highly variable environment, security testing procedures often need to be modified in accordance with the auditee peculiarities and unfolding circumstances." (p.178)
Additional note.	
83	**Data extracted from (Rosenthal 2010)**
Reference	Rosenthal, D.S.H., 2010. Keeping bits safe: How Hard Can It Be? *Communications of the ACM*, 53(11), pp.47–55.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Measuring Failures** It wasn't until 2007 that researchers started publishing studies of the reliability that actual large-scale storage systems were delivering in practice.
Additional note.	
84	**Data extracted from (Wang et al. 2012)**

Reference	Wang, J., Xiao, N. & Rao, H.R., 2012. An exploration of risk information search via a search engine: Queries and clicks in healthcare and information security. *Decision Support Systems*, 52(2), pp.395–405. Available at: http://dx.doi.org/10.1016/j.dss.2011.09.006.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	The general public is increasingly using search engines to seek information on risks and threats. Based on a search log from a large search engine, spanning three months, this study explores user patterns of query submission and subsequent clicks in sessions, for two important risk related topics, healthcare and information security, and compares them to other randomly sampled sessions. We investigate two session-level metrics reflecting users' interactivity with a search engine: session length and query click rate. Drawing from information for aging theory, we find that session length can be characterized well by the Inverse Gaussian distribution. Among three types of sessions on different topics (healthcare, information security, and other randomly sampled sessions), we find that healthcare sessions have the most queries and the highest query click rate, and information security sessions have the lowest query click rate. In addition, sessions initiated by the users with greater search engine activity level tend to have more queries and higher query click rates. Among three types of sessions, search engine activity level shows the strongest effect on query click rate for information security sessions and weakest for health- care sessions. We discuss theoretical and practical implications of the study.
Additional note.	
85	**Data extracted from (Wozak et al. 2007)**
Reference	Wozak, F., Schabetsberger, T. & Ammmenwerth, E., 2007. End-to-end Security in Telemedical Networks - A Practical Guideline. *International Journal of Medical Informatics*, 76(5-6), pp.484–490. Available at: http://www.ncbi.nlm.nih.gov/pubmed/17097916 [Accessed June 22, 2014].
Study type Journal/ Conference/ book	Journal
Data that address the research questions	The interconnection of medical networks in different healthcare institutions will be constantly increasing over the next few years, which will require concepts for securing medical data during transfer, since transmitting patient related data via potentially insecure public networks is considered a violation of data privacy. The aim of our work was to develop a model-based approach towards end-to-end security which is defined as continuous security from point of origin to point of destination in a communication process. We show that end-to-end security must be seen as a holistic security concept, which comprises the following three major parts: authentication and access control, transport security, as well as system security. For integration into existing security infrastructures abuse case models were used, which extend UML use cases, by elements necessary to describe abusive interactions. Abuse case models can be constructed for each part mentioned above, allowing for potential security risks in communication from point of origin to point of destination to be identified and counteractive measures to be directly derived from the abuse case models. The model-based approach is a guideline to continuous risk assessment and improvement of end-to-end security in medical networks. Validity and relevance to practice will be systematically evaluated using close-to-reality test networks as well as in production environments.
Additional note.	
86	**Data extracted from (Clarke & Meiris 2006)**

Reference	Clarke, J. & Meiris, D., 2006. Electronic Personal Health Records Come of Age. *American Journal of Medical Quality*, 21(3), p.5S–5S.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Barriers to Adoption of PHRs** The number of PHR options is increasing (eg, iHealthRecords [Medem], MyChart [Epic], About MyHealth [Medscape]), and the potential benefits are many (eg, improved patient self-management, enhanced patient-provider communication, increased collaborative decision making, improved access to data in emergency situations, reduced costs). However, consumer and provider acceptance and adoption are not assured. Among the many complex issues that may prevent the widespread use of PHRs are Consumer-related issues: • Trust (eg, who will have access to the information?) • Privacy and security concerns (eg, will private PHR companies be regulated?) • Cost (eg, will consumers be willing to pay all or part of the cost if the PHR is not linked to any of their providers? Will consumers understand the nuances of different PHR products and be able to select the one with the best tools and functionality for their needs?) • User interface • Digital divide (eg, will PHRs increase health care disparities by further enlarging the gulf between the "haves" and "have-nots"?) • Maintaining data (eg, who will be responsible for ensuring that data are updated accurately and in a timely fashion?) Provider-related issues: • Limited electronic data systems in small-scale practitioner offices • Cost (eg, cost of producing the EMR, cost of lost productivity during the transition period) • Reimbursement for online communication • Integrating the information from the EMR and PHR into the practice workflow (eg, how much additional time will be required to make the information intelligible and accessible to patients?) • Maintenance of data and transfer of EMR data into PHRs • Technical issues: • Interoperability • Data repository • Data standards (eg, variations in coding and documentation exist, handwritten and through data entry) • Security
Additional note.	
87	**Data extracted from (Ceusters & Smith 2006)**
Reference	Ceusters, W. & Smith, B., 2006. Strategies for referent tracking in electronic health records. *Journal of Biomedical Informatics*, 39(3), pp.362–378.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	The goal of referent tracking is to create an ever-growing pool of data relating to the entities existing in concrete spatiotemporal reality. In the context of Electronic Healthcare Records (EHRs) the relevant concrete entities are not only particular patients but also their parts, diseases, therapies, lesions, and so forth, insofar as these are salient to diagnosis and treatment. Within a referent tracking system, all such entities are referred to directly and explicitly, something which cannot be achieved when familiar concept-based systems are used in what is called ''clinical coding.'' In this paper, we describe the components of a referent tracking system in an informal way and we outline the procedures that would have to be followed by healthcare personnel in using such a

	system. We argue that the referent tracking paradigm can be introduced with only minor though nevertheless ontologically important technical changes to existing EHR infrastructures, but that it will require a radically different mindset on the part of those involved in clinical coding and terminology development from that which has prevailed hitherto.
Additional note.	
88	**Data extracted from (The Office of Cyber Security and Information Assurance, Cabinet Office 2011)**
Reference	The Office of Cyber Security and Information Assurance, Cabinet Office, U.K., 2011. *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world*, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.
Study type Journal/ Conference/ book	Report
Data that address the research questions	The internet will become increasingly central to our economy and our society. But the growing role of cyberspace has also opened up new threats as well as new opportunities – we have no choice but to find ways to confront and overcome these threats if the UK is to flourish in an increasingly competitive and globalised world. The digital architecture on which we now rely was built to be efficient and interoperable. When the internet first started to grow, security was less of a consideration. However, as we put more of our lives online, this matters more and more. People want to be confident that the networks that support our national security, our economic prosperity, and our own private lives as individuals are safe and resilient.
Additional note.	
89	**Data extracted from (Brooks & Warren 2006)**
Reference	Brooks, W. & Warren, M., 2006. A methodology of health information security evaluation. *HIC 2006 and HINZ 2006*, 10(3), p.464. Available at: http://hcro.enigma.co.nz/website/results/20060926165844738O2578.pdf\nhttp://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=emed7&NEWS=N&AN=2006474025.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Objectives and Aims Conducting a health information security evaluation allows a health organisation to obtain a realistic measure of how secure its information resources are. The evaluation method under discussion provides a baseline and comparative set of criteria against which appropriate countermeasures to security risks or weaknesses, and the success of their implementation, can be gauged. It will assist with: • Identifying security weaknesses, possible threats and attacks • increasing organisational awareness of security issues • improving the security of information systems • reducing the costs of and the level of complexity required to perform an information security evaluation • providing evaluation results that non-IT professionals can understand • assisting healthcare organisations towards fulfilling the criteria for certification according to a recognised health information security management standard From a research point of view, the stimulus for now carrying out the proposed case study includes, but is not limited to, evaluating: • the usability of the evaluation method by all participants, i.e., management, IT professionals, and non-IT Professionals involved. • the efficiency of the method

	• the intelligibility of the processes involved and the outputs produced • the effectiveness of the results • the integrity of the method's design A case study validating the evaluation research method will be undertaken, testing the method within a large healthcare establishment in the state of Victoria, Australia. Case Study Description The case study will enable an in-depth, longitudinal examination of the evaluation method in a health organisational framework within a well-defined environment. It will provide a systematic way of collecting data, analysing information, and reporting the results. The case study approach will also allow a real-life validation of the research solution. Overview The evaluation method being tested comprises four basic processes: 1. Scenario construction and modelling 2. Health information security analysis 3. Comparison of the current security measures and the ideal security system. 4. Post-implementation analysis Figure 1: Workflow processes for the evaluation method For the case study, the "Researcher" will be the primary author and the "Participant" will be a member of the organisation with moderate IT knowledge. This person will be selected by the IT Director of the organisation and the primary author. 1. At first step, diagrams of physical and logical artefact are developed in order to map the security weaknesses and possible threats and attacks. 2. The participant will analyse the security countermeasures the organisation already has in place by means of a checklist… to complete the security assessment, the participant will compare the security controls already in place against the information security criteria, i.e., defined in the checklist. If a countermeasure has been installed then a value of 1 will be given on the checklist and a value of 0 if it has not been installed (table 1). The participant may need to examine the diagrams created in step 1 or consult the researcher if he/she has any doubts or questions concerning the security analysis. The rationale behind choosing a member of the organisation to perform the security analysis is to prohibit the fabrication, and publication, of any biased results for the case study and validation of research. That is, with two people performing the evaluation method, it will be impossible for either member to bias the evaluation because the results from step 1 and step 2 have to match. 3. Comparison of the Current and Ideal Security: The researcher will then convert the results from the checklist assessment (which will give the existing security level) into a percentage figure and plot them onto a two-dimensional evaluation histogram, where the vertical axis defines the information security control key areas and the horizontal axis defines the percentage of ideal security (100 percent) achieved in each category. 4. Post-Implementation Analysis The final step will be to improve the overall security level of the system by introducing new security features and analysing their probable effectiveness before implementation.
Additional note.	
90	**Data extracted from** (Appari & Johnson 2008)
Reference	Appari, A. & Johnson, E.M., 2008. Information Security and Privacy in Healthcare : Current State of Research., pp.1–39.
Study type Journal/ Conference/ book	Report
Data that address the research questions	HIPAA compliance has become a business necessity in healthcare maintenance organizations (HMO). Recently Warkentin et al. (2006) undertook a study to characterize the compliance behavior among administrative staff and medical staff of public as well private-sector healthcare facilities. The authors observed that healthcare professionals at public hospitals have higher self efficacy, i.e. belief in their capability to

	safeguard and protect patient's information privacy, compared to their counterparts in private healthcare facilities. Further, on average, administrative staff exhibited higher self efficacy than medical staff across both public and private healthcare facilities. Moreover, the behavioral intent of healthcare professionals, including medical and administrative staff, was positively correlated to self efficacy and perceived organizational support. Another set of studies show that healthcare workers, having access to patient data, are highly concerned about maintaining accuracy of patient records, unauthorized access to patient data, and believe that patient data should not be used for unrelated purposes except for medical research (Baumer, et al. 2000),
Additional note.	
91	**Data extracted from** (Calder 2013)
Reference	Calder, A., 2013. *ISO27001/ISO27002 A Pocket Guide* Second., Cambridgeshire: IT Governance.
Study type Journal/ Conference/ book	Standard
Data that address the research questions	**Information Security Management System** An Information Security Management System (ISMS) is defined (in ISO/IEC 27000) as 'part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes organisational structure, policies,planning activities, responsibilities, practices, procedures, processes and resources'. **The ISMS** An ISMS – which the Standard is clear includes 'organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources,'1 – is a structured, coherent management approach to information security, which is designed to ensure the effective interaction of the three key components of implementing an information security policy: 1- process (or procedure) 2-technology 3-user behaviour. The Standard's requirement is that the design and implementation of an ISMS should be directly influenced by each organisation's 'needs and objectives, security requirements, the organisational processes used and the size and structure of the organisation'. ISO27001 is not a one-size-fits-all solution, nor was it ever seen as a static, fixed entity that interferes with the growth and development of a business. The Standard explicitly recognises that: • the ISMS 'will be scaled in accordance with the needs of the organisation', and • the ISMS is 'expected to change over time'.
Additional note.	
92	**Data extracted from** (Chandler 1962)
Reference	Chandler, A.D., 1962. *Strategy and Structure: Chapters in the History of the American Industrial Enterprise*, MIT Press.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Strategy as a process that not only determines the wider long-term goals of the business, but also helps it to adopt a course of action and to deploy enough resources to achieve those goals.

Additional note.	
93	**Data extracted from** (Data Protection Audit Manual 2001)
Reference	Data Protection Audit Manual, 2001. Data Protection Audit Manual., (June).
Study type Journal/ Conference/ book	Report
Data that address the research questions	[Data Protection Audit manual's] use servers to identify possible areas of non-compliance requiring attention by a data controller. Although use of the manual has been piloted, there is no substitute for experience of its use, the checklist questions will be refined and may be expanded to cover issues specific to a particular sector… Ensuring compliance with the data protection standards is not simply an issue of operating within the law; it is also about the effective handling of personal information and respecting the interests of individual data subjects. This manual has been produced by the Information Commissioner to assist with data protection compliance auditing … under section 51(7) of the Data Protection Act 1998. The manual contains a methodology of conducting data protection compliance audits together with a series of checklists aimed at testing compliance with each of the Acts main provisions… It has been written in such a way that any data controller can use it to help judge their own data protection compliance. Similarly, it may also be used by other organisations offering such services to data controllers. Given that potential users may have different levels of existing audit expertise, the manual also includes general guidance on compliance auditing [for a diverse audience]… [However] it is expected that the checklist questions may develop over time as experience is gained in using these in practical situations. Given that the checklists are aimed at assessing compliance with the main elements of the Act, there is also scope for the development further sector specific checklists such as in connection with The Telecommunications (Data Protection and Privacy) regulations 1999. The manual is divided into five parts: introduction, the audit method, the audit process, general guidance on auditing, and series of annexes providing essential documents such as checklists containing compliance questions for each of the Acts. (Refer to the original document for checklists and other details about methods, types, and processes of audits)
Additional note.	
94	**Data extracted from** (Dogaheh 2010)
Reference	Dogaheh, M.A., 2010. Introducing a framework for security measurements. In *Proceedings 2010 IEEE International Conference on Information Theory and Information Security, ICITIS 2010*. pp. 638–641.
Study type Journal/ Conference/ book	Conference
Data that address the research questions	The paper introduces a new approach to measure the security of organisation with a recommended framework. this would be an interface system named SM-Framework acts as a system management which yields in the figures of merit of an organisation security. It has given numerically and graphically, the level of security in different times for an organisation.
Additional note.	
95	**Data extracted from** (Gerber et al. 2001)
Reference	Gerber, M., Von Solms, R. & Overbeek, P., 2001. Formalizing information security requirements. *Information Management & Computer Security*, 9(1), pp.32–37.

Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Formalising information security requirements** **A formalized approach to determining security requirements** This formalized approach will be referred to as the Security Requirements Exercise. The primary goal of the Security Requirements Exercise is to determine the information security requirements of an organization. These security requirements should provide an easy way in which the most appropriate set of information security controls can be identified, based on the predetermined information security requirements, to meet the specific information security need, which exists within an organization(BS 7799-1, 1999, p.2)
Additional note.	
96	**Data extracted from** (Hart 2001)
Reference	Hart, B., 2001. Implementing a Successful Security Assessment Process. *SANS*, pp.1–10.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	**Purpose of the Security Assessment** The goal of a security assessment, (also known as a security audit or security review), is to ensure that necessary security controls are integrated into the design and implementation of a project. A properly completed security assessment should provide documentation outlining any security gaps between a project design and approved corporate security policies. Management can address security gaps in three ways: Management can decide to cancel the project, allocate the necessary resources to correct the security gap, or accept the risk based on an informed risk/reward analysis. **Conducting a Security Assessment** Many methodologies exist for conducting a successful security assessment. Every organisation will require a slightly different approach. However, assessments are generally conducted using the same basic steps. Project initiation, information discovery. **Project Initiation** Of a business unit proposes a project, it is distributed to any corporate supporting groups i.e., IT groups, including security, finance, and marketing groups etc that may need to support or may be impacted by the new project. The security assessment policy should require that any new project proposal be reviewed by security. Security team may determine to conduct or not to conduct the security assessment of the project depending upon the needs of the project. **Information Discovery** Gathering information about a project and assessing appropriate security controls can be accomplished many different ways. One effective way for gathering high-level security information is through a security checklist. A security checklist must be based on corporate security policies and procedures. According to C&A Systems Security Ltd., "a computer audit must embrace a variety of requirements. Consideration of risk is of growing importance, but fundamental to the whole security audit programme is compliance with the audit checklist and of course the organisation's information security policies." Security Assessment Categories Network Security System Security Application Security Data Security and Classification Business Resumption Assessing External Parties Closing the Discovery Phase

	Security Assessment Phase The process flow for the assessment phase begins with a detailed evaluation of the identified security gaps, or issues. The security manager should work closely with the project team to define and understand these gaps. To be successful, the security manager must develop an open and trusted relationship with key members of the project team. In a recent Information Security magazine article, Ira Winkler emphasises the importance of this relationship: "In an assessment, the assessor should have the full cooperation of the organisation being assessed. The organisation grants access to its facilities, provides network access, outlines detailed information about the network, etc. All parties acknowledged that the goal is to study security and identify improvements to secure the systems. An assessment is potentially the most useful of all security tests, but it is also the hardest to define." Though the security manager can provide advice on security solutions, the project team is the one responsible for identifying specific tools for mitigating security risk, and integrating these tools into the project design. After the gaps are defined and solution identified, a draft assessment can be written. The draft assessment will describe the overall project design, the security controls that are currently implemented, and any outstanding security issues that remain. Based on resource requirements, the project manager may address some security issues, but not others. After reviewing the draft assessment with the project manager, a final assessment can be written and distributed. policy should require that the project sponsor sign the assessment. This sign-off provides an essential audit trail showing that the project sponsor received and understood the assessment, and acknowledged the existence of any outstanding security risks. **Policy Exceptions** If no policy violations are identified in the assessment, the process is essentially complete. If the assessment contains identified policy violations (previously not addressed), then a special approval, or policy exception must be obtained to proceed. A Final Word on Security Assessment The assessment process should facilitate and enable business objectives, not hinder or prevent innovation.
Additional note.	
97	**Data extracted from** (Hawkey et al. 2008)
Reference	Hawkey, K. et al., 2008. Human, organizational, and technological factors of IT security. In *Proceedings of ACM CHI 2008 Conference on Human Factors in Computing Systems*. pp. 3639–3644. Available at: http://doi.acm.org/10.1145/1358628.1358905.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	This paper describes the HOT Admin research project, which is investigating the human, organizational, and technological factors of IT security from the perspective of security practitioners. We use qualitative methods to examine their experiences along several themes including: unique characteristics of this population, the challenges they face within the organization, their activities, their collaborative interactions with other stakeholders, the sub-optimal situations they face as a result of distributed security management, and the impact of the security management model in place. We present preliminary results for each theme, as well as the implications of these results on the field of usable security and other research areas within HCI.
Additional note.	
98	**Data extracted from** (HSCIC 2014)
Reference	HSCIC, 2014. *Code of practice on confidential information*, UK.

Study type Journal/ Conference/ book	Code of practice
Data that address the research questions	**Establish the purpose of arrangements to handle confidential information** Before confidential information is handled, the purpose needs to be understood in detail. Purposes may be for managing the delivery of care for a population, research or another purpose. 1. Organisations seeking to handle confidential information should define and describe the intended purpose(s) of handling that confidential information. 2. In addition, organisations seeking to handle data relating to an individual who can be identified must define and describe the intended purpose(s) of handling that data. The Health and Social Care Information Centre can only use its general dissemination powers where the intended purpose is in connection with the provision of health care or adult social care, or the promotion of health. This encompasses a wide range of health and care related intended purposes including for the commissioning of those services, and the epidemiological research that is needed at the earlier stages of developing new treatments but not for solely commercial intended purposes such as for commercial insurance. 3. Organisations seeking to handle confidential information should assess the impact of handling that confidential information on privacy. 4. Organisations seeking to handle confidential information should assess the availability and quality of information and whether that information will meet the intended purpose. 5. Organisations seeking to handle confidential information should inform individuals and organisations about the proposed uses of their personal information. 6. A research study should adhere to the Research Governance Framework for England.
Additional note.	
99	**Data extracted from** (ISO/IEC13335-1 1996)
Reference	ISO/IEC13335-1, 1996. *Information Technology -Guidelines for the Management of IT Security - Part 1: Concepts and Models for IT Security*, Geneva: International Standards Organization.
Study type Journal/ Conference/ book	Guidelines
Data that address the research questions	
Additional note.	
100	**Data extracted from** (ISO/IEC17799 2005)
Reference	ISO/IEC17799, 2005. Information technology -- Security techniques -- Code of practice for information security management.
Study type Journal/ Conference/ book	International standard
Data that address the research questions	This standard is very important and must be all considered Each clause contains a number of main security categories. The eleven clauses (accompanied with the number of main security categories included within each clause) are: a) Security Policy (1);

	b) Organizing Information Security (2);
	c) Asset Management (2);
	d) Human Resources Security (3);
	e) Physical and Environmental Security (2);
	f) Communications and Operations Management (10);
	g) Access Control (7);
	h) Information Systems Acquisition, Development and Maintenance (6);
	i) Information Security Incident Management (2);
	j) Business Continuity Management (1);
	k) Compliance (3).

Additional note.	
101	**Data extracted from** (ISO/IEC 21827 2008)
Reference	ISO/IEC 21827, B., 2008. Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM).
Study type Journal/ Conference/ book	Standard
Data that address the research questions	There is more than one way to group practices into common features and common features into capability levels. The following discussion addresses these common features. The ordering of the common features stems from the observation that implementation and institutionalization of some practices benefit from the presence of others. This is especially true if practices are well established. Before an organization can define, tailor, and use a process effectively, individual projects should have some experience managing the performance of that process. Before institutionalizing a specific estimation process for an entire organization, for example, an organization should first attempt to use the estimation process on a project. However, some aspects of process implementation and institutionalization should be considered together (not one ordered before the other) since they work together toward enhancing capability. Common features and capability levels are important both in performing an assessment and improving an organization's process capability. In the case of an assessment where an organization has some, but not all common features implemented at a particular capability level for a particular process, the organization usually is operating at the lowest completed capability level for that process. For example, an organization that performs all but one of the Level 2 generic practices for some process area should receive a Level 1 rating. An organization may not reap the full benefit of having implemented a common feature at any given capability level if the common features at lower capability levels have not been implemented. An assessment team should take this into account in assessing an organization's individual processes. In the case of improvement, organizing the practices into capability levels provides an organization with an “improvement road map,” should it desire to enhance its capability for a specific process. For these reasons, the practices in the SSE-CMM® are grouped into common features, which are ordered by capability levels. An assessment should be performed to determine the capability levels for each of the process areas. This indicates that different process areas can and probably will exist at different levels of capability. The organization will then be able to use this process-specific information as a means to focus improvements to its processes. The priority and sequence of the organization's activities to improve its processes should take into account its business goals. Business goals are the primary driver in interpreting a model such as the SSE-CMM®. But, there is a fundamental order of activities and basic principles that drive the logical sequence of typical improvement efforts. This order of activities is expressed in the common features and generic practices of the capability level side of the SSE-CMM® architecture.

Additional note.	
102	**Data extracted from** (ISO/IEC 27001:2005 2005)
Reference	ISO/IEC 27001:2005, 2005. *Information technology — Security techniques — Information security management systems — Requirements,*
Study type Journal/ Conference/ book	Standard
Data that address the research questions	This standard is very important and must be all considered
Additional note.	
102	**Data extracted from** (ISO/IEC 27001:2013 2013)
Reference	ISO/IEC 27001:2013, 2013. *Information technology - Security techniques - Information security management systems - Requirements,*
Study type Journal/ Conference/ book	Standard
Data that address the research questions	This standard is very important and must be all considered This International Standard specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this International Standard.
Additional note.	
103	**Data extracted from** (ISO/IEC 27002:2013 2013)
Reference	ISO/IEC 27002:2013, 2013. *Information technology — Security Techniques — Code of practice for information security controls,*
Study type Journal/ Conference/ book	Standard
Data that address the research questions	This standard is very important and must be all considered This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations)
Additional note.	

104	**Data extracted from** (Niazi et al. 2005)
Reference	Niazi, M., Wilson, D. & Zowghi, D., 2005. A framework for assisting the design of effective software process improvement implementation strategies. *Journal of Systems and Software*, 78(2), pp.204–222.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	A number of advances have been made in the development of software process improvement (SPI) standards and models, e.g. Capability Maturity Model (CMM), more recently CMMI, and ISO?s SPICE. However, these advances have not been matched by equal advances in the adoption of these standards and models in software development which hasresulted in limited success for many SPI efforts. The current problem with SPI is not a lack of standards or models, but rather a lack of an effective strategy to successfully implement these standards or models.
Additional note.	
105	**Data extracted from** (Persusco 2006)
Reference	Persusco, L., 2006. Using scenario planning in the evaluation of information security applications K. Michael & M. G. Michael, eds. *First Workshop on the Social Implications of National Security (Workshop on the Social Implications of Information Security Mesures on Citizens and Business, 2006)*, pp.105–117. Available at: http://www.secureaustralia.org/.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	This paper provides a broad overview of the scenario approach as it relates to the evaluation of location based services (LBS) technologies and their application. A scenario is a plausible vision of the future, based around a particular technology or application and developed via a scenario planning methodology. The main worth of the scenario planning approach is that it allows an application to be evaluated in terms of potential social impacts as well as technical merit and commercial viability. A sample scenario is presented within the paper to illustrate how the scenario planning methodology can be used. This scenario is analysed via deconstruction to draw out major issues presented regarding the use of LBS. The major contribution of this paper is a demonstration of the merits of scenarios in evaluating new technologies.
Additional note.	
106	**Data extracted from** (Purser 2004)
Reference	Purser, S., 2004. *A practical guide to managing information security*, Artech House, Boston. London.
Study type Journal/ Conference/ book	Book
Data that address the research questions	
Additional note.	
107	**Data extracted from** (Sajko et al. 2010)

Reference	Sajko, M., Hadjina, N. & Pešut, D., 2010. Multi-criteria model for evaluation of information security risk assessment methods and tools. *MIPRO*, pp.1215–1220. Available at: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5533650&url=http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5533650.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Methods and tools for supporting the process of information security risk assessment are determined through several attributes. These attributes make a particular method and tool more or less suitable for solving risk assessment problems in companies. During the process of selecting these methods, companies have limitations such as financing, human resources, knowledge, time, etc. These limitations determine the approach to solving the problem of risk assessment. In respect to these limitations on one side and the attributes of risk assessment methods/tools on the other, we can establish a model for assisting the selection of a suitable method/tool. The experience gained in some Croatian companies when applying this model for the selection of their appropriate risk assessment support is also presented in this paper.
Additional note.	
108	**Data extracted from** (Von-Solms 1996)
Reference	Von-Solms, R., 1996. Information security management: The second generation. *Computers & Security*, 15(4), pp.281–288.
Study type Journal/ Conference/ book	Journal
Data that address the research questions	Information Security Evaluation and Certification Techniques A number of evaluation and certification techniques, models and schemes exist that can be linked to information security. The following will be discussed in more detail: Trusted Security Evaluation Criteria schemes. IS0 9000 (BS 5750), the leading international quality assurance scheme. The Code of Practice for Information Security Management (BS 7799) and, self-evaluation.
Additional note.	
109	**Data extracted from** (Wylder 2004)
Reference	Wylder, J., 2004. *Strategic Information Security*, USA: Auerbach Publications.
Study type Journal/ Conference/ book	Book
Data that address the research questions	
Additional note.	

Appendix C:

Quality Assessment

All the 114 selected articles were assessed for quality simultaneously with data extraction. The quality of each study was determined by pre-set criteria for quality. The criteria for quality were set following in the footsteps of Dyba and Dingoyr [25]. These criteria were used in the SLR when there were a number of different study types. It was realised that this SLR was pulling together studies of different types, therefore this criteria was considered appropriate and useful. The following are questions used for quality assessment:

1. Is the paper based on research or is it a "lessons learned" report based on expert opinion?
2. Is there a clear statement of the aims of the research?
3. Is there an adequate description of the context in which the research was carried out?
4. Was the research design appropriate to address the aims of the research?
5. Was the recruitment strategy appropriate to the aims of the research?
6. Was there a control group with which to compare treatments?
7. Was the data collected in a way that addressed the research issue?
8. Was the data analysis sufficiently rigorous?
9. Has the relationship between researcher and participants been considered to an adequate degree?
10. Is there a clear statement of findings?
11. Is the study of value for research and practice?

The questions for quality assessment were answered Yes or No with the corresponding values 1or 0. The first three criteria were used to exclude non- empirical research items and studies without clarity of aims. This factor represents the minimum quality threshold. In total five studies were rejected as they did not meet the minimum quality criteria (Brenner 2010; Anthes 2010; Lampson 2009; Hoffmann 2009; Saydjari 2006). The aim of the remaining nine criteria is to determine the rigour and credibility of the research methods applied and also to determine the relevance of studies selected to the SLR.

The following table shows results of the quality assessment for the selected studies from the SLR:

No	**Selected studies from the SLR**	**Research**	**Aim**	**Context**	**Design**	**Recruitment**	**Control**	**Data collect**	**Data analysis**	**Relationship**	**Finding**	**Value**	**Total score**
1.	(Tarwireyi et al. 2011)	1	1	1	1	1	1	1	1	1	1	1	**11**
2.	(Goel & Chengalur-Smith 2010)	1	1	1	1	1	0	0	1	0	1	1	**8**
3.	(Goel et al. 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
4.	(Doherty et al. 2009)	1	1	1	1	1	0	1	1	0	1	1	**9**
5.	(Jafari et al. 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
6.	(Kuang & Ibrahim 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
7.	(Sheppard et al. 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
8.	(Win & Fulcher 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
9.	(Hamill et al. 2005)	1	1	1	1	0	0	1	1	0	1	1	**8**
10.	(Wiant 2005)	1	1	1	1	0	0	1	1	0	1	1	**8**
11.	(Loef et al. 2002)	1	1	1	1	1	1	1	1	0	1	1	**10**
12.	(Humaidi et al. 2011)	1	1	1	1	1	1	1	1	0	1	1	**10**
13.	(Persusco 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
14.	(Anthes 2010)	0	0	1	0	0	0	0	0	0	0	1	**2**
15.	(Kumar & Puri 2012)	1	1	1	1	0	0	1	1	0	1	1	**8**

16.	Brenner 2010	0	0	0	0	0	0	0	0	0	0	1	**1**
17.	(Kazemi et al. 2012),	1	1	1	1	0	0	1	1	0	1	1	**8**
18.	(GAO 2006)	1	1	1	1	1	0	1	1	0	1	1	**9**
19.	(Anderson 2000)	1	1	1	1	0	0	1	1	0	1	1	**8**
20.	(Booker 2006),	1	1	1	1	0	0	1	1	0	1	1	**8**
21.	(Eminağaoğlu et al. 2009)	1	1	1	1	1	1	1	1	0	1	1	**10**
22.	(Dogaheh 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
23.	(Fung et al. 2003)	1	1	1	1	0	0	1	1	0	1	1	**8**
24.	(Kankanhalli et al. 2003)	1	1	1	1	1	0	1	1	0	1	1	**9**
25.	(Von-Solms 1998)	1	1	1	1	0	0	1	1	0	1	1	**8**
26.	(Jirasek 2012)	1	1	1	1	0	0	1	1	0	1	1	**8**
27.	(Linden et al. 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
28.	(Reni et al. 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
29.	(Bakker 1998)	1	1	1	1	0	0	1	1	0	1	1	**8**
30.	(Wozak et al. 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
31.	(Gupta et al. 2003)	1	1	1	1	0	0	1	1	0	1	1	**8**
32.	,(Kiely et al. 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
33.	(Chi et al. 2008)	1	1	1	1	1	0	1	1	0	1	1	**9**
34.	(Park et al. 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
35.	(Liu et al. 2011)	1	1	1	1	0	0	1	1	0	1	1	**8**
36.	(Gong et al. 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
37.	Lampson 2009	0	0	1	0	0	0	0	0	0	1	1	**3**
38.	(Tzelepi et al. 2002)	1	1	1	1	0	0	1	1	0	1	1	**8**
39.	(Gritzalis & Lambrinoudakis 2000)	1	1	1	1	0	0	1	1	0	1	1	**8**
40.	(Stewart 2003)	1	1	1	1	1	0	1	1	0	1	1	**9**
41.	(Abraham et al. 2011)	1	1	1	1	1	0	1	1	0	1	1	**9**
42.	(Hoffmann 2009)	0	0	1	0	0	0	0	0	0	1	1	**3**
43.	(Lukasik 2011)	1	1	1	1	0	0	1	1	0	1	1	**8**
44.	(Safran et al. 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
45.	(Kulmala 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
46.	(Sajko et al. 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
47.	(Wang et al. 2012)	1	1	1	1	1	1	1	1	0	1	1	**10**
48.	(Ko et al. 2005)	1	1	1	1	0	0	1	1	0	1	1	**8**
49.	(Schumacher et al. 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**

50.	(Shoniregun et al. 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
51.	(Ekelhart et al. 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
52.	(Mohammad 2010)	1	1	1	1	1	0	1	1	0	1	1	**9**
53.	Saydjari 2006)	0	0	0	0	0	0	0	0	0	0	1	**1**
54.	(Tyson & Slocum 2012)	1	1	1	1	1	0	1	1	0	1	1	**9**
55.	(Saleh et al. 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
56.	(Bottino 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
57.	(Biskup 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
58.	(Blyth & Kovacich 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
59.	(Barnard & von Solms 2000)	1	1	1	1	0	0	1	1	0	1	1	**8**
60.	(Atymtayeva et al. 2012)	1	1	1	1	0	0	1	1	0	1	1	**8**
61.	(Pishva et al. 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
62.	(Gerber et al. 2001)	1	1	1	1	0	0	1	1	0	1	1	**8**
63.	(Farn et al. 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
64.	(Vladimirov et al. 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
65.	(Häyrinen et al. 2008)	1	1	1	1	1	0	1	1	0	1	1	**9**
66.	(NHS 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
67.	(Takeda et al. 2000)	1	1	1	1	0	0	1	1	0	1	1	**8**
68.	(Clarke & Meiris 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
69.	(Papazafeiropoulou & Gandecha 2008)	1	1	1	1	0	0	1	1	0	1	1	**8**
70.	(Siougle & Zorkadis 2002)	1	1	1	1	0	0	1	1	0	1	1	**8**
71.	(Kluge 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
72.	(Brooks & Warren 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
73.	(Niazi et al. 2005)	1	1	1	1	0	0	1	1	0	1	1	**8**
74.	(DH/Digital Information Policy 2007)	1	1	1	1	0	0	1	1	0	1	1	**8**
75.	(Stahl et al. 2012)	1	1	1	1	1	0	1	1	0	1	1	**9**
76.	(Smith & Eloff 1999)	1	1	1	1	1	0	1	1	0	1	1	**9**
77.	(Ceusters & Smith 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
78.	(Otieno et al. 2008)	1	1	1	1	1	0	1	1	0	1	1	**9**
79.	(Rosenthal 2010)	1	1	1	1	0	0	1	1	0	1	1	**8**
80.	(Meingast et al. 2006)	1	1	1	1	0	0	1	1	0	1	1	**8**
81.	(Commonwealth of Australia 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
82.	(Afanasyev et al. 2011)	1	1	1	1	0	0	1	1	0	1	1	**8**
83.	(The Office of Cyber Security and Information Assurance, Cabinet Office	1	1	1	1	0	0	1	1	0	1	1	**8**

	2011)												
84.	(Gaunt 1998)	1	1	1	1	0	0	1	1	0	1	1	**8**
85.	(ISO/IEC13335-1 1996)	1	1	1	1	1	0	1	1	0	1	1	**9**
86.	(ISO/IEC17799 2005)	1	1	1	1	1	0	1	1	0	1	1	**9**
87.	(Knapp et al. 2009)	1	1	1	1	0	0	1	1	0	1	1	**8**
88.	(Speed & Ellis 2003)	1	1	1	1	0	0	1	1	0	1	1	**8**
89.	(Mintzberg 1978)	1	1	1	1	0	0	1	1	0	1	1	**8**
90.	(Chandler 1962)	1	1	1	1	0	0	1	1	0	1	1	**8**
91.	(Burke & Jarratt 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
92.	(Tipton & Krause 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
93.	(Hawkey et al. 2008)	1	1	1	1	1	0	1	1	0	1	1	**9**
94.	(Kotulic & Clark 2004).	1	1	1	1	0	0	1	1	0	1	1	**8**
95.	(Gerber & von Solms 2008)	1	1	1	1	0	0	1	1	0	1	1	**8**
96.	(Wylder 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
97.	(FFIEC 1998)	1	1	1	1	1	0	1	1	0	1	1	**9**
98.	(Andress 2003)	1	1	1	1	0	0	1	1	0	1	1	**8**
99.	(Höne & Eloff 2002)	1	1	1	1	1	0	1	1	0	1	1	**9**
100.	(Mohapatra & Singh 2012)	1	1	1	1	0	0	1	1	0	1	1	**8**
101.	(Thigarajan 2006)	1	1	1	1	1	1	1	1	0	1	1	**10**
102.	(Sunyaev 2011)	1	1	1	1	1	1	1	1	0	1	1	**10**
103.	(Appari & Johnson 2008)	1	1	1	1	1	0	1	1	0	1	1	**9**
104.	(Calder 2013)	1	1	1	1	0	0	1	1	0	1	1	**8**
105.	(Data Protection Audit Manual 2001)	1	1	1	1	0	0	1	1	0	1	1	**8**
106.	(Hart 2001)	1	1	1	1	0	0	1	1	0	1	1	**8**
107.	(HSCIC 2014)	1	1	1	1	1	0	1	1	0	1	1	**9**
108.	(ISO/IEC 21827 2008)	1	1	1	1	0	0	1	1	0	1	1	**8**
109.	(ISO/IEC 27001:2013 2013)	1	1	1	1	1	0	1	1	0	1	1	**9**
110.	(ISO/IEC 27002:2013 2013)	1	1	1	1	0	0	1	1	0	1	1	**8**
111.	(ISO 27799:2008 2008)	1	1	1	1	1	0	1	1	0	1	1	**9**
112.	(Purser 2004)	1	1	1	1	0	0	1	1	0	1	1	**8**
113.	(Von-Solms 1996)	1	1	1	1	0	0	1	1	0	1	1	**8**
114.	(Yoo et al. 2007)	1	1	1	1	1	0	1	1	0	1	1	**9**

Appendix D:

Audit Checklist

The data collected through the checklist, and marked against the suggested criteria mentioned above, was processed with the help of Microsoft Excel. The objective of processing the data was to attain the information security score for each detailed control, control subcategory, and control category, with the help of each question about the information security in the hospital. Replies were received for all the security questions and assigned values during the data collection process.

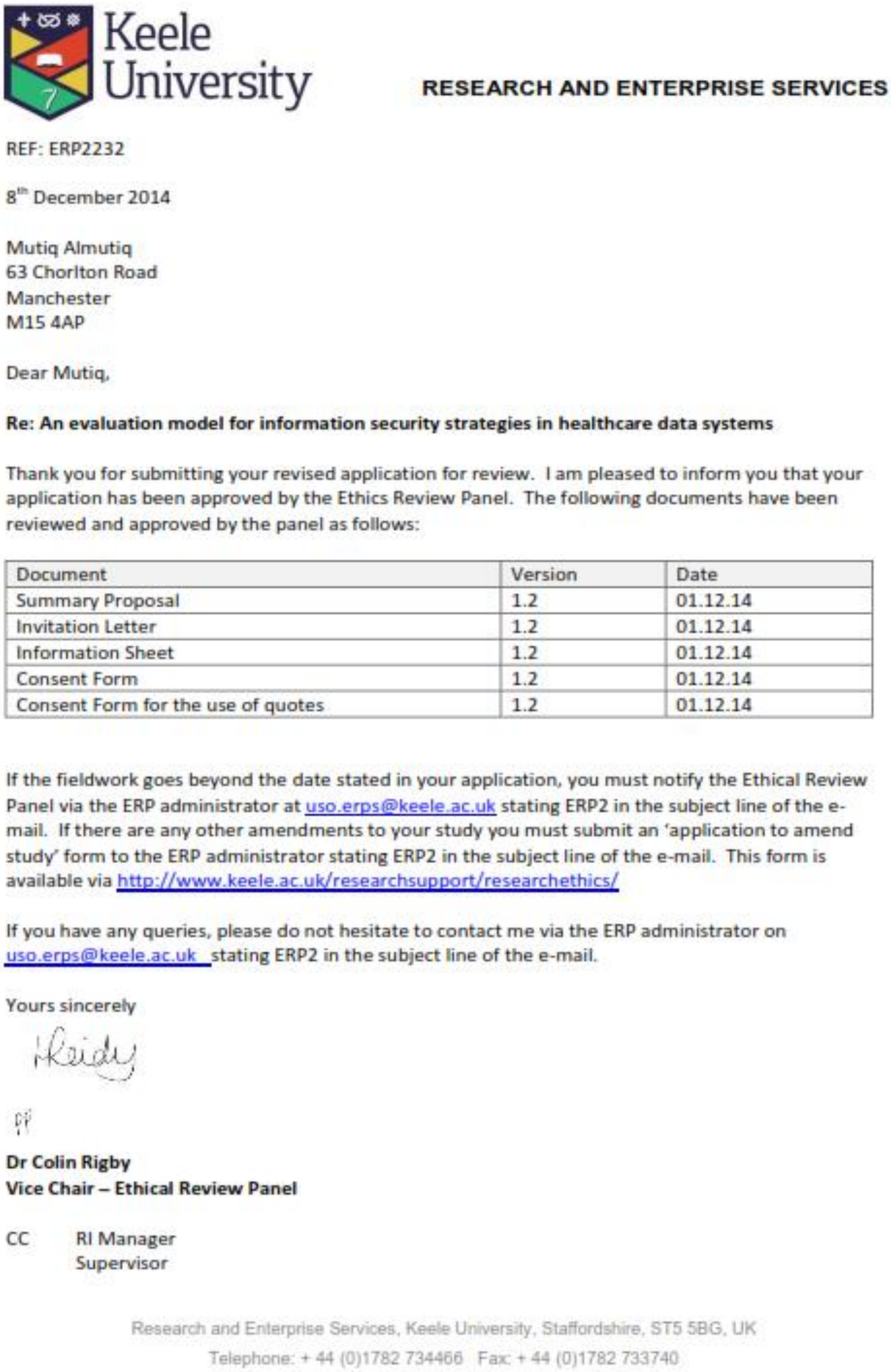
Control Category	Sub Control Category	Detailed Control Items	No	Evaluation Result
Asset management	Responsibility for assets	Inventory of assets	1.1	5
		Ownership of assets	1.2	5
		Acceptable use of assets	1.3	3
	Information classification	Classification guidelines	1.4	4
		Information labelling and handling	1.5	3
Average evaluation score for the control category				4.00
Human Resources security	Prior to employment	Roles and responsibilities	2.1	5
		Screening	2.2	5
		Terms and conditions of employment	2.3	5
	During employment	Management responsibilities	2.4	4
		Information security awareness, education and training	2.5	3
		Disciplinary process	2.6	5
	Termination or change of employment	Termination responsibilities	2.7	5
		Return of assets	2.8	3
		Removal of access rights	2.9	4
Average evaluation score for the control category				4.33
Communications and operations Management	Operational Procedures and responsibilities	Documented Operating procedures	3.1	5
		Change management	3.2	4
		Segregation of duties	3.3	3
		Separation of development, test and operational facilities	3.4	4
	Third party service delivery management	Service delivery	3.5	4
		Monitoring and review of third party services	3.6	4

		Managing changes to third party services	3.7	4
	System planning and acceptance	Capacity Management	3.8	4
		System acceptance	3.9	4
	Protection against malicious and mobile code	Controls against malicious code	3.10	4
		Controls against mobile code	3.11	3
	Backup	Information backup	3.12	3
	Network Security Management	Network Controls	3.13	4
		Security of network services	3.14	4
	Media handling	Management of removable media	3.15	5
		Disposal of Media	3.16	4
		Information handling procedures	3.17	3
		Security of system documentation	3.18	4
	Exchange of Information	Information exchange policies and procedures	3.19	5
		Exchange agreements	3.20	4
		Physical Media in transit	3.21	5
		Electronic Messaging	3.22	3
		Business information systems	3.23	4
	Electronic Commerce Services	Electronic Commerce	3.24	4
		On-Line Transactions	3.25	5
		Publicly available information	3.26	4
	Monitoring	Audit logging	3.27	3
		Monitoring system use	3.28	3
		Protection of log information	3.29	4
		Administrator and operator logs	3.30	4
		Fault logging	3.31	4
		Clock synchronisation	3.32	4
Average evaluation score for the control category				3.94
Access Control	Business Requirement for Access Control	Access Control Policy	4.1	4
	User Access Management	User Registration	4.2	5
		Privilege Management	4.3	4
		User Password Management	4.4	4
		Review of user access rights	4.5	4
	User Responsibilities	Password use	4.6	3
		Unattended user equipment	4.7	4
		Clear desk and clear screen policy	4.8	4
	Network Access Control	Policy on use of network services	4.9	4
		User authentication for external connections	4.10	5
		Equipment identification in	4.11	5

		networks		
		Remote diagnostic and configuration port protection	4.12	5
		Segregation in networks	4.13	5
		Network connection control	4.14	5
		Network routing control	4.15	5
	Operating system access control	Secure log-on procedures	4.16	4
		User identification and authentication	4.17	4
		Password management system	4.18	4
		Use of system utilities	4.19	5
		Session time-out	4.20	5
		Limitation of connection time	4.21	4
	Application and Information Access Control	Information access restriction	4.22	5
		Sensitive system isolation	4.23	5
	Mobile Computing and teleworking	Mobile computing and communications	4.24	5
		Teleworking	4.25	5
Average evaluation score for the control category				4.48
Compliance	Compliance with legal requirements	Identification of applicable legislation	5.1	4
		Intellectual property rights (IPR)	5.2	5
		Protection of organizational records	5.3	4
		Data protection and privacy of personal information	5.4	3
		Prevention of misuse of information processing facilities	5.5	5
		Regulation of cryptographic controls	5.6	5
	Compliance with security policies and standards, and technical compliance	Compliance with security policies and standards	5.7	3
		Technical compliance checking	5.8	4
	Information Systems audit considerations	Information systems audit controls	5.9	4
		Protection of information system audit tools	5.10	4
Average evaluation score for the control category				4.10

Appendix E:

Ethical approval letter



Keele University

RESEARCH AND ENTERPRISE SERVICES

REF: ERP2232

8th December 2014

Mutiq Almutiq
63 Chorlton Road
Manchester
M15 4AP

Dear Mutiq,

Re: An evaluation model for information security strategies in healthcare data systems

Thank you for submitting your revised application for review. I am pleased to inform you that your application has been approved by the Ethics Review Panel. The following documents have been reviewed and approved by the panel as follows:

Document	Version	Date
Summary Proposal	1.2	01.12.14
Invitation Letter	1.2	01.12.14
Information Sheet	1.2	01.12.14
Consent Form	1.2	01.12.14
Consent Form for the use of quotes	1.2	01.12.14

If the fieldwork goes beyond the date stated in your application, you must notify the Ethical Review Panel via the ERP administrator at uso.erps@keele.ac.uk stating ERP2 in the subject line of the e-mail. If there are any other amendments to your study you must submit an 'application to amend study' form to the ERP administrator stating ERP2 in the subject line of the e-mail. This form is available via http://www.keele.ac.uk/researchsupport/researchethics/

If you have any queries, please do not hesitate to contact me via the ERP administrator on uso.erps@keele.ac.uk stating ERP2 in the subject line of the e-mail.

Yours sincerely

pp

Dr Colin Rigby
Vice Chair – Ethical Review Panel

CC RI Manager
Supervisor

Research and Enterprise Services, Keele University, Staffordshire, ST5 5BG, UK
Telephone: + 44 (0)1782 734466 Fax: + 44 (0)1782 733740

Appendix F:

Relevant Legislation

Relevant Legislation

The Act	Date
The Health Information National Centre in Saudi Arabia	2013
Law of Practicing Healthcare Professions in Saudi Arabia	2005
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
Information Security Policies and Procedures Development Framework for Government Agencies in Saudi Arabia	2011
Anti-Cyber Crime Law in Saudi Arabia	2007
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 J:

Observation form

Observation form

Date: / / Time: AM□ PM□

Observer Name:…………………………….. Department:……………………………

Room Number:……………………………. Comment………………………………

…………………………………………………………………………………..

No	Questions **(Part One)**	Secure	Insecure	Undecided	N/A
1	How do healthcare professionals log in?	□	□	□	□
2	How do healthcare professionals record data?	□	□	□	□
3	How do healthcare professionals log off?	□	□	□	□
Comments and observations:					

No	Questions (Part Two)	Yes/Secure	Yes/In-secure	No	N/A
4	Do they make any copies of the records?	□	□	□	□
5	Do they use their personal devices to use healthcare records?	□	□	□	□
6	Do they use portable or removable media to copy or use healthcare records?	□	□	□	□
7	Do they ask someone else to record the data?	□	□	□	□
8	Do they complete the healthcare records in a timely manner?	□	□	□	□
9	Do they use paper-based records sometimes?	□	□	□	□
Comments and observations:					

No	Questions (Part Three)	Yes	No	Don't Know	N/A
10	Do they show any special commitment to the information security of the healthcare records? (Or do they think that imparting health services is a more important job?)	□	□	□	□
11	Are they comfortable with using information technology and the available devices?	□	□	□	□
12	Are IT devices and healthcare records facilitating the job of the healthcare professionals?	□	□	□	□
13	Are the healthcare records available all the time without any delays or interruptions?	□	□	□	□
14	Are they using encrypted and password protected personal devices which may keep the data safe?	□	□	□	□
Comments and observations:					

No	Questions (Part four)	Intensive	High	Noticeable	Low
15	What are the chances of data being stolen from their clinic?	□	□	□	□
16	What are the chances of data being stolen or lost while they are on the move?	□	□	□	□
17	What are the chances of data being stolen or lost while they are at home?	□	□	□	□
18	What are the chances that healthcare professionals may maliciously compromise the information security in seeking some undue benefits?	□	□	□	□
Comments and observations:					