Information Security in Distributed Healthcare

Exploring the Needs for Achieving Patient Safety and Patient Privacy

Rose-Mharie Åhlfeldt
Abstract
In healthcare, patient information is a critical factor. The right information at the right time is a necessity in order to provide the best possible care for a patient. Patient information must also be protected from unauthorized access in order to protect patient privacy. It is furthermore common for patients to visit more than one healthcare provider, which implies a need for cross border healthcare and continuity in the patient process.

This thesis is focused on information security in healthcare when patient information has to be managed and communicated between various healthcare actors and organizations. The work takes a practical approach with a set of investigations from different perspectives and with different professionals involved. Problems and needs have been identified, and a set of guidelines and recommendations has been suggested and developed in order to improve patient safety as well as patient privacy.

The results show that a comprehensive view of the entire area concerning patient information management between different healthcare actors is missing. Healthcare, as well as patient processes, have to be analyzed in order to gather knowledge needed for secure patient information management. Furthermore, the results clearly show that there are deficiencies both at the technical and the administrative level of security in all investigated healthcare organizations.

The main contribution areas are: an increased understanding of information security by elaborating on the administrative part of information security, the identification of information security problems and needs in cross border healthcare, and a set of guidelines and recommendations in order to advance information security measures in healthcare.
Acknowledgements

Writing a scientific dissertation like this is by its definition an individual effort. However, such work cannot be completed without various people in the environment giving support in different ways. I have met so many people during the process, who have given both inspiration and new knowledge for continuing this work. I appreciate you all and would like to thank you from the bottom of my heart.

First of all, special thanks to my supervisor and friend Benkt Wangler, for your support and always being there when needed. I am so grateful that you were the one who crossed my path at the right time and in the right situation. I would also like to thank the other members of my research supervisor group; Louise Yngström, Eva Söderström and Hans Åhlfeldt. Thanks for all the comments and feedback throughout the process, which have improved the work. Thanks Eva for the hardcore support, not least in the English language.

Many thanks to the IS research group at the School of Humanities and Informatics at the University of Skövde, for all the discussions during the formal as well as informal meetings in the coffee room. Thanks also to Vera Lindroos, for your proofreading of the thesis and Susanne Kjernald, for your support and friendship. Furthermore, thanks to all members of the VITA Nova Hemma project, KIO-network, SWITS and INTEROP.

Special thanks to professor Peter Linington, his wife Janet and the Computing Laboratory at the University of Kent, Canterbury, UK. Thanks for your hospitality, kindness and support during my visit to Canterbury. I will never forget you.

Last, but certainly not least, I would like to thank my family for your inexhaustible support. Roland - my better half and life partner, Daniel and Emma - our lovely children. I love you so much and without you this would not have been possible. Nils-Gunnar and Ingrid – my dad and his wife. I also often think about my mother. I know you would have been proud of me. See you.

Thank you all!
## Table of Content

### PART I  The Research Frame

1  Introduction 3
1.1  The Problem 4
1.2  The Aim 5
1.3  The Research Questions 6
1.4  The Objectives 6
1.5  The Research Approach 7
  1.5.1  Research from Complementary Viewpoints 8
  1.5.2  Elaborating the Information Security Model 8
  1.5.3  Information Security Guidelines and Recommendations for Distributed Healthcare 10
  1.5.4  The Research Design 10
1.6  Research Delimitations 12
1.7  Results and Contributions 13
1.8  Related Research 14
  1.8.1  Related Development Work in Sweden 14
  1.8.2  Related Work on the International Research Scene 16
1.9  Thesis Structure 17

2  Background 21
2.1  Information Security 21
2.2  Information Security Model 22
2.3  Swedish Healthcare 23
  2.3.1  Healthcare Actors and Distributed Healthcare 23
  2.3.2  Electronic Health Record 25
  2.3.3  Acts which Impact on IT in Healthcare 26
2.4  Information Security in Healthcare 31
  2.4.1  Patient Safety and Patient Privacy 35
  2.4.2  Patient Process 37
  2.4.3  The Need for Information Security in Distributed Healthcare 39

3  The Research Design 41
3.1  The Research Strategy 41
  3.1.1  Case Studies 42
  3.1.2  Literature Analysis 42
  3.1.3  Data Analysis 43
3.2  Compiling and Enhancing the Information Security Model 44
### Part II Research Result

#### 4 Initial Research
- **Case No. 1: Information Security in Home Healthcare** 59
- **Case No. 2: Information Security in EHR** 59
- **Case No. 3: System and Network Security in a Heterogeneous Healthcare Domain** 60
- **Synthesized Results** 61

#### 5 The Swedish National Perspective
- **Problems and Needs** 63
- **Positive Aspects** 64
- **Patient Safety and/or Patient Privacy** 65
- **Conclusions** 66

#### 6 International Outlook
- **England** 67
  - **Problems and Needs** 67
  - **National Program for IT (NPfIT)** 68
  - **Patient Safety and/or Patient Privacy** 68
  - **Comparison with Sweden** 69
  - **Conclusions** 70
- **Norway and Finland** 71
  - **Problems and Needs** 71
  - **Positive Aspects** 72
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.4</td>
<td>Scientific Quality</td>
<td></td>
</tr>
<tr>
<td>10.4.1</td>
<td>Credibility</td>
<td>107</td>
</tr>
<tr>
<td>10.4.2</td>
<td>Conformability</td>
<td>107</td>
</tr>
<tr>
<td>10.4.3</td>
<td>Dependability</td>
<td>108</td>
</tr>
<tr>
<td>10.4.4</td>
<td>Relevance</td>
<td>108</td>
</tr>
<tr>
<td>10.4.5</td>
<td>Transferability</td>
<td>108</td>
</tr>
<tr>
<td>10.5</td>
<td>Future Work</td>
<td>109</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>111</td>
</tr>
</tbody>
</table>

**PART III Publications**

| Paper 1        | Information Security in Healthcare: A Case Study                     | 119  |
| Paper 2        | Information Security in Electronic Medical Records: A case study with the user in focus | 131  |
| Paper 4        | Information Security in a Distributed Healthcare Domain: A Case Study | 159  |
| Paper 6        | Information Security Problems and Needs in Healthcare: A Case study of Finland and Norway vs Sweden | 191  |
| Paper 7        | Patient Safety and Patient Privacy in Information Security from the patient's view: A Case Study | 203  |
| Paper 8        | Improving the Information Security Model by using TFI                | 217  |
| Paper 9        | The Need for a Coordinator for Cross Border Healthcare Planning       | 231  |

Appendix          | 239  |
Part I of this thesis consists of three chapters and presents the background and structure of the research.

- **Chapter 1** presents the research problem, aim and objectives together with a brief overview of the research approach, delimitations and contributions. Related research and the thesis structure are also described.
- **Chapter 2** presents the research background through describing important concepts and by providing a deeper understanding of the research problem.
- **Chapter 3** presents the research design in more depth
Introduction

1 Introduction

In healthcare, the patient is the most important actor. According to the Healthcare Act (SFS, 1982), the aim of healthcare is to provide the citizens with good health and with respect to all people’s equal worth and the individual person’s dignity. Hence, one should provide patients with opportunities for the best care, with care decisions based on the right information at the right time, i.e. one should make every effort to obtain as high level of patient safety\(^1\) as possible. Lack of information should not lead to incorrect treatments or unnecessary care activities, such as extra patient visits to the doctors because patient information from a different healthcare organization is unavailable. On the other hand, one must also protect sensitive patient information from being distributed to unauthorized persons, that is, one should strive to maintain patient privacy.

Patient information is thus a critical factor in healthcare and should follow the patient during the whole patient process\(^2\) even if the patient visits more than one healthcare provider, that is, in distributed healthcare\(^3\). Protecting patient information has always been a high priority within the healthcare domain. When electronic healthcare records (EHR) are used, the availability of patient information increases. This places new demands on the healthcare sector to maintain a sufficient level of information security. The requirement for strong security is one reason that the implementation of IT in healthcare has been so slow. Consequently, availability of patient information has not always been achieved. All healthcare records have not yet been computerized, but there is much work going on in this area. In the near future, the whole Swedish healthcare sector will have EHR (SOU 2006:82).

Some work has been done to explore how the healthcare sector fulfils the extensive demands for protecting patient information (SITHS, 1999a; 1999b; 2000). These investigations have primarily focused on one specific type of healthcare provider, the county councils (Section 2.3 further explains how the Swedish healthcare system is organized). However, so far we have not been able to identify any investigation, concerning the level of information

---

\(^1\) The terms patient safety and patient privacy will be further explained in Section 2.4.1.

\(^2\) The term patient process refers to the sequence of investigations, treatments and other activities that the patient experiences during a period of illness. It will be further explained in Section 2.4.2.

\(^3\) Distributed healthcare refers to the healthcare sector including various healthcare actors and organizations. The use of the term will be further explained in Section 2.3.1.
security, that has focused on several kinds of healthcare organizations run by different authorities and which manage the exchange of patient information.

One condition for obtaining a sufficient level of security, in information that is increasingly becoming easily available, is to maintain an adequate quality of protection in the existing systems and networks of healthcare organizations. Several investigations (Data Inspection Board, 1998; 2005) have revealed current deficiencies concerning information security in healthcare organizations, primarily in regions and county councils. These investigations also point to the need for further research in this area.

1.1 The Problem

Information systems in healthcare are important for society. Disturbances can result in serious consequences for the population. Moreover, the information systems involve health information in many forms, from data expressed in words and numbers to medical images. Whatever form the information takes it must always be appropriately protected. Hence, information security in healthcare is an important element to consider.

Most security problems are generic and concern information systems in general. These problems include both technical and administrative aspects of security, but the focus has mainly been on technical security while the administrative part has been omitted. The Swedish Emergency Management Agency (SEMA, 2005) pointed out some significant conclusions concerning all important information systems in Swedish society, for instance: the lack of a comprehensive view of information security; the need for a base level of security in important social welfare systems; the need for a comprehensive political view concerning risks, crimes and threats related to information security; that the main threats are unintentional ones, and the vital need for qualified education. Since these conclusions are generic for information security, the healthcare sector must also address these issues. Hence, there is a need to increase the body of knowledge concerning information security in healthcare, particularly in relation to the administrative part of security.

Swedish healthcare is facing a challenging task in dealing with the increasing number of elderly and infirm citizens (Carelink, 2002). There are reports, which indicate that if healthcare, with limited resources, is to succeed in the future, it needs effective and efficient IT support. The healthcare business claims that IT-support is necessary to preserve and improve service, availability and quality of care (Carelink, 2002). Therefore, maintaining and improving information security in healthcare is a demanding task. According to SEMA (2005), there is a substantial need for research and development in this area.

The Data Inspection Board of Sweden has conducted a number of inspections concerning how Swedish healthcare actors manage and protect

4
patient information to ensure patient privacy (Data Inspection Board, 1998; 2005). These investigations show that there are deficiencies in how patient information in healthcare is managed. Consequently, there is a need for further studies in this regard involving different healthcare organizations in order to explore the problems and needs at a generic level.

In order to achieve an adequate level of care quality and hence to attain patient safety, one needs to have IT support throughout the patient process, as well as effective and efficient work processes. However, the patient information must follow the patient throughout the process, that is, as registered by the various involved personnel or by the patient him/herself. The patient information hence needs to be managed both within an organization, that is, in a particular unit (e.g. a ward) or between different units in the same organization (e.g. a hospital), across organizational borders, (e.g. among hospitals, primary care and municipal home healthcare), and between healthcare organizations and the patient. Consequently, the patient information is to be managed in a distributed environment. This is currently not possible despite the ongoing work to make patient information available to other healthcare providers. When the availability of information increases, additional demands are placed on information security.

To summarize, the healthcare sector faces a great challenge concerning how patient information security can be managed in distributed healthcare in order to achieve both patient safety and patient privacy for the citizens. However, before suitable actions are taken, the nature and content of the demands must first be understood and elaborated, along with an understanding of potential problems that may occur.

1.2 The Aim

Based on the above discussion, the aim of this work is to identify and elaborate, from several perspectives problems and needs regarding information security in distributed healthcare. In doing so, we also aim to propose well founded suggestions for how to achieve a reasonable level of information security, particularly in situations where patient information has to be exchanged between different healthcare organizations.

In order to fulfil the aim, three research questions have been formulated. The following section elaborates on each of these.

\[Section 1.4 \text{ clarifies our view of reasonable level.}\]
1.3 The Research Questions

The following research questions have been formulated:

1. How can information security in healthcare be better understood, particularly in relation to patient safety and patient privacy?

2. What are the particular information security problems and needs concerning patient information in situations involving several healthcare providers and organizations?

3. What security measures are required in order to achieve a reasonable level of information security, taking into account the patient’s need for safety and privacy?

1.4 The Objectives

In order to fulfil the aim and answer the research questions, as formulated above, a number of objectives were drawn up. These objectives together with motivations are listed below.

Since information security is a concern for the entire healthcare sector, it was necessary to conduct investigations with actors and managers from different types of healthcare organizations and authorities in Sweden (objective 1) as well as internationally, to a limited extent (objective 2).

Objective no 1: To identify problems and needs of information security regarding patient information in distributed healthcare from a national Swedish perspective. In order to relate these problems and needs, an information security model will be compiled.

Objective no 2: To obtain an understanding of how problems and needs identified in Sweden compare to the situation in other countries with similar welfare and living conditions. This will be conducted in an international outlook.

Since the patient is the prime object of interest in the healthcare sector, it is important to delve deeper into the actor dimension by further investigating the views of the patients. It is particularly relevant to assess how the patient experiences and values such issues as patient safety and patient privacy.

Objective no 3: To bring to light what patients themselves think when it comes to safety and privacy. In what situations they do and do not object to having their information revealed to others, and when safety is more important than privacy and vice versa.

Administrative security is an important but neglected area. Hence, there is a need to increase the understanding thereof.
Objective no 4: *To obtain an increased understanding of administrative security by elaborating this branch of information security. This will contribute to clarifying what measures are needed to ensure a sufficient level of administrative security.*

In order to achieve a reasonable level of information security in healthcare, it is necessary to provide guidelines and recommendations for people working in the area, in particular when looking at the identified and defined problems and needs in combination with the aims and requirements that the healthcare sector has to fulfil. A reasonable level here refers to a level where the defined problems and needs are practically managed with a firm hand in order to achieve the aims and requirements of the governmental healthcare authorities. A reasonable level of security originates from business analysis, current state analysis and risk analysis in order to determine a suitable level of information security for the healthcare sector.

Objective no 5: *To propose suggestions for security measures that are needed to achieve a reasonable level of security, technical and administrative, by developing a set of guidelines and recommendations.*

In the following section, we further describe our research approach.

### 1.5 The Research Approach

The research has employed a qualitative approach involving a set of explorative studies. This section aims to provide an overview of how the research work has been conducted and implemented, while Chapter 3 describes the research design in more detail.

The research started with an initial phase, which explored problems and needs of information security from a local perspective involving two municipalities, one primary care unit and one hospital. This research resulted in an information security model according to which identified problems and needs were classified. The latter is depicted in Figure 1:1 where each problem is represented by an index. The results were reported in the form of a licentiate thesis January 2006 (Åhlfeldt, 2006). A summary of this work is presented in Chapter 4.

The remaining research included additional views that elaborated on the problems and needs and enhanced the information security model such that it illustrates the results more clearly and explains the content of information security in more detail. Furthermore, a set of guidelines and recommendations for how to achieve a reasonable level of security has been compiled from the results. The following subsections discuss these three aspects together with a description of the research design.
1.5.1 Research from Complementary Viewpoints

One additional requirement for continuing the research concerned how to better ground and possibly extend our results by including complementary views in order to obtain a better coverage of the problems and needs of information security. The complementary perspectives included in the continued work are in reference to the statement above:

1. A Swedish national view (objective 1); to use the information security model to identify the problems and needs of both healthcare authorities and information security managers from multiple regions of Sweden.

2. An international outlook (objective 2); to compare Sweden with several other countries in northern and Western Europe. The UK is particularly interesting since it has an ongoing process of implementing one single system for patient information. Other Nordic countries are also of interest for comparison since they have essentially the same social structure as Sweden.

3. The patients’ view (objective 3); to investigate how patients themselves deal with information security based on the goal of patient safety and patient privacy. This is relevant since the availability of patient information increases when healthcare providers share information.

1.5.2 Elaborating the Information Security Model

The information security model (cf. Figure 1:1) was compiled in the initial phase and is a combination of four common characteristics for achieving information security and the SIS model for security measures (SIS, 2003). The latter is used in order to divide the security measures from an information security perspective. The information security model is further presented in Section 2.2.

However, since the term “information security” includes several security concepts, the information security model has been useful in obtaining an understanding of information security and its content, in research as well as in education. The model has also been a useful tool for expressing where the information security problems and needs arise and exist. Figure 1:1 presents how the initial research has identified a number of problems and needs in the administrative security area. These problems and needs are further described in Chapter 4 and the included Papers 1-3.
One deficiency in the model is that the administrative security aspect has not been further elaborated. The reason is that results of technical measures have in general been given a higher priority for a longer period of time. The need for more attention on administrative security has only recently been recognized (SEMA, 2005). There is hence a need to further detail this aspect of the model, in order to increase the understanding of the information security domain and to develop a well founded theoretical framework which can be used both in the analysis and the design phase of interoperable systems (objective 4). The approach is a literature analysis with the principal aim of studying other information security models, primarily where administrative security is taken into account (Björck, 2005; and Liebenau and Backhouse 1990).

Figure 1:2 illustrates the PhD work direction. The section above the dotted line illustrates research reported in the licentiate thesis, while the part below the dotted line illustrates the complementary work, that is, the different additional views, as well as the elaboration of the information security model and the set of guidelines and recommendations. The domain for the research work was the healthcare sector including various healthcare actors and organizations.
Introduction

1.5.3 Information Security Guidelines and Recommendations for Distributed Healthcare

In order to obtain a set of guidelines and recommendations (objective 5) for people working with information security issues in the healthcare sector, practitioners as well as authorities, the results from the complementary views (objective 1-3) together with the results from the initial work (objective 1) have been further analyzed in the synthesis. Furthermore, the set of guidelines and recommendations has been elaborated from the synthesis and then visualized in the extended information security model (objective 4).

1.5.4 The Research Design

In order to fulfil the aim, obtain answers to the research questions and achieve the objectives, the thesis has applied a practical approach in the form of an explorative study. Furthermore, in order to achieve a sufficient coverage of the problems and needs concerning information security in healthcare, seven case studies have been conducted to cover healthcare
actors from different healthcare organizations. A literature analysis has also been carried out in order to increase the understanding of administrative security. The research approach is further elaborated in Chapter 3. Figure 1:3 visualizes the research design. The initial research is included in research question 2 and constitutes the local part of the first objective.

Figure 1:3  The research design with respect to the aim, research questions and objectives.

The results from the case studies in the initial work are reported and published in the following papers included in the thesis:

Case study 1    Paper 1  Information Security in Home Healthcare: A Case Study
Case study 2    Paper 2  Information Security in Electronic Medical Records: A case study with the user in focus.
Case study 3    Paper 3  System and Network Security in a Heterogeneous Healthcare Domain: A Case Study
The results from the remaining case studies, literature analysis and a part of the synthesis are reported and published in the following papers included in the thesis:

Case study 4  Paper 4  Information Security in a Distributed Healthcare Domain: A Case Study
Case study 5  Paper 5  Information Security Problems and Needs in Healthcare: A Case Study of England vs Sweden
Case study 6  Paper 6  Information Security Problems and Needs in Healthcare: A case study of Norway and Finland vs Sweden
Case study 7  Paper 7  Patient Safety and Patient Privacy in Information Security from the Patient’s View: A Case Study
Literature analysis  Paper 8  Improving the Information Security Model by using TFI
Synthesis  Paper 9  The Need for a Coordinator for Cross-Border Healthcare Planning

The specific research question, aim, objectives, as well as approach and results from the initial research are further presented in Chapter 4. Summaries of the results from the case studies 1-7 and the literature analysis are further presented in Chapters 5-8.

1.6 Research Delimitations

The research area of this thesis is located at the intersection of the domains information security and healthcare. Healthcare is controlled by legislation and regulations that are often nationally unique, even if many nations have similar laws. Our work is mainly based on Swedish healthcare and the laws and regulations that control it. An international outlook is however, included as a specific activity, although the Swedish conditions are in focus. We refer to it as an “international outlook” to emphasize that it only concerns a few countries in north Western Europe. Contrasting other countries with the Swedish situation could also have been of interest. The choice of countries included in the outlook firstly depended on our criterion that they should more or less have the same welfare and living conditions as Sweden, since they would be compared with the Swedish situation. Secondly, the choice depended on our contacts and the opportunities that would make it possible to carry out the study within the limited timeframe that was available. England is of particular interest since their approach to implementing IT and information security in healthcare differs completely from the Swedish approach. Norway and Finland are good examples of countries with similar social and organizational structures as Sweden, but differ in their views and ways of managing information security in healthcare.
Introduction

The study applies to the public healthcare sector. Although private healthcare providers are not explicitly investigated, one provider is included as a minor part of one study in the initial work. The private sector also needs further investigation in the future, since privatization of hospitals and primary care units means that the importance of information security is steadily growing in Sweden. However, since a distributed healthcare implies a number of different healthcare organizations, the private sector has been excluded in order to narrow the focus.

It is worth emphasizing that this work focuses on information security as a whole, that is, it includes technical as well as administrative and organizational aspects. The concept is further defined and described in Section 2.1.

The intention is not to identify all the problems and needs of the area, but to identify the most important ones in order to achieve appropriate answers to the research questions.

1.7 Results and Contributions
The healthcare sector is burdened with considerable demands not least in the IT area. Patient information shared between different healthcare organizations must be reliably transmitted and distributed in order to provide good quality patient care and at the same time guarantee privacy. Thus, to achieve this, information security in healthcare must maintain high quality.

Our work contributes with the following:

• providing an increased understanding of information security by compiling and extending an information security model, and by emphasizing the entire concept of information security and the need to address administrative security particularly, and by relating patient safety and patient privacy to the information security area
• identifying existing problems and deficiencies in the area of information security and the existing security needs of distributed healthcare, and by stressing the importance to identify and analyzing the patient process as well as the patient involvement
• suggesting solutions for those responsible for and working with security issues in all levels in cross-border healthcare by providing a set of guidelines and recommendations to advance information security measures in distributed healthcare.
• providing a comprehensive view by covering several perspectives from different healthcare organizations and from different actors in the healthcare sector as well as the patient him/herself

These contributions are more extensively elaborated in Section 10.3.
1.8 Related Research

This section presents related work in the area of information security in healthcare. It is divided into two parts: related development work in the Swedish healthcare sector as well as related work on the international research scene.

1.8.1 Related Development Work in Sweden

Many healthcare organizations consider the most important healthcare process to be the patient process (SITHS, 1999a). As previously mentioned, this is the process that takes the patient through a sequence of treatments and other care activities. This may involve contacts with several different healthcare providers. It consequently demands that these providers cooperate with the patient and each other, in order to achieve high quality care for the patient. The patient information must accompany the patient throughout his/her contact with the different healthcare providers. However, there are different opinions about how the patient process should be supported. Consequently, a number of business projects have been started and some of them are presented below.

The organization, Carelink, was established in 2000 for the purpose of advancing the use of IT in Swedish healthcare. Carelink runs several projects which include a uniform electronic directory, a common infrastructure, facilitating communication between systems, creating a virtual medication list, and establishing a common terminology and other common standards. The aim of the National Patient View is to compile predefined data concerning a unique patient. Only an authorized healthcare provider with patient consent can search and access that patient information. Furthermore, only basic information will be presented, irrespective of where the information is documented. In addition, the service will only provide an opportunity to read information, not writing. The aim is for all healthcare providers, public as well as private, to have access to the Patient View in the future. In addition, patients should have access to their information (SOU 2006:82).

In the Stockholm area, a similar project is concerned with compiling information from different care providers into the so-called, Common Care Documentation (in Swedish: gemensam vårddokumentation, GVD). The aim is to store patient information from the council’s public and private healthcare providers in a common care database. In order to obtain access to patient information, a care relationship with a patient is required. To access patient information from another healthcare provider, the patient must give his or her consent to the use of the information thus exposed (SOU 2006:82).

Furthermore, an on-going project, in the eastern region of Sweden, works with the integration of different healthcare systems using a service based
platform architecture to create IT-support. In addition, a number of fundamental base services such as authentication, access logs and Single Sign on etc. are connected to the platform. The platform can then connect other service components, such as time reservation systems and national registration systems. Furthermore, they have chosen a technical authorization system which uses passwords and various logging techniques. The project also uses an authorization system in which the patient must give his/her consent to the exchange of information (SOU, 2006:82).

Another project in the south of Sweden, The Clinical Portal, deals with the same issues as the projects mentioned above. This project includes a number of accessible compiling services, such as Care Survey, Important Medical Information and a Common Medicine List. Healthcare professionals must have an allocated authority to access some of the services in the Clinical Portal. Furthermore, he or she must use a smart card for authentication. Since all the information passing the Clinical Portal is logged, it is possible to see what kind of information has been sent, to whom and when (SOU 2006:82).

Carelink (2002) has made a survey of the use, needs and visions of IT in municipal care. The report shows, for instance, that there is considerable need for cooperation across the boundaries of other care providers to achieve information exchange. Such exchanges can be provided using IT, but results indicate that new solutions for communication techniques for this purpose are required. Even in the simplest care activity where the patient has contact with different healthcare providers, or physically moves between them, information must be available at the right time to the right person. There is a need to access the necessary patient information in order to guarantee safe and secure care regardless of the patient’s place in the care chain. Results also show that competence development and education among the staff is required. When the municipalities introduce IT-support, new requirements arise for the professional roles (Carelink, 2002).

Common to these projects is the need for a holistic view of information security. This should not only include a cooperative infrastructure for information security, but also techniques concerning strong authentication, as well as generic services, such as authorization, access controls, accountability, confidentiality and so on. The SITHS project has created an infrastructure and model to meet all the demands mentioned above. However, these measures have not yet been adopted by the healthcare organizations and only the few pilot projects mentioned above are in progress. Consequently, there is still a long way to go. One of the reasons for the delay is limited economical resources. The projects show that there is also a need for further studies and research in this area. Above all, it is necessary to point out the advantages in the long-term perspective (Carelink, 2003a).
1.8.2 Related Work on the International Research Scene

Internationally, there is extensive work in progress to integrate different healthcare systems with different healthcare units. The demands, stated in the projects above, are not unique for Swedish healthcare. Even if traditions, culture and legal aspects differ between countries, the main problems are the same. The European Commission states in the eHealthNews (2006) that Europe still underestimates the risks of insufficiently protecting networks and information. Security presently represents only about 5-13% of IT expenditure. Consequently, the European Commission is promoting a greater awareness through an open and inclusive multi-stakeholder dialogue on a new IT security strategy for Europe. A key-role in that concern is to be placed on public authorities, although it is largely up to the private sector to provide solutions (eHealthNews, 2006).

Strong authentications and generic services, such as authorization, access controls, accountability, integrity and confidentiality, have been important requirements to meet for a long time (Blobel, 1997; 2000; Blobel and Roger-France, 2001; and CEN, 1999). In order to support strong authentication, the use of hard certificates, for example smart cards, is preferable (Wenzlaff et al., 1999). In the DIABCARD project (Blobel et al., 2001) the aim is to implement and evaluate a chip card based medical information system to facilitate communication and cooperation between healthcare professionals in different organizations or departments caring for the same patient. Issues that have also arisen in this project include the lack of a coordinated infrastructure, as well as social and psychological aspects, such as the acceptance of electronic means in electronic commerce (Blobel et al., 2001).

When healthcare systems are to be integrated, the interest in a process oriented approach for healthcare information systems increases (Poulymenopoulou et al., 2003). There is a need to look at the healthcare processes in a more holistic way, especially the patient process which involves several healthcare providers. This patient process has both a technical and an organization level. Technically it implies that different institutions are connected in an IT system in which the process focuses on providing equal access to healthcare information for all the involved care providers and under the conditions of the continuity of care that cross the borders of individual healthcare organizations (Vissers, 1998). The organizational level implies collaboration, cooperation and coordination among the involved care providers (Winge et al., 2007). This situation not only increases the technical and organizational security demands. It is also important to maintain patient privacy when patient processes are extended into distributed systems, which also include sensitive information. Louwerse (1998) claims that distributed systems in healthcare demand increased awareness, improved procedures and software, and a more centralized approach or systems management.
Introduction

One way for the healthcare units to become process-oriented and integrated with other units’ processes and IT systems is to introduce a process manager, who visualises and executes the communication between different IT systems. The process is realized by using graphical and executable process models. Furthermore, the process manager also communicates directly with the healthcare personnel via desktop computers and mobile devices. VITA Nova (Perjons et al., 2005a) was a Swedish project which introduced a prototype system for healthcare processes based on a process manager. The result reveals, for example, that when a process manager is introduced in healthcare, new ways of dealing with security issues (protection, ethics, and legality) are required. The healthcare units also revealed significant differences in security awareness and IT maturity.

Transferring information between organizations must be achieved by designing solutions that satisfy and meet the demands of the patient, the patient’s relatives and legislation. If healthcare in the future is to integrate its business processes with those of other care providers, and if the transfer of patient information is to be satisfactorily performed from a security perspective, routines for a minimum level of security must be designed, documented and implemented jointly by all involved units (Perjons et al., 2005a).

In the report for the World Summit on Information Society (WHO, 2005), the WHO states that the barrier to increasing the implementation of eHealth is no longer only technical or financial. The greatest challenge in this context is the ability to plan and implement eHealth on a large scale, while adapting it to local health problems. This is also the goal of the initiative i2010: European Information Society 2010. “It is an enormous task, and one that cannot be achieved alone – active collaboration is crucial” (WHO, 2005, p1).

With regards to information security in eHealth, WHO states that basic security measures are required to ensure that critical resources and building a global culture of security and cooperation is vital. “A holistic approach includes technology measures, standards, legislation, norms and education. Since the legal process is often slow, other complementary measures need to be taken, such as industry initiatives, better enforcement and international cooperation” (WHO, 2005, p. 7).

This thesis illuminates some of the needs mentioned above, such as a holistic approach to public healthcare coverage, and points out the necessity of information security in the long-term perspective, as well as including new knowledge in this research area.

1.9 Thesis Structure

This thesis consists of three parts. The remainder of Part I comprises a presentation of the terminology of information security and its impact on the healthcare domain. An elaboration of the research approach follows. The
Introduction

The purpose of Part I is primarily to provide an extended background to the papers included in Part 3 of the thesis.

Part II contains descriptions and results from the different case studies and activities included in the work. The purpose of Part II is primarily to provide a summary of the particular perspectives presented in the papers included in the third part together with the presented results derived from the synthesis. This part of the thesis also includes a discussion of the research contribution and quality.

Part III comprises nine publications, of which each reports on research of information security from the thesis perspectives. In Papers 1-3, the focus is on the national Swedish perspective from a local view, while Paper 4 focuses on the national Swedish perspective from a management view. While the emphasis, in Paper 5, is on the international outlook with England in focus, Paper 6 also concentrates on the international outlook but with Norway and Finland in focus. Paper 7 emphasizes the patients’ view of information security with a particular focus on patient safety and patient privacy. In Paper 8, the attention is on the elaboration of the information security model and how it could be improved by using TFI\(^5\). Finally, Paper 9 emphasizes the need of a coordination function in order to increase the patient safety in cross border healthcare planning. Papers supporting the thesis indirectly but not included are presented in Section 3.5.3. In Table 1:1, the overall structure of the thesis is presented.

---

\(^5\) The TFI-model adapting the view of an information system as constituted of the technical (T), formal (F) and informal (I) elements
### Table 1:1 Structure of the thesis

<table>
<thead>
<tr>
<th>Part I</th>
<th>Chapter 1</th>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chapter 2</td>
<td>Background</td>
</tr>
<tr>
<td></td>
<td>Chapter 3</td>
<td>Research Design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part II</th>
<th>Chapter 4</th>
<th>Initial research</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Chapter 5</td>
<td>The National Perspective</td>
</tr>
<tr>
<td></td>
<td>Chapter 6</td>
<td>The International Outlook</td>
</tr>
<tr>
<td></td>
<td>Chapter 7</td>
<td>The Patient’s View</td>
</tr>
<tr>
<td></td>
<td>Chapter 8</td>
<td>The Extended Information Security Model</td>
</tr>
<tr>
<td></td>
<td>Chapter 9</td>
<td>Synthesized results and Suggested Guidelines and Recommendations</td>
</tr>
<tr>
<td></td>
<td>Chapter 10</td>
<td>Concluding Discussions and Suggestions for Future Research</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper 1</th>
<th>“Information Security in Home Healthcare: A Case Study”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Paper 2</th>
<th>“Information Security in Electronic Medical Records: A Case Study with the user in focus”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Paper 3</th>
<th>“System and Network Security in a Heterogeneous Healthcare Domain: A Case Study”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Paper 4</th>
<th>“Information Security in a Distributed Healthcare Domain: A Case Study”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Submitted and early accept to the Health informatics Journal.</td>
</tr>
</tbody>
</table>

|---------|--------------------------------------------------------------------------------------------------|

<table>
<thead>
<tr>
<th>Paper 7</th>
<th>“Patient Safety and Patient Privacy from a Patient’s View: A Case Study”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Paper 8</th>
<th>“Improving the Information Security Model by using TFI”</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Paper 9</th>
<th>“The Need for a Coordinator for Cross-Border Healthcare Planning”</th>
</tr>
</thead>
</table>
Introduction
2 Background

This chapter presents an overview of concepts significant for this thesis. Firstly, information security is described in general, followed by a presentation of the information security model. Thereafter, a short account of Swedish healthcare actors is presented along with an explanation of how they are organized. Finally, the notion of information security in healthcare is discussed more explicitly, including descriptions of the concepts, patient safety, patient privacy and the patient process.

2.1 Information Security

In the context of information systems and information technology (IT), information security is an all-embracing concept, which has become more and more common, and comprises, in fact, all parts of most businesses. Accordingly, there is a need to consider information security issues both from a comprehensive as well as a practical level. The Swedish National Encyclopedia (NE, 2007) states that information security focuses on the information the data is representing and on related protection requirements.

According to ISO/IEC 27001, (2006) information security has historically been called a number of different things, for instance, data security, IT security and computer security. The correct term to use is information security because information is always and most certainly, worth much more than the computers or networks it runs on (ISO/IEC, 2006). SIS (2003) has classified the terms in hierarchical order, cf. Figure 2:1.

![Figure 2:1 SIS conceptual classification of different security concepts (SIS, 2003)](image)

Information security covers security issues in all kinds of information processing and could be seen as a process of protecting information assets, aiming to achieve availability, confidentiality, integrity and accountability (SIS, 2003; ISO/IEC, 2005a). Traditionally, the most common key characteristics form the core principles of information security:
confidentiality, integrity and availability. These are known as CIA. Confidentiality relates to protecting data unauthorized access. Integrity concerns protection against undesired changes, and Availability refers to the expected use of resources within the desired time frame.

It has been suggested and argued that other terms should be added to the concept of information security. SIS (2003) has added accountability as the fourth characteristic of information security derived from BS 7799 (2002), ISO/IEC 17799 (2005a) and ISO/IEC 27002 (2005b). Accountability refers to the ability to distinctly trace performed activities to an individual. Someone is personally accountable and responsible for the protection of an asset or set of assets. The emphasis here is on someone and being personally accountable.

Both technical and administrative security measures are required to achieve these four characteristics. Administrative security concerns the management of information security; strategies, policies, risk assessments and so on. Furthermore, planning and implementation in security work requires a structured way of working. This part of the overall security is thus at an organizational level and concerns the business as a whole. It is positioned towards what the overall security requirements should be. Technical security deals with measures to be taken in order to achieve the overall requirements. Technical security is subdivided into physical security and IT security. While physical security concerns, for instance, the physical protection for data media and alarm, IT-security refers to the security of information in technical information systems. IT-security can then be subdivided into computer- and communication security. Computer Security relates to the protection of hardware and its contents, while Communication Security involves the protection of networks and other media that communicate information between computers.

2.2 Information Security Model

In order to better understand how these characteristics and the security measures relate to one another, an information security model was developed and used in the initial research. (Figure 2:2). The aim of the model is to describe, in a simple way, what information security represents. The model combines the definitions and descriptions mentioned above.
The main concept, information security, is situated in the middle. The four characteristics are placed at the top and together represent information security. To fulfill only parts of them is not enough; all the organizations’ requirements concerning these characteristics must be fulfilled in order to achieve information security. The lower part of the model presents the different security measures, ranked in hierarchical order. These are obtained directly from the SIS conceptual classification (SIS, 2003), cf. Figure 2:1. Required security measures include both Technical and Administrative security.

2.3 Swedish Healthcare

The research work has a focus on Swedish healthcare. This section includes a brief description of the actors in Swedish healthcare and how they are organized. The laws that impact Swedish healthcare are subsequently also briefly described. In addition, the situations for the countries included in the International Outlook view are described in Chapter 6.

2.3.1 Healthcare Actors and Distributed Healthcare

Many different actors carry out Swedish healthcare which has a decentralized care system, with 20 county councils and 290 municipal councils as principals and healthcare providers (Ministry of Health and Social Affair, 2007). Public healthcare is the responsibility of regions, county councils and municipalities, while private healthcare actors play a main role in the large cities (The National Board of Health and Welfare, 2004). However, both county and municipal councils employ the services of private care providers to a greater or lesser extent (Ministry of Health and Social Affair, 2007). Since this work is focused on the public healthcare, the private sector will not be further described.
Swedish public healthcare can be divided into three parts: primary care, secondary care and home healthcare. Primary care is the first instance that citizens normally contact when they need medical care. It is mainly provided by healthcare centers located in different geographical areas. Some types of special open clinics located in hospitals also offer primary care. Secondary care constitutes special care located in hospitals to which patients are admitted for treatment for a period of time (The National Board of Health and Welfare, 2004).

Home healthcare is defined as non-institutional care that through the commitment and liability of the responsible authority is provided in the patient’s place of residence. This type of care should be of some duration, usually more than two weeks, though shorter periods of care exist in practice (Landstingsrevisorerna 2000).

Swedish geriatric care has traditionally been the responsibility of two authorities. The county council has the total responsibility for measures that need medical competence, while the municipality is liable for the social efforts which include living conditions, social service, technical aid and economical support (The National Board of Health and Welfare 1996). However, at the beginning of 1992, the Ådel reform came into effect, which made municipalities responsible for long-term services as well as care for the elderly and the disabled except that involving physicians. The municipalities became liable for nursing in specially constructed service houses, homes for the aged, group residences and nursing homes. The municipalities became responsible for payment to the county councils for all somatic long-term medical care and for medically finished treatments. The municipalities’ responsibility of payment has probably contributed to shorter nursing time at hospitals for older patients and reduced the number of hospitals beds for somatic short-term medical treatment. The goals for the care of elderly people in the future emphasize their right to their own living quarters with attached care facilities, the needs for cooperation between different care providers, support from relatives, as well as special forms of accommodation and care for citizens with exceptional help needs. Furthermore, the Ådel reform provided the opportunities for the municipalities and county councils to make individual agreements concerning the responsibility for the organization of primary as well as home healthcare. However, the authorities responsible for the nursing and care organizations differ throughout the country (The National Board of Health and Welfare, 1996 and Ministry of Health and Social Affairs, 2007).

Various healthcare actors and organizations need to interact and communicate with each other and with the patient in order to fulfil the aim of the healthcare. As mentioned, patient information must be managed at different levels; within the healthcare organization, between healthcare organizations, and between healthcare organizations and the patients. Different terms can be used to describe this situation, for instance; seamless
healthcare, cross-border healthcare or a process oriented healthcare. In our research we chose the term “distributed healthcare”. Figure 2.3 illustrates the various Swedish healthcare actors in said distributed healthcare.

![Distributed Healthcare Diagram](image)

**Figure 2.3 Healthcare Actors in the Swedish Healthcare Sector.**

### 2.3.2 Electronic Health Record

One of the most central units of care information is the patient record. The traditional paper-based patient record used in a healthcare setting generally contains the notes of the clinic staff and other care providers. These notes are often supplemented with data from other sources; various laboratory tests as well as other tests results, such as X-rays, pathology, ultrasound, lung function and endoscope (Bemmel and Musen, 1997).

Dahlin and Arnesjö (1996) argue that the overall purpose of the patient record is to facilitate and support the provision of excellent and secure patient care. This purpose presumes that the recorded data is reliable and available when needed for that care and understandable for the care providers.

Furthermore, Dahlin and Arnesjö (1996) describe patient record documentation as a “documentation wheel” with many spokes. It includes everything from registration of administrative patient-related information to pure medical data, such as anamnesis, status and diagnosis. All the included documentation is important and must be available and managed by computerized record systems.
According to Dahlin and Arnesjö (1996) the advantages of EHR are, for instance: extensive availability, diverse presentation possibilities, searchability, a possibility for quality development, and so on.

In order to use all these advantages, the authors claim that an openness towards obtaining new technology is required and that information and information transmission are standardized, which is illustrated in the following quotation: “In that case, the EHR will in the future be more user-friendly and useful, standardized and certified, i.e. quality tested and quality approved” (Dahlin and Arnesjö 1996).

Despite the advantages mentioned above, the implementation of EHR in Swedish healthcare has been slow. Currently, almost all (95 %) primary care centers have EHR, but only 69 % of the employees in hospitals use it (Jerlvall and Pehrsson, 2006). In only nine of twenty-one county councils are hospitals able to exchange digitalized information with the primary care. Furthermore, only every other county council can share information between hospital clinics. From a patient perspective, collaboration between county councils and municipalities is crucial. The systems thus far essentially reflect that healthcare organizations have implemented EHR independently of one another. Since the implemented systems are autonomous, the organizations are trapped in their old systems and have difficulty communicating with each other when demands arise for better communication between different healthcare providers in order to provide the required patient care. These old systems are, however, too expensive to simply discard. Therefore, new requirements arise for solutions that integrate old systems and achieve interoperability between the different healthcare organizations.

In order to facilitate coordinated care planning between municipalities and county councils, IT-support with message management has been implemented in several county councils. Thus far, nine councils are completed, and six more are currently implementing coordinated care planning (Jerlvall and Pehrsson, 2006). There is considerable support within this area for the information to follow the patient. The National Strategy for eHealth (Ministry of Health and Social Affairs, 2006) focuses on these issues and the Patient Data Proposal (SOU 20006:82) is investigating the legal conditions in order to facilitate the desire of the supporters (Jerhvall and Pehrsson, 2006).

2.3.3 Acts which Impact on IT in Healthcare

Swedish healthcare is controlled by a number of acts, regulations and statutes. There are six specific acts that effect EHR; Freedom of the Press Act, the Secrecy Act, the Patient Record Act, the Health and Medical Personnel Act, the Personal Data Act and the Act on Healthcare Records (Utbult et al., 2004).
The Freedom of the Press Act is one of the Sweden’s constitutional laws from 1766. According to the interpretation of the act, all patient records in public healthcare are public documents. Since this is not compatible with patient privacy requirements, the Freedom of the Press Act is complemented by The Secrecy Act. In the private sector, the Secrecy Act corresponds to the Health and Medical Personnel Act. The Personal Data Act is related to The Act on Healthcare Record. Finally, the Patient Record Act places demands on how healthcare providers manage the patient records. Figure 2:4 illustrates how these acts are related to one another (Utbult et al., 2004).

The most important acts that impact the use of IT in healthcare are: The Health and Medical Service Act, The Patient Record Act, The Secrecy Act, The Personal Data Act and The Act on Healthcare Records. Each is described below.

**The Health and Medical Service Act**
The Health and Medical Service Act (SFS 1982:763) is a frame act, which mainly includes the aim and directions of healthcare. The act states that the overall aim of the health and medical care services is a healthy population and healthcare on equal terms. Priority is to be given to those with the greatest need of care. According to the Ministry of Health and Social Affairs (2006, p. 6) the act has a number of criteria that must be met if healthcare is to be considered of a “high standard”. Healthcare must:

- be of good quality, based on scientifically established knowledge and proven experience
• be based on respect for patients' dignity and right to self-determination and be open to patient participation and influence
• be accessible
• offer patients the greatest possible degree of choice
• provide citizens and patients with comprehensive information on access to health and elderly care and on the quality and effect of these services
• use care resources efficiently, effectively and responsibly

Furthermore, patients must be given individually adapted information about their health status and existing methods of investigation, care and treatment. If the information cannot be given to the patient, it must be given to the person designated the patient’s next of kin. The act also includes regulations concerning the healthcare and management responsibility of county councils and municipalities (SOU, 2006:82).

The Patient Record Act

The Patient Record Act (SFS 1985:562) came into force 1985 and is technically independent, that is, it concerns information on paper as well as information in any other form of medium. The act uses the term journal documentation, which implies everything pertaining to medical information. Those persons who are obligated to handle patient records according to the act are either certified or specifically appointed individuals who engage in a special profession or people with no certification who perform the tasks which otherwise would be carried out by speech therapists, psychologists or psychotherapists. In addition, people who work as occupational therapists, welfare officers or physiotherapists are also obliged to handle patient records according to the act (Sjölenius, 1996).

Within healthcare, patient records shall be recorded in circumstances of care, the examination and treatment of patients. A patient record shall contain data about the patient’s identity, anamnesis, diagnosis as well as the treatment and requirements of care. Furthermore, the record shall contain information regarding the identity of the person making a notation and when it is written. The recorded notation shall, if nothing particular prevents it, be signed by the person responsible for the data (Sjölenius, 1996).

It is important for the credibility of healthcare that security is guaranteed and that no recorded data is accessible to unauthorized persons. In this context, one can talk about internal and external secrecy. The patient record regulates the internal secrecy, that is, questions concerning the routines for the use of the patient record within the business area where the patient record is stored. The external secrecy is regulated by The Secrecy Act (Sjölenius, 1996).

In §7 it is prescribed that every handling of the patient record is to be achieved and stored so that no unauthorized persons can have access to it. In the case of care, access should be limited to that part of the staff requiring the patient records in their work. Respect for a patient’s privacy requires that
no one outside this circle has access to the record. Reading patient records from sheer curiosity can never be permitted.

Data in a record document may not be deleted or made unreadable in cases other than those referred to in §17 of The Patient Record Act, and additionally in the cases of prescribed screening. Concerning the correction of faults and errors, it should be shown when the correction is done and who made it (Sjölenius, 1996).

If a record document, a transcription or a copy of a document is distributed to someone else, the person sending it shall identify and sign in the patient record who is to receive the document, transcription or copy as well as when the record is distributed. A record document shall be stored for at least three years after the last data is recorded in it (Sjölenius, 1996).

**The Secrecy Act**

The Secrecy Act (SFS 1980:100) concerns regulations about the obligation to observe professional secrecy in public business and prohibits the distribution of public documents. The aforementioned includes limitations of the regulations for the rights of access of public documents provided in The Freedom of Press Act. The regulations concern the prohibitions to display information either verbally or by distributing public documents in other ways. The Act also includes regulations concerning limitations on the right to publish information or its use in radio programs, films, audio recordings or other media where basic regulations are provided by The Freedom of Press Act and The Freedom of Speech Act (SFS 1980:100).

The primary purpose of the Secrecy Act is to protect people’s privacy. In healthcare, secrecy applies to information about the state of health or other private circumstances of individuals in the event that the information, if revealed, could be disadvantageous to a private person or someone close to him/her. Furthermore, secrecy applies to the business of the management of medical records in private healthcare, information about the state of health or other private circumstances of the individual. Information can only be available to the healthcare staff if it is necessary for the treatment of the patient. This kind of secrecy of public documents has been in force for 70 years (Sjölenius, 1996).

**The Personal Data Act**

The Data Act (SFS 1973:289) came into force 1973 and was one of the first acts in the world concerning restrictions in the handling of personal data. The Data Act applies license requirements to store names or other computerized data about people. The purpose of the act was to protect individuals from the indiscreet encroachment of information through automatic data processing by governments or other private interests. There is a widely spread public apprehension that the Data Act has become antiquated and lost its consideration in the public legal conscience. The
above mentioned requirements have resulted in a new act, one more concerned with the storage of personal data without any particular bureaucracy but the application of restrictions about what is permitted and what is not (Carlén-Wendels, 1998).

The Personal Data Act (SFS 1998:204) contains provisions to protect people against violation of their personal privacy by the processing of personal data. The Act, which is adapted to EU rules, came into force on October 24, 1998.

According to this new act, the processing of personal data includes, for example, the collection, recording, storage, adaptation or alteration, compilation or retrieval of information. The Act also applies to personal data transmitted, disseminated or made available by other means. There is no requirement that data, which is processed by computer, should be structured in a register or the like (Ministry of Justice, 2006).

Personal data may only be processed if the registered person (data subject) has given consent, but there are exceptions. Very stringent rules apply to the processing of particularly sensitive personal data. Such sensitive personal data includes, for example, information about health, political opinion and religion (Ministry of Justice, 2006).

In the area of healthcare, very extensive processing of personal data exists. Almost every unit in healthcare will soon be computerized. Computers and their information systems are used for cash processing, appointment reservations, examinations, in casualty departments, clinics, and so on. These information systems have a character of sensitivity because the data in them concerns information about people’s health. In a healthcare record, the healthcare staff must note everything needed for the care of the patient. Furthermore, information may exist, for example, about compulsory care and criminality (Data Inspection Board, 1998).

According to the report from the Swedish Data Inspection Board (DIB) about patient registration in hospitals, the Data Act does not require any permission from the DIB with regard to patient information processing for authorization processes in the healthcare area. This exception mainly concerns patient administration systems of hospitals and other care units (Data Inspection Board, 1998).

With regard to computerized healthcare records, permission from the DIB to manage those records must exist because these records contain more information than health and illness, for example, valuations, opinions, custody data, criminality data, and so on.

The Act on Healthcare Records
Background

records. The Act’s definition of healthcare encompasses dental care, compulsory psychiatric, as well as legal psychiatric care, and infection protection care. In the Act on Healthcare Records there are no provisional regulations. Therefore, all records concerned with the Act are included in the Act’s regulations from 24 October 1998 (Data Inspection Board, 1998).

While according to The Act on Healthcare Record, the data, which is described as sensitive by the Personal Data Act, cannot be used as searchable terms in the healthcare record, the data concerned with the ailment and patient’s state of health can be used. Only those who need access to the data in order to perform their work can have direct access to the data in the healthcare record. The acquisition of the data can only refer to the data needed for the performance of care (SFS 1998:544).

The patient may have access to information about the management of the record. According to the Act of Healthcare Record (SFS 1998:544), the information shall include, among other things, explanations about:

- the identity of the controller of personal data
- the purpose of the register
- the type of information included in the register
- the secrecy and security regulations enforced by the register
- the right to make corrections
- if the registration is voluntary

2.4 Information Security in Healthcare

Information security as a term has been described previously in this chapter. However, in SITHS’ (1999b) second report, the information requirements are summarized, without considering IT or other aids, as “The right information to the right person in the right time and at the right place”, cf. Figure 2:5 (SITHS, 1999b). This is meant more as a vision than a definition, and the following descriptions further clarify the concepts:

- The right information implies that one is provided with sufficient correct and uncorrupted information.
- The right person implies that the person with the specified role in a particular situation has access to the information. People are given different roles for different situations, for example, citizens, politicians, physicians, and so on.
- The right time means that the information is offered when it is needed.
- The right place refers to the information being available where it is needed.
It is notable that usability is not mentioned as a security requirement in the vision. If a user does not understand how to manage the information provided, even with sufficient infrastructure, information security could possibly be disregarded.

If IT-support is used for handling information, the requirements are further enhanced. To achieve the above mentioned vision of information security, the SITHS-project presents a summary of the basic functions of information security (Table 1:1) in the report (SITHS, 1999b).
Table 2.1. Information security (From SITHS, 1999b, pp. 46)

<table>
<thead>
<tr>
<th>Information Security</th>
<th>Administrative Security</th>
<th>System Security</th>
<th>IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>Security obtained with help from related administrated resources</td>
<td>Connect security with transmission or steering signal</td>
<td>Authority</td>
</tr>
<tr>
<td>IT-security</td>
<td>Communication Security</td>
<td>IT-security</td>
<td>Authority</td>
</tr>
<tr>
<td>Accountability</td>
<td>Distinctly trace performed activities to an individual</td>
<td>IT-security</td>
<td>Control of given identity</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Receiving or dispatch of a message can never be denied</td>
<td>Non-repudiation</td>
<td>Control of given identity</td>
</tr>
<tr>
<td>Accountability</td>
<td>Accountability</td>
<td>Accountability</td>
<td>Non-repudiation</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Data must not be accessible to unauthorized people</td>
<td>Confidentiality</td>
<td>Accountability</td>
</tr>
<tr>
<td>Accountability</td>
<td>Accountability</td>
<td>Confidentiality</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Availability</td>
<td>To use resources as required in expected extension and within desired line</td>
<td>Availability</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Accountability</td>
<td>Accountability</td>
<td>Availability</td>
<td>Accountability</td>
</tr>
<tr>
<td>Integrity</td>
<td>Protection against undesired changes</td>
<td>Integrity</td>
<td>Accountability</td>
</tr>
<tr>
<td>Accountability</td>
<td>Accountability</td>
<td>Integrity</td>
<td>Accountability</td>
</tr>
</tbody>
</table>

Confidentiality: Data must not be accessible or revealed to unauthorized people.

Availability: To use resources as required in expected extension and within desired line.

Accountability: Distinctly trace performed activities to an individual.

Integrity: Protection against undesired changes.

Confidentiality: Data must not be accessible or revealed to unauthorized people.

Availability: To use resources as required in expected extension and within desired line.

Accountability: Distinctly trace performed activities to an individual.

Integrity: Protection against undesired changes.

Confidentiality: Data must not be accessible or revealed to unauthorized people.
A significant element of the information security area is the awareness of the importance of data protection within the organization. Activities are necessary to make the members of an organization aware of the importance of data protection. This process will stimulate the recognition of the existence of risks on the one hand, and it will enhance the acceptance and the effects of measures to be taken on the other. This is a continuous activity in the organization, since new staff will always be joining it. There is also the danger that attention to data security by those who have been in service for a longer period will relax over time (Bemmel and Musen, 1997).

The nursing staff normally instinctively understands that sensitive information must be protected against observation, improper access and the possibility of manipulation. At the same time, there is an uncertainty among the healthcare staff about the limits allowed when information is being handled. This uncertainty has increased since the introduction of IT in healthcare and new legislation (SITHS, 1999a).

With regard to the availability of patient information, the SITHS project mentions two models for accessing information (SITHS, 2000): the authority model and the logging model, cf. Figure 2:6.

Figure 2:6. The balance between the authority model and the logging model (Redrawn and translated from SITHS, 1999a, pp. 13).
The authority model implies that a user's access to information is totally managed in advance by the regulated acquisition. The logging model illustrates how a user has full access to information on his/her own responsibility and all measures can be checked afterwards. The authority model puts stringent demands on the person managing the authorization, while the logging model mostly resembles other models legally applied in our society. Which model would be the best to choose? According to the SITHS project (SITHS, 2000; Carelink 2003b), a combination is recommended. An isolated logging model runs the risk of minimizing the trustworthiness in the handling of information in healthcare, while an isolated authority model would probably be overwhelmed by the extensive administration it requires.

2.4.1 Patient Safety and Patient Privacy

The main purpose of information security in healthcare is to achieve the two important aims, patient safety and patient privacy. These terms are well recognized in the healthcare community. Patient safety can briefly be described as, providing patients with the opportunities for the best care with the right information at the right time and patient privacy as, protecting sensitive patient information being distributed to unauthorized persons (Sågänger and Utbult, 1998). However, since these terms are central to our research, they are further defined and clarified in this section.

Patient Safety

In §2 SOSFS 2005:12, the National Board of Health and Welfare (2007) defines patient safety as protection against medical injury where medical injury is defined as affliction, malaise, physical or mental injury, illness or death caused by healthcare and not an inevitable consequence of the patient's condition. A similar definition comes from the Centre for Patient Safety in San Diego (2007); the patient's freedom from accidental injury when interacting in any way with the healthcare system; and Weinger (2007) continues; avoiding injuries to patients from the care that is intended to help them. The National Patient Safety Foundation further states that patient safety has to do primarily with the avoidance, prevention, and amelioration of adverse outcomes or injuries stemming from the processes of healthcare itself. It should address events that span the continuum from what may be called “errors” and “deviations” to “accidents” (NPSF, 2000). Besides these descriptions, patient safety includes factors such as reducing human and medical errors. It is clear that the term is closely related to patient information. In order to be able to suggest solutions for improving patient safety and increasing the quality of care, it is necessary to secure the management of patient information.

Patient Privacy

Finding a clear definition of the term, patient privacy, is not as easy. Even privacy itself is indefinable due to a lack of boundaries and that it has different meanings for different people. The Business Dictionary (2007) states that privacy in general is the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed. Furthermore, the PatientPrivacyRight organization states that
The right of privacy is: the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated” (PatientPrivacyRight, 2007). The National Encyclopedia (2007) declares privacy as “private life, secrecy and personal integrity”. Personal integrity is also the term commonly used in Sweden instead of patient privacy. However, integrity has a broader meaning when it also includes the person (or patient) him/herself. In the Act on Healthcare Records §4 “the healthcare record must be designed with respect to the patient’s integrity”. According to the SOSFS (1993:20), this is self-evident. However, due to excessive carelessness and ill-founded record notes that have been hurtful and detrimental to the patient, this necessary regulation in the law has been disposed of. Patient information is sensitive and must be protected from unauthorized access in order to respect the patients and to achieve trustworthiness in healthcare.

Therefore, patient safety and patient privacy are closely related to patient information and hence also to information security. In order to achieve patient safety, the right information at the right time is needed, that is, availability and integrity of patient information. In the same way, in order to achieve patient privacy, only the right person should have access to patient information, that is, confidentiality and accountability. In order to clarify the relation of patient safety and patient privacy to information security, we have used the reasoning above and included them in the information security model (c.f. Figure 2:7).

![Figure 2:7. Information Security Model related to the main aims of healthcare: achieving patient safety and patient privacy.](image)

However, it should be noted that these relations are not absolute, since there are cases when confidentiality and accountability are needed in order to achieve patient safety, and availability and integrity are needed to achieve patient privacy. One example is when false information about a patient’s sexual preferences is recorded and revealed to others. The patient’s privacy is affected, but not necessarily his/her safety. Unavailable patient information
can affect patient privacy and safety, since the respect for the patient can be questioned. For instance, a surgeon discovers that the x-ray images he/she needs before a surgery are too old, and the surgery is cancelled the day before its scheduled time. This affects both the patient’s privacy and safety.

Figure 2:7 clarifies the necessity to balance patient safety and patient privacy in the same manner that the information security community must do with the main concepts of information security in order to achieve a sufficient level of information security.

### 2.4.2 Patient Process

The patient process is defined in Winge et al. (2007) to denote the sequence of treatments and other activities performed by health or social care personnel for the patient and in which the patient and his relatives participate. Hence, the patient process follows the patient through an event of illness. In simple diseases, the patient only has contact with one healthcare provider. When diagnoses become more complicated, however, the patient has to visit different healthcare specialists and actors for the one event of the disease. During this process, important patient information must follow the patient in order to secure care of good quality. We therefore need to transfer patient information not only within one healthcare organization, but also to several kinds of healthcare providers. For instance, a patient first visits a healthcare center (primary care) where they establish one diagnosis which requires treatment from a specialist. The patient will then be referred to a hospital (secondary care) for further treatment. When the patient’s treatment at the hospital has been concluded, he/she may still need care in order to deal with the daily task of life. The patient can then receive assistance from the municipality’s home healthcare. It should also be noted that, within the healthcare sector, many private healthcare actors also exist, with which the patient may be in contact. One current problem is that there are no adequate IT-tools supporting this patient process. Each healthcare organization has its own systems, which cannot talk with each other. This is a risk for the patient safety. Furthermore, when IT tools are developed in healthcare, security measures must be implemented in order to protect the sensitive patient information, that is, achieve patient privacy. One example of a patient process and the care providers involved is shown in Figure 2:8.
Figure 2:8 represents an abstract view of a real patient process, and illustrates how many care providers can be involved and their connections in what seems a not so complicated patient process. The patient is the important actor and is located in the middle. The process starts with a patient visiting a doctor for pain in her left foot. An X-ray is carried out which indicates a need for further investigations. The doctor at the healthcare center consults the orthopedist at the local hospital and the patient is given a new X-ray examination with a magnet X-ray-camera. The result indicates a tumor and further specialists must hence be involved. The patient is referred to the regional hospital for more tests at the cytology laboratory with support from the X-ray department. After three weeks, the suspicion of cancer can be disregarded. Instead it appears to be a “ganglion”, which has to be removed. Five months later, surgery is scheduled. The day before the procedure, the surgeon himself calls the patient and declares that the operation must be canceled due to out-dated X-ray images. A new round of examinations is started with emergency referral to Magnet X-ray and a new evaluation at the local hospital. Two and a half months later, the patient receives the surgery and is declared healthy two weeks later, when the stitches are removed. This ends the patient process. Four different healthcare organizations with two to three different units at each are involved in this example. In total, we have eight different care providers who need patient information in order to provide a “good quality of care”. In this example, 42 different contacts between the healthcare sector and the patient were taken. The number of contacts between the healthcare providers is not known. Twenty of the 42 contacts, of which 14 were taken by the patient herself, depended on poor information management. Furthermore, the whole process was extended with, two and a half months due to ineffective information management.

One problem, to our knowledge, is that no one has seriously modeled and analyzed the patient process. Some research projects have pointed out the need for this kind of work, and have done such process modeling (VITA Nova Hemma, 2007; S@ms, 2007 and Mobis@ms, 2007). However, in
healthcare, only business processes are modeled internally in the organization. A comprehensive view of the patient process from the patients’ perspective does not exist. Consequently, there is a risk that the patient may be disregarded, which thus may jeopardize both patient safety and patient privacy.

2.4.3 The Need for Information Security in Distributed Healthcare

Swedish healthcare is undergoing extensive changes. Healthcare is to some extent moving out from the hospitals and instead is being carried out in other forms and locations. Patients with complex care needs receive extensive care treatments, for instance, in their home. They have contact with several different healthcare providers, both within municipalities and county councils. These changes increase the requirements for secure communication and cooperation between several different organizations and authorities.

Proper functions controlling unauthorized access to patient information are still lacking, when IT-systems are extended to more and more users. The Data Inspection Board declares in its report that, in practice, county councils have little or no control of who has access to information about specific patients (Data Inspection Board, 2005). When using an open authorization, for example, the logging model, additional and stronger security measures, such as regular and systematic follow-up routines of logs, are required. The Data Inspection Board (2005) also claims that “thresholds” should exist in the systems in order to force the users to make active choices when accessing sensitive data about a specific patient.

In its report, the National Board of Health and Welfare (2004) identifies cooperation and information transmission between different healthcare providers as a risk area for patient safety. This not only concerns computerized systems. Instead, all media useful for patient information transmission between different healthcare providers are risk factors. The connection between the systems and the use of different media does not yet work satisfactorily. Furthermore, the board claims that the healthcare providers must offer systematic measures in order to achieve sufficient

---

6 Open authorization refers to an extensive use of authorization implying that various healthcare roles and organizations have access to information without any specific restrictions in the authorization control systems.

When IT-systems and different healthcare organizations exchange patient information with each other in the future, new demands on information security will arise. Each organization must have satisfactory security routines. However, this is not enough. Instead, the security boundaries will expand and the availability of sensitive information will increase. This poses new and greater demands on security concerning networks, patients’ privacy, access control systems and so on. Furthermore, the administrative security will have further elements to take into consideration. The working processes and routines of the cooperating healthcare organizations must also be considered.

The demands mentioned above are not unique to Swedish healthcare compared to other countries. Even if traditions and legal aspects differ between countries, the main problems are the same. Strong authentications, derived services as authorization, access controls, accountability, integrity and confidentiality, are importunate demands to achieve (Blobel, 1997; CEN, 1999; Smith and Eloff, 1999; Wenzlaff et al., 1999; and Blobel and Roger-France, 2001).

In distributed healthcare, there is also a particular need for a process-oriented approach (Poulymenopoulos et al., 2003). We have described the patient process in the previous section. In this thesis, the patient process is in focus since it extends beyond the boundaries of one organization, and consequently leads to patient information being available to multiple healthcare providers. Hence, there is a need for greater awareness, improved procedures, improved software, and a more centralized approach or systems management (Louwerse 1998). Furthermore, the European Observatory on Healthcare Systems (2007) states in its report on Healthcare Systems in Transition – Sweden (2007) “Unfortunately, to a large extent, (Swedish) reforms have focused on a piecemeal approach of solving one problem at a time. Also, healthcare reforms have been followed insufficiently and an assessment of their impact on the system as a whole has been lacking.” (EOHS, 2007, p. 92)
3 The Research Design

This chapter presents the research design together with a description of the research process as well as the conducted investigations. Finally, the papers published on the basis of the material resulting from the investigations are presented.

3.1 The Research Strategy

The healthcare area includes many actors with different roles, organizational forms and business processes. Furthermore, the healthcare sector is characterized by intensive information flows, for example, of patient information. The area is thus best investigated as close to the business as possible; to participating in the business, observing its activities, and questioning persons involved about the relationship between its various aspects. According to the conditions of the investigated phenomenon mentioned above, a qualitative approach has been employed with a set of explorative studies. According to Williamson et al., (2002), explorative researchers frequently use qualitative research methods such as case studies and phenomenological studies. These methods are known for their flexibility and suitability for unstructured problems (Wiederselm-Paul & Eriksson, 1991). Hence, case study has been chosen as the main research method implemented with observations and interviews as data collection techniques.

The purpose of the study is to obtain a holistic view of information security in healthcare. A holistic view has its grounding in holism, which means that the wholeness is primary in relation to the parts, and that the parts must be understood from the wholeness rather than the reverse (NE, 2007). Hence, a holistic view includes both a broad and a deep perspective. In order to achieve the broad perspective the patient process is in focus. This means that different healthcare providers and different roles in the organisations are included in the investigations as well as the patient him/herself, that is, stressing a distributed healthcare. The international outlook entails an increased breadth to the research. For the deep perspective, it is important to focus on information security as a generic security concept, which has more of an organizational perspective including both technical and administrative security aspects. Furthermore, in order to gain both breadth and depth, information security is related to the healthcare sector by emphasizing the concepts, patient safety and patient privacy. The field of research is complex, and obtaining a holistic view of information security in healthcare can at first appear overwhelming. However, the motivation for this thesis is based on prior experience, which indicates that the view on information security in healthcare is so fragmented that a holistic perspective seems to be lacking. While on one hand, healthcare is split among different organizations and authorities, on the other, information security (including its main parts, technical security and administrative security) is usually more focused on technical security. The expression, “the whole is greater than the sum of its
parts”, indicates that too much fragmentation increases the risk of losing the wholeness.

One problem is how much information is required to be able to claim that a holistic view has been obtained. Since it is impossible to cover all the perspectives and angles, this will not be claimed. However, the intention is to encompass as much of the area as possible.

3.1.1 Case Studies

As mentioned, case study research is the most common qualitative method used in information systems (Orlikowski and Baroudi, 1991; Alavi and Carlson, 1992). According to Yin (1994, p. 13), a case study is defined as: ”an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when boundaries between phenomenon and context are not clearly evident”. In this thesis, the “phenomenon” is information security in healthcare. Furthermore, case studies are a suitable approach for examining and understanding social phenomena in the natural settings. “Areas where there is little understanding of how and why processes and phenomena occur, where the experiences of individuals and the contexts of actions are critical, or where theory and research are at their early, formative stages can be useful addressed using case study research” (Darke and Shanks, p. 112, 2002). Furthermore, Darke and Shanks (2002) claim that a single case is formed by the complete collection of compiled data for one study of the unit of analysis. Since the investigations are spread over a number of perspectives including specific groups (patients and managers) and various organizations in healthcare, the unit of analysis is clearly defined. Previous discussions in this thesis have shown that information security in healthcare meets the set of conditions mentioned above.

The potential disadvantage of case studies is the risk of subjectivity and influence from the researcher’s background and characteristics. The case study also relies on the researcher’s interpretation of events, documents and interview material (Darke and Shanks, 2002). The large amount of data can also be difficult to manage. In order to avoid these risks as much as possible, it is essential to be aware of them and the consequences they can lead to. It should also be noted that some subjectivity, for instance, the researcher’s experiences, may have a positive effect on the studies. Knowledge of the domain increases the understanding thereof, and may hence give rise to new thoughts and ideas concerning problems and aspects. However, qualitative research in all forms needs to be rigorous, and validity as well as reliability are primary means of ensuring integrity of the research (Williamson et al., 2002). The quality of our research work is discussed in Section 10.4.

3.1.2 Literature Analysis

It is necessary to undertake a comprehensive literature analysis of the research topics and related areas in order to scope and complementing case study projects. Furthermore, the literature analysis helps to understand the
existing research body and helps to position the proposed research within
the context (Williamson et al., 2002). The involved areas in our research
include: healthcare informatics, information security and the information
security model, and healthcare business processes.

It is worth emphasizing that the thesis focuses on Swedish healthcare, which
implies a difficulty in directly relating the results to studies of information
security in healthcare conducted in other countries. Swedish healthcare is
controlled by legal statutes, which differ from those of other countries.
However, directives and standards from the European Union suggest that
European countries are working together to build a common structure
concerning information security in general as well as in the healthcare sector.
This includes the recently developed healthcare version of the ISO/ISE
standard 27002 (previous ISO/IEC 17799) (ISO/IEC 2005a;
ISO/IEC2005b and SIS 2001), to be titled ISO/DSE 27799 (2007) and a
standardization organization in the field of health information and
communication technology (CEN 251, 2005).

Even if laws and regulations are dissimilar, it is still important to obtain
knowledge from other countries, as well as their solutions. The UK, Norway
and Finland have been included in this work, as case studies of specific
investigations and comparisons: see the following section. However, other
countries, both from Europe and other parts of the world, have to be
studied since this knowledge will be necessary in the future when, hopefully
common approaches for transferring information internationally have been
achieved.

3.1.3 Data Analysis

Data analysis was carried out by using content analysis, in order to identify
core consistencies and meanings (Patton, 2002). The transcriptions have
been structured and categorized by using the “code and retrieve” process,
meaning that “labeling passages of the data according to what they are about or other
content of interest in them (coding or indexing) then providing a way of collecting identically
labeled passages (retrieving)” (Richards, 1998, p 214). The data collected from
the interviews have been coded by using color markings and then
categorized according to the contents by naming the evident themes.
According to Darke and Shanks (2002), the way to uncover themes is to
think about what the respondents say and what issues are being raised, in
order to discover if they are part of a broader issue. We ground our use of
themes in the information security model. In addition, the suggested
guidelines and recommendations have been formulated from the code and
retrieve process, as well as from reasoning about the results of the case
studies.
3.2 Compiling and Enhancing the Information Security Model

As mentioned, the information security model was compiled in the initial phase as a result from the literature study. The SIS conceptual classification, cf. Figure 2.1, was combined with the four common characteristics of information security. However, the model was insufficient in that administrative security was not elaborated. In order to further detail this part, contacts where taken in the Network of Excellence – INTEROP (Interoperability Research for Networked Enterprise Application and Software), Task group 7 (TG7), Non Fundamental Aspects. A study was initiated as an activity in TG7 with members interested in administrative security. The study was a literature analysis and continued for one year. It was implemented both individually and in working groups at specific meetings. The basis for the study was the TFI- model even if other models were also analyzed. The study resulted in a publication, Paper 8, which is included in the thesis. A further description of the result of this study is provided in Chapter 8.

3.3 Case Studies Description

Following the aim of this thesis, the choice of case studies must be distributed over different healthcare providers, as well as across their boundaries, in order to cover distributed healthcare; it must also include some countries to achieve an international outlook; and also it has to include the patient, in order to obtain the patient view. The first three case studies cover different healthcare organizations from a local perspective. The fourth case study employs a national approach and is focused on the management level. Case studies numbers 5 and 6 are part of the international outlook. Case study number 5 is conducted in the UK and has the same foundation and implementation structure as case studies 1-3, while case study number 6 is focused on Norway and Finland, and has the same base and structure as case study number 4. Table 3:1 illustrates how the seven case studies are spread over the healthcare organizations and actors. Private healthcare units are not included, even if they are mentioned in one of the case studies (case number 3).

<table>
<thead>
<tr>
<th></th>
<th>Objective 1</th>
<th>Objective 2</th>
<th>Objective 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Local</td>
<td>National</td>
<td>Local</td>
</tr>
<tr>
<td>Different healthcare providers and actors</td>
<td>Case 1-3</td>
<td></td>
<td>Case 5</td>
</tr>
<tr>
<td>National and region managers</td>
<td>Case 4</td>
<td>Case 5</td>
<td>Case 6</td>
</tr>
<tr>
<td>Patients</td>
<td></td>
<td></td>
<td>Case 7</td>
</tr>
</tbody>
</table>
The Research Design

The following subsections briefly describe each case study with respect to how they were conducted and implemented. The result from each case study is presented in Part II of this thesis.

3.3.1 Case No. 1
The first case study (Åhlfeldt, 2002) was conducted in the home healthcare of two municipalities. Previous work in this area has mainly concentrated on county councils. Municipalities have less experience of healthcare, and there is a lack of investigations describing how they manage patient information security. The focus in this case study was patient information management and information from the Data Inspection Board was used as a basis for the interviews.

The work was conducted in the form of interviews with the responsible persons and the home healthcare staff. In order to obtain an idea of how personal data is managed healthcare staff was followed and observed in their work. Six people were observed: district nurses, staff nurses and nurses’ aides. Furthermore, besides those being observed, two unit managers and two medically responsible nurses were also interviewed, making a total of ten persons, five from each municipality.

3.3.2 Case No. 2
The second case study (Åhlfeldt and Ask, 2004) includes observations and interviews with healthcare staff at a hospital in the western region of Sweden. The aim of the study was to determine how users of EHR 7 are affected by the requirements of information security, as well as how the users themselves affect information security, and in what way they follow the recommendations and advice of the Data Inspection Board.

The study was conducted on a limited group of Swedish healthcare workers in the form of observations and interviews. During three days of observations at three different sections, ten employees with different status levels using EHR and sharing the same computer were observed. These staff levels comprised staff nurses, nurses, unit manager, doctors and occupational

7 In paper no 2 the term EMR (Electronic Medical Record) is used. In this thesis however the term EHR (Electronic Healthcare Record) is used since this is a more common and recommended term for electronic healthcare records.
therapists. Furthermore, five employees were interviewed; one system administrator and four nurses.

3.3.3 Case No. 3

The third case study was part of the VITA Nova Hemma research project (Åhlfeldt and Nohlberg, 2005). In this research project, different healthcare providers participated in investigating how a process manager can be used to support a treatment process for leg ulcers. This process connects different healthcare actors: primary care, secondary care and municipalities (Wangler et al., 2003; VITA Nova Hemma, 2007; Perjons et al., 2005a, 2005b; and Johannesson et al, 2005).

Part of the case study included a system analysis of different security aspects of the healthcare systems involved. Interviews were held with the administrators of the respective healthcare systems. A second part included further studies of the healthcare organizations’ systems and networks. The suppliers of the patient record systems and the people responsible for the communication networks in the included healthcare organizations were interviewed.

The basis for the questions in the security analysis was the ISO-standard ISO/IEC 27002 Information Security Management (ISO/IEC, 2005b). Different issues related to system and network security were formulated based on the standard, and further refined into questions useful for interviews with participants from suppliers and healthcare organizations. Three system administrators (one from each healthcare organization), three suppliers (one from each existing EHR) and three network administrators (one from each healthcare organisation) were interviewed.

3.3.4 Case No. 4

The fourth case study was constructed as a small study and comprised 5 interviews (Åhlfeldt and Söderström 2007). Its aims were twofold: to investigate how healthcare business managers8 perceive current information security from a holistic perspective; and to explore their views on information security when patient information is to be exchanged between different healthcare providers. The study was conducted from a national Swedish perspective.

---

8 Healthcare business management refers to governments/ organisations of interests with a national responsibility for healthcare and information security responsible actors within regions and county councils.
Two governmental institutions (The National Board of Health and Welfare and The Data Inspection Board) and one special interest organization (Carelink) were selected. Furthermore, two information security managers were also chosen from two of the largest regions and county councils in Sweden. The National Board of Health and Welfare is the Swedish expert and supervisory authority for social services, public health, infectious diseases prevention and the health services. The Board seeks to ensure that efforts in these areas are of good quality and distributed according to need (National Board of Health and Welfare, 2007a). The Data Inspection Board is a public authority and their task is to protect the individual's privacy in the information society without unnecessary prevention or complication in the use of new technology (Data Inspection Board, 2007). Carelink is a member organization of Swedish county councils, municipalities and private healthcare providers. Through this cooperation, Carelink contributes to the development of IT within Swedish health and welfare (Carelink, 2007). These three authorities/organizations were chosen because the interviewed persons representing them are known for their knowledge and experience of Swedish healthcare. Two persons from The National Board of Health and Welfare were interviewed together. While one is responsible for the technical security issues in healthcare, the other is a legal expert whose focus is on security aspects of the healthcare sector. They are both involved in several national healthcare projects. In addition, two persons from the Data Inspection Board were interviewed in a similar manner. One of them is involved in the Board’s regular inspections of the healthcare sector. The other is a legal expert with a focus on security aspects in healthcare. This person is also involved in national projects, which focus on healthcare, and holds a position as information security manager. No one else in the organization has this kind of information security knowledge. The choice of the two information security managers was based on their broad knowledge in the area of information security within their region and county council respectively. Both hold positions as information security managers and have the best knowledge concerning these issues in their respective organizations. The region was chosen because it is one of the largest in Sweden and previous research has been done therein. The county council was chosen because it is in the front line of IT development support and future commitments to IT in healthcare.

The interviews comprised a number of main questions, the basis for which was the Info Sec model. These questions were constructed to encompass the broad perspective of information security in healthcare, and partly concerned the exchange of patient information between different healthcare providers, and partly the balance between the need of availability of patient information and the protection of patient privacy.
3.3.5 Case Study No. 5
This case study was conducted in collaboration with the EU-sponsored Network of Excellence “INTEROP” (Åhlfeldt and Söderström, 2008b). INTEROP (2007) provided contacts with a university in the southeast of England, the area in which the study was conducted. The study continued for six weeks, and was conducted at the end of 2006. Three types of healthcare actors where interviewed; managers, nurses and system administrators. The actors came from different NHS9 organizations; hospitals, general practitioners and a representative (a security manager) from the National Program for IT (NPfIT), NHS. Nine detailed interviews with four managers, three nurses and two system administrators were conducted.

The interview questions were mainly derived from the Swedish studies, which had a similar approach (case no 1-3). These in turn were based on common advice and guidance from the Swedish Data Inspection Board (1998; 2002). Some questions were also based on the international information security standard ISO/IEC 27002 (ISO/IEC, 2005b), with a focus on system and network security issues therein.

The information security model (InfoSecModel) was used to visualize the results. The InfoSec model has been used in the Swedish study to illuminate problems and needs concerning patient information transfer in a distributed healthcare domain (Åhlfeldt, 2006). Hence, the InfoSecModel facilitates comparisons between the Swedish and English results.

3.3.6 Case Study No. 6
The sixth case study was constructed as two small studies with a total of four interviews, two from Norway and two from Finland (Åhlfeldt and Söderström, 2008a). Their aims were twofold: to investigate how healthcare management perceives current information security; and to explore their view of information security when patient information is exchanged. The study was conducted at a national level in Norway and Finland.

The interview questions were mainly derived from the Swedish study, which had a similar approach (case no 4). This study comprised a number of key questions, which were based on the Info Sec model. The questions concerned the broad perspective of information security in healthcare, and partly concerned the exchange of patient information between different

---

9 NHS refers to the National Health Service in the UK, the largest health organization in Europe (NHS, 2007).
healthcare providers, and partly the balance between the need for availability of patient information and the protection of patient privacy.

In addition, one interest organization and one information security manager from a large hospital were selected in each country. The two organizations were chosen for their superior knowledge and experience of Norwegian and Finnish healthcare respectively:

• KITH (Norwegian Centre for Informatics in Health and Social Care): a company owned by the Ministry of Health and Care Services, Ministry of Labor and Inclusion and the Association for Municipalities. Their mission is: Information Technology for improved Health and Social Care (KITH, 2007).

• STAKES (National Research and Development Centre for Welfare and Health): a Finnish expert agency whose key functions are research, development and statistics for policymakers and other stakeholders (STAKES, 2007).

The two information security managers’ selection was based on their broad knowledge in the area of information security within their respective hospital. Both of these hospitals are in the frontline of implementing IT in healthcare. Although the persons interviewed could not provide a complete picture of the conditions in their countries, these respondents have such experience and knowledge that they were able to provide adequate and clear presentations of the status of their respective nation’s standpoint in the area. Consequently, relevant conclusions could therefore be drawn from the results. The interviews were conducted during a period of one working month.

3.3.7 Case Study No. 7

This small case study comprised five interviews. Its aim was to investigate the patients’ view of patient safety and patient privacy with focus on patient information exchange between several healthcare providers (Åhlfeldt and Söderström, 2008c).

Conducting an investigation from the patient perspective is important, but complicated. Since time was limited, a questionnaire for a large number of patients could not be used. This would have been preferable in order to reach as broad a range of patients as possible. Instead, five patient representatives were chosen. These persons are all previous patients who after their treatment continued their interest in patient issues in different ways. While two of them work in patient organizations, three try to plead the patients’ cause in different interest organizations, projects and investigations.

We do not claim that these persons provided a complete picture of the patients’ view of the observed area. However, their experiences and knowledge meant that they could present an adequate, clear report about the
The status of the patients’ situation. From the results, relevant conclusions could be drawn which can then be used to encourage further studies.

The basis for the questions was the Info Sec model and its relation to the two concepts; patient safety and patient privacy. From this model, questions were constructed about patient safety and patient privacy from a holistic view of healthcare. The interviews were conducted during a period of two working months.

3.4 Data Collection Techniques

In order to conduct the case studies, observations and interviews were chosen for data collection techniques. Each technique, including how they relate to one another, is briefly described in this section.

3.4.1 Observations

Observation is a suitable technique for studying specific phenomena in real life. As an observer, it is important not to interact or disturb the observed person in any way. This is a difficult task since the subject is often aware that he/she is being watched. It is therefore important to establish contact and a rapport with the participants early in the study, to enable them to become familiar with the situation and to work in a more relaxed way. In order to achieve a comprehensive perspective, interviews with the observed persons were also conducted (Berndtsson et al. 2002, Williamson, 2002).

In this thesis, observations were made in the first two case studies. These were conducted by following the participants and watching how they relate to the investigated phenomenon. Notes were taken during the observations and the results were documented afterwards. In addition, these results were included in the material from which the interview questions were elicited.

3.4.2 Interviews

Semi-structured interviews were employed in the case studies. This is common in qualitative studies. Although a number of questions are used, the discussion is open. According to Kvale (1996), Berndtsson et al. (2002), and Darke and Shanks (2002), the interviewer must listen carefully to the discussion and ask follow-up questions, depending on what is emphasized, in order to obtain a deeper understanding of what the interviewed person really means and considers important. The interviews are thus more of a discussion and dialogue than just straight questions and answers.

The interview questions were mainly derived from three different sources: the recommendation and advice of the Data Inspection Board (1999), the ISO-standard ISO/IEC 27002 Information Security Management (ISO/IEC, 2005b) and the Information Security Model, (see Section 3.3.1 – 3.3.7 for more information).
The Research Design

The interviews for this thesis were conducted in all the case studies, but in two different ways. In case studies 1 and 3, notes were taken manually during the interviews, and later detailed and sent to the interviewees for validation. For the remaining case studies, the interviews were electronically recorded and transcribed. There is no particular reason for using these two variations of interview methods. The disadvantage of manual writing is the risk of missing essential data, while the advantage is that the amount of unnecessary data is reduced. The advantage of transcribing recorded interviews is that all the data is included and the risk of missing essential information during the coding process is minimal. The disadvantage of this method is managing the large amount of data, and hence the existence of much unnecessary information of no importance for the results.

3.5 Deriving the Guidelines and Recommendations

In order to derive suggestions for security measures that are needed to achieve a reasonable level of information security, a set of guidelines and recommendations has been developed. The derivation process was based upon the research results as well as the knowledge from the literature study (literature, seminars, projects, working groups, and so on) during the whole research process. The results have been coded, and compiled in tables and then further elaborated by relating the problems and needs in order to suggested solutions. Hence, the suggested guidelines and recommendations have been formulated using analysis and reasoning from the results. Furthermore, the guidelines and recommendations have been classified and visualized in the extended information security model. The extended model was chosen from the need to clarify the security measures required in the specific parts of administrative security and in the same way that the technical security measures are visualized.

3.6 The Research Process

The research process was divided into two phases. Each phase was iterative even though the case studies were conducted sequentially. Parallel to the case studies, a literature survey was carried out during the whole research process. Much knowledge was obtained from participating in relevant seminars, conferences and projects. Furthermore, the authors drew on their own experiences in healthcare, as well as in different types of organizations: municipalities, county councils, the private sector and government service. These experiences and pre-insights have contributed to a deeper understanding of the problems and needs in the organizations of different healthcare providers. Figure 3:1 illustrates the research process activities and presents how observation and interviews were distributed over the cases.
Phase I consists of the initial work and includes seven different activities numbered 1-7, and phase II further eight activities, numbered 8-15. The activities as well as the case studies have been numbered irrespective of one another and have no connection.

Activity 1 illustrates the initiating work from which the background information is collected, thoughts and ideas on the investigation are considered and the course of action is outlined.

Activities 2-4 constitute the implementation stages of case studies 1-3. These were performed sequentially.

Activity 5 includes the literature analysis, as well as an evaluation of the knowledge from seminaries, conferences and projects. Furthermore, this activity was performed iteratively so that the research area was analyzed at different points in time and in relation with the conducted case studies. This activity was carried out in parallel to activities 2-13 during the research process.

Activity 6 includes the processing and analysis of the collected data.

Activity 7 includes the summary and discussion of the results from the initial research. Conclusions were drawn and documented.

Activity 8 illustrates the initiating stage, and includes where the results from the initial research was elaborated and further background information was
collected. Thoughts and ideas on the investigation were considered and the course of action outlined.

Activities 9-13 comprise the implementation stage of case studies 4-7 and the specific literature analysis. These were performed sequentially.

Activity 14 includes the processing and analysis of the collected data for the whole work.

Activity 15 includes the synthesized results together with a set of guidelines and recommendations, which are the result of analyzing and reasoning from the earlier research activities.

3.7 Research Documentation

During the research process the following published papers were written or co-authored. Nine of these papers serve as the foundation for Part III of this thesis. The numbering of the papers relates to the different activities presented in Figure 3:1, and are as follows; papers 1-3 relate to case studies numbered 1-3. Papers 4 -7 relate to case studies numbered 4-7. While paper 8 relates to the elaboration activity in the information security model, paper 9 is not related to any specific activity. Instead it is a contribution to a well-founded suggestion in order to improve information security in distributed healthcare. The papers included in the thesis have undergone minor updates and design modifications in order to conform to the thesis template.

3.7.1 PhD Papers

The following nine papers are included in the thesis:

Paper 1 Information Security in Home Healthcare: A Case Study
Rose-Mharia Åhlfeldt

Paper 2 Information Security in Electronic Medical Records: A case study with the user in focus
Rose-Mharia Åhlfeldt and Lena Ask

Paper 3 System and Network Security in a Heterogeneous Healthcare Domain: A Case Study
Rose-Mharia Åhlfeldt and Marcus Nohlberg
The Research Design

<table>
<thead>
<tr>
<th>Paper 4</th>
<th>Information Security in a Distributed Healthcare Domain: A Case Study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
<tr>
<td></td>
<td>Submitted and early accept to the Health Informatics Journal.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper 6</th>
<th>Information Security Problems and Needs in Healthcare: A Case Study of Norway and Finland vs Sweden</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper 7</th>
<th>Patient Safety and Patient Privacy in Information Security from the Patient's View: A case study</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper 8</th>
<th>Improving the Information Security Model by using TFI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rose-Mharie Åhlfeldt, Paolo Spagnoletti and Guttorm Sindre</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Paper 9</th>
<th>The Need for a Coordinator for Cross-Border Healthcare Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
</tbody>
</table>

3.7.2 Additional Papers

The following published papers support the thesis indirectly but are not included:

**Journals and Book Chapters**


The Research Design


Conference and Workshop Proceedings


The Research Design
Part II

Research results

Part II consists of 7 chapters and presents the results of the research as well as the concluding discussion and suggestion for future work.

- **Chapter 4** - the results from the initial research – the local view.
- **Chapter 5** - the results from the national view.
- **Chapter 6** - the results from the international outlook – England, Norway and Finland
- **Chapter 7** - the results from the patient perspective
- **Chapter 8** - the results from the elaboration of the extended information security model
- **Chapter 9** - the synthesized results from Chapters 4-8 and the suggested guidelines and recommendations derived from the results.
- **Chapter 10** concludes the thesis by discussing the work as well as suggesting directions for future research.
4 Initial Research

This chapter presents the results from the three papers included in the Licentiate thesis (Åhlfeldt, 2006) in Sections 4.1-4.3. The results from the specific case studies are described and discussed in more detail in the respective papers: Åhlfeldt (2002); Åhlfeldt and Ask (2004); and Åhlfeldt and Nohlberg, (2005); which are included in Part III (Papers 1-3). Section 4.4 includes a synthesized summary of the results classified according to the information security model, along with a presentation and analysis of the needs derived from the studies.

4.1 Case No. 1: Information Security in Home Healthcare

The first study highlights the following main problems and needs:

a) Basic strategies are either deficient or non-existent (1a), e.g., IT-strategies, information security policy documents etc.

b) Security education is lacking (1b), e.g., there is no specific educational program for information security in either municipality.

c) There are no routines for the follow-up and evaluation of how information security is managed (1c).

d) Access profile levels are inadequate (1d), e.g., the municipality with the computerized EHR uses the same access profile level in the whole organization.

e) Security measures in facsimile transmissions are lacking (1d), e.g., the transfer of patient information from institutional care to the municipality or the primary care giver is mostly performed by facsimile transmissions without any security measures.

4.2 Case No. 2: Information Security in EHR

The second study reveals the following main problems and needs:

The users are affected by the requirements of information security when

a) The log-on function does not work satisfactorily (2a); e.g., the log-on routine is not compatible with the users’ way of working, the password-exchange routine in the system is inadequate, the log-on and log-out routines are time-consuming, and the users have difficulty remembering the passwords.

b) The users are unaware of or have inadequate knowledge of information security issues (2b); e.g., the different regulations and statutes, various functions in the systems, as well as the risks and threats.

c) The system’s log-on and log-out routines are used in order to support traceability (2c), e.g., users are unaware that IT-systems in healthcare are logged and do not know how the organization manages and checks the log.
d) The availability of EHR is interrupted (2d), e.g., interruptions convey more work for the staff since they are forced to duplicate registrations of patient information.

The user affects the information security in EHR, among other things, when e) Log-on and log-out functions are lacking (2e); e.g., when the user leaves the computer for other tasks without logging out from the system; one another’s identities and authorizations are used.

f) Information is handled and registered incorrectly (2f); e.g., users leave print-outs at the printer; they fail to check a receiver’s authorization to access information; users register information on wrong patients, or send patient information by facsimiles without removing the identity of the information.

g) Deficiencies in and inadequate knowledge (2g) with regard to applying application and registering information in several places in the EHR; routines connected with implementing the sign-technique, and the use of simple passwords often associated with the names of relatives.

4.3 Case No. 3: System and Network Security in a Heterogeneous Healthcare Domain

The third study identified the following main system security problems and needs:

a) The organizations’ security requirements of the system are inadequate (3a), e.g., there are no security requirements from the healthcare organizations for system developers when new systems are developed. The security requirements of EHR are defined by the system developers themselves and based on their own experiences.

b) Security policy documents are deficient or absent (3b).

c) Security mechanisms such as automatic functions for managing user accounts and signing techniques are inadequate (3c), e.g., no functions for reporting unused user accounts during a period of time.

d) General security awareness in the organization is inadequate (3d), e.g., managing passwords and system logs.

The third study highlighted the following main network security problems and needs:

e) Inadequate security projection of authentication and passwords (3e), e.g., no authentication techniques other than passwords will be used in the near future.

f) Inadequate security mechanisms in mobile devices (3f), e.g., there are no sufficient update routines for virus protection etc.
g) Insufficient interest for managing logs (3g), e.g., minimizing the logging activity in order to avoid journalists who request information.

h) There are no routines for training the users in information security (3h).

4.4 Synthesized Results

The results from 4.1-4.3 are classified and illustrated in the information security model in Figure 4:1. The symbols (e.g., 1a, 2b etc) refer to the results from the specific case study, for instance, 1a refers to case study number one and to the highlighted problem and needs noted “a” from Section 4.1. Papers 1-3 presents the results from each case study in more detail.

![Information Security Model](image)

With regard to administrative security, there are obvious common results from the three case studies. Primarily, there are major deficiencies concerning education in information security and the lack of security awareness of the users. This relates to the organizations’ general lack of documentation and implementation of management documentation of IT. Consequently, this particularly concerns information security as a whole. IT-strategies are missing or not useful. Security policy documents do not exist or are incomplete, and are not anchored in the organization.

These deficiencies are not unique for the healthcare sector. The results are in accordance with the “Survey of Information Security 2005” from SEMA (2005). SEMA points out that the lack of security education is obvious. They argue that resources for education must be allocated to train users in security awareness to preserve the trustworthiness of IT in the different government authorities including the healthcare sector.
Concerning technical security, the studies show that the lack of authentication and authorization techniques is a particular security risk. Passwords as an authentication technique are used in all three investigations and the results reveal: 1) the users’ frustration about the slowness of log-on procedures, or 2) difficulty remembering the passwords. The results also indicate insufficient access levels and signing techniques. Another interesting discovery is the lack of management techniques in networks, for instance, managing logs and user accounts. Additionally, there is a need to improve the reliability of network systems in order to minimize the risk of interruption.

In the healthcare area where sensitive information about patients is managed, it is important to implement a sufficient level of security. Such security solutions must be based on different security frameworks; organizational as well as legal (Bemmel and Musen, 1997; Data Inspection Board, 1998, 2005].

The answers to the part of the research question that focuses on what needs the healthcare sector must adhere to concerning information security are summarized below.

In **Administrative security** there is a need for

- IT-strategies and information security policies in the organizations where they do not exist.
- Dissemination of IT-strategies, information security policies and other security related documentation for end-users.
- Education
- Specific training programs including both application and information security knowledge.
- Opportunities for formal and informal meetings and for creating dialogs between users in order to increase their information security awareness.

In **Technical security** there is a need for

- Improvement of authentication, authorization and signing techniques
- Minimizing interruptions in existing network systems.
- Implementation of network management techniques in order to manage user accounts and control the logs.
- Secure mobile equipment in order to enable flexibility and mobility.

The transfer of information between organizations must be achieved by designing solutions that are satisfactory from the perspective of the patients’ and their relatives’, as well as from the legal aspects. If healthcare in the future is to be able to integrate its business processes with those of other healthcare providers, and if the transfer of patient information is to be satisfactorily performed from a security perspective, routines for the minimum level of security have to be designed, documented and implemented jointly by all involved organizations.
5 The Swedish National Perspective

This chapter presents a brief summary of the specific results from the national perspective. The results are described and discussed in more detail in Åhlfeldt and Söderström (2007) included in Part III (Paper 4). The summary is presented from the three main question areas. Section 5.1 presents the problems and needs, Section 5.2 the positive aspects of information security and Section 5.3 the patient safety and patient privacy aspects.

In Chapter 9, we further summarize and classify the results from all the papers in the information security model together with the included guidance and advice derived from the studies.

5.1 Problems and Needs

The question area of problems and needs revealed the following issues:

Technical Security Problems
- Vulnerabilities, such as inadequate functionality in and insufficient availability of communication networks
- No tools for log management
- Deficient techniques for access levels and authentication
- Theft of equipment
- Insufficient back-up routines
- No possibility for system integration at the present times

Administrative Security Problems
- Insufficient availability of patient information
- Absence of information security policies and regulations – of both internal and inter-organisational policies and regulations
- Incomplete work routines
- Insufficient security education
- Deficient compliance and follow-up routines
- No clearly defined responsibility when patients are being transferred between healthcare actors and organizations.
- No clear and identified business-level process

Technical Security Needs
- Improve the technical solutions for authorization and authentication
- Tools for logging management

Administrative Security Needs
- Clear regulations, both legally and from the healthcare sector itself.
- Focus on risk management.
- Continuous development of strategies and policies.
- Awareness
• Communication and dialogs between actors and individuals.
• The healthcare business must take their responsibility
• Survey of healthcare business processes.

**Needs Concerning both Technical and Administrative Security**
Some aspects that concern both technical and administrative security were also mentioned.
• The healthcare sector must raise its competence level concerning how to formulate and put forward requirements for information security
• All healthcare organizations and their actors must know what they want and be able to formulate it.

These common aspects require both organizational routines and education of staff, as well as technical insight.

**5.2 Positive Aspects**
Information security in healthcare is not only associated with problems. The healthcare sector also experiences several positive aspects with regard to securing its information. Therefore, positive aspects of information security were also investigated, as a complement to the problem perspective. The following positive aspects were highlighted in our study.

Care flows (the whole of the patient process) will become more efficient, and the quality of care and patient safety will improve. Patients also have a better chance of recovering earlier than expected, which implies an improved quality of care. These improvements in efficiency are very important from a national perspective, both in terms of quality, and cost savings. Furthermore, when patient information availability increases, it is also possible to increase the availability of expert assistance to help care for the patient. These aspects relate to both technical and administrative security. However some specific technical and administrative security aspects were also defined.

**Positive Technical Security Aspects**
• Having patient information computer-based rather than paper based patient records
• The possibility of using new technological developments to obtain help from experts in other countries

**Positive Administrative Security Aspects**
• Improving the number of risk analyses
• Increasing the common view on security requirements
• Achieving confidentiality and accountability even if there is still a lot of work to do in this area.
5.3 Patient Safety and/or Patient Privacy

Although patient safety and patient privacy often contradict one another, the results showed a desire to balance them. The questions were structured into three areas concerning the focus of the relationship between these concepts: the current focus, the desired focus, and the probable future focus (noted a, b and c in the figure). Figure 5:1 presents a compilation of the results from the questions concerning the balance between these two concepts. The notation in the figure represents the respondent as well as the specific focus. For instance, ‘A’ refers to respondent A while ‘a’ refers to the current focus.

Current Focus

- Two respondents claim that the current focus is patient privacy, since legislation focuses on protecting this very issue. Sometimes, patient privacy legislation is so strict it almost hinders patient safety.
- Two respondents claimed there should not be a polarization between the two aims, but that privacy is a part of safety.
- One respondent considers that patient safety dominates the practise of healthcare, while patient privacy dominates legislation.

Desired Focus

- Three of the interviewed persons stated the necessity of achieving a balance between the two. It should be possible to achieve a high level of patient safety as well as a good level of patient privacy.
- One respondent expressed a desire to unite the two aims into one, and not to polarize them.
- One respondent wanted the focus to be on patient safety, even though patient privacy should be protected as well.

Probable Future Focus

- Two respondents claim that there will be a balance between privacy and safety.
- Three respondents stated that the focus will change depending on the healthcare sector requirements on improved availability of information. These requirements will change the focus to patient safety with the risk of reducing the role of patient privacy.

Figure 5:1. The balance between patient safety and patient privacy (National view).
The small square in the patient safety box represent the respondents desire to unite the two aims into one, and not to polarize them.

5.4 Conclusions
The results show deficiencies primarily in administrative security. For example, clear regulations are missing, both legal and organizational. These deficiencies seem to be more obvious when considering at the need for cross border patient information exchange between several healthcare organizations. However, the positive effects of such an opportunity are significant enough to advise the healthcare sector to proceed in that direction, not least with respect to available resources and to increase the quality of care. However, technical problems and needs should not be neglected. It is remarkable that in spite of the forceful and rapid developments in this area, technical deficiencies still remain. Sufficient secure authorization and authentication techniques exist in the market place, if the willingness to implement them is strong enough. Furthermore, techniques also exist for managing communication networks, for example, with regard to checking logs.

Our study shows apprehensions from some of the respondents that patient privacy will be neglected in the need to make patient information available to more healthcare providers. The openness of availability depends on the difficulty of creating and implementing adequate technical solutions for the sufficient level of access techniques. Another interesting point was that a technically increased availability may imply a decrease in the willingness to make necessary notes in the documentation.

The next chapter presents the results from the international outlook. These results are compared with those presented in this chapter and in Chapter 4.
6 International Outlook

This chapter presents a brief summary of the specific results from the international outlook. The results are described and discussed in more detail in Åhlfeldt and Söderström (2008a) and Åhlfeldt and Söderström (2008b) included in Part III (Papers 5 and 6). The chapter comprises two main sections. While Section 6.1 presents the results from the English study, Section 6.2 includes the results from the study in Norway and Finland.

As mentioned in Chapter 5, we further summarize and classify the results from all the papers in the information security model together with the included guidance derived from the studies in Chapter 9.

6.1 England

This section presents the results from the English study and compares it with a similar Swedish investigation included in Chapter 4. Section 6.1.1 provides the analysis of current problem and needs, Section 6.1.2 briefly describes the National Program of IT, Section 6.1.3 presents the results concerning patient safety and patient privacy aspects and Section 6.1.4 provides a comparison with the Swedish situation.

6.1.1 Problems and Needs

The following problems and needs were highlighted:

Technical Security

- Weak authentication techniques in the local systems
- Wide access levels
- Insufficient distribution techniques for patient information exchange
- No encryption of sensitive information
- Weak signing techniques
- Unequal level of physical security between the healthcare organizations
- Remote access of communication networks
- No regular audits
- No IDS
- No tools for logging management
- Lack of security measures for mobile equipment

Administrative Security

- Insufficient management of patient identity
- No prescribed information security policies apart from the national standards and those of the Data Protection Act
- Poor follow-up routines of security work
- Lack of education concerning general information security issues
High level of security awareness concerning confidentiality and physical security but less in other parts of information security.

No approach for logging management in the national system – trust of the need to know model

6.1.2 National Program for IT (NPfIT)

The expectations of NPfIT are, in general, very high, not the least concerning information security. However, the question is if the program can solve all the existing problems, for instance, those mentioned in Section 6.1.1. The aim and the vision of the program are impressive, and based on the international standard of information security, ISO/IEC 27002 (2005b). This standard originates from England, and it is therefore natural to base this kind of gigantic project on the standard, according to a representative from the NHS. They also have the ambition to implement strong authentication techniques such as smart cards and a strong authority “need to know” model as a primary task. Both the NHS and the interviewees really want level access that only includes those and only those who are involved with the patients’ care.

However, with regard to how information security will be improved in the new national system, the answers from the respondents differ. One manager believes that one improvement will be support of different access levels for the staff. The information will not float around in the office. Another manager says that she will not have her own patient information in the new system for two reasons: 1) the number of people she believes may be able to view that record; and 2) the lack of a clear definition of what is available to whom. The nurses believe that security will be improved compared with the current situation, not the least with regard to the levels of access. But for some special units at the hospital, the nurses claim it will not make any difference. The hospital system administrator considers the smart card process and the role-based access will improve the security, in general, but that it is administratively overwhelming. The GP system administrator really does not know how security could be further improved with the new system.

The main risks of the new national program are considered to be the structure of a great number of people, access levels together with the risk of hacker attacks, a central database and risks related to new functions that are not adaptable to the healthcare domain, and so on. According to the system administrators, the delay of the program is the greatest risk, but at the same time, that implementation must not proceed too quickly and be too ambitious.

6.1.3 Patient Safety and/or Patient Privacy

This group of questions concerned three aspects: the current focus, the desired focus and the probable future focus (noted a, b, and c). Figure 6:1 presents a compilation of the results from the questions concerning the
balance between these two concepts. The notation follows the same structure as in Figure 5.1 (‘A’ refers to respondent A while ‘a’ refers to the current focus).

![Figure 6:1. The balance between patient safety and patient privacy (England).](image)

**Current Focus**

One nurse favored patient safety, while another favored patient privacy, and a third that both of them should be emphasized. One manager believed that patient privacy is important to the patients, while patient safety is more important to the organization. Although one manager favored patient safety, yet another said both. The system administrators stated they do not differentiate between the concepts in their daily work. Sometimes privacy is more emphasized, since patient safety is taken for granted. But this is not a subject they discuss. The GP administrator stated that the concepts cannot be separated.

**Desired Focus**

All the interviewees claim that the two concepts can be balanced, but not at 100 percent. However, it is something to strive for. If a choice must be made, two of the interviewees said that patient safety should be prioritized because it is the most important aspect for healthcare.

**Probable Future Focus**

All the interviewees believed that when NPfIT has been implemented, the emphasis will be more on privacy from a patient perspective. The motivation was that they all believed patient privacy was neglected in the National Program. Hence, from both the organizational and the NHS perspective, patient privacy will be more prioritized than it is now.

### 6.1.4 Comparison with Sweden

The two studies from Sweden and England respectively identify the following similarities and differences between the countries:
• Managing patient identity: the UK uses NHS numbers, while Sweden uses personal numbers. In both countries, patients’ identities have been mixed up.

• Strategies concerning the Data Protection Act: The UK is more focused on these strategies than Sweden.

• Technical security: the UK has implemented NHS-net for all NHS Trusts. In Sweden, Sjunet has only voluntary membership except for county councils. Both countries have weak authentication techniques, wide access levels, system integration problems, and weak signing techniques. The two communication networks (NHS-net and Sjunet) are similar but cannot be used for all types of patient information.

• Administrative security: The UK is more focused on education concerning confidentiality, and the confidentiality awareness is therefore higher than in Sweden. Both countries lack a general security policy, are deficient in following up security work, and lack in information security awareness.

• Patient record systems: the UK solves the system integration problems with a top-down approach – NPfIT, meaning the use of one patient record system in the whole of England. Sweden uses a bottom-up approach, in which 21 county councils and regions have different patient record systems. They try to solve the problem with an integration platform for general patient information.

• Patient safety and patient privacy: the UK emphasizes patient privacy, while Sweden emphasizes patient safety.

6.1.5 Conclusions
The problems and needs in technical security are similar in England and Sweden: weak authentication techniques, wide access levels, integration problems between different systems, no encryption of sensitive information, weak signing techniques, and so on. There is a special situation in England at the moment, because they are currently implementing the new national system NPfIT, while still using the old patient record systems. For natural reasons, technical weaknesses are not addressed while they are awaiting the new system. However, it should be emphasized that implementing a new system does not automatically solve all the problems. The study shows that the old local systems have functions that the new one does not, but the new system is still needed. The question must be asked if the users still have to use the poor security solutions in the local systems or if the old functions can be integrated with the new system. The NHS-net has already been implemented, which implies that security levels of communication security have increased considerably. It should be noted, however, that not all information is sent via the NHS-net. Information is still managed manually to other units. Remote work is not included either which must be seen as a major shortcoming, since in a long-term sense it could impact patient safety if the healthcare staff cannot access patient information from other places than from a specific healthcare unit.
The level of physical security varies. At the new hospital and at GPs, the level of physical security is sufficient. On the other hand, the physical security level at the home visitor unit is weak. The staff seems to be aware of the problem, and this is primarily a management issue. Compared to Sweden, the physical security levels in England are higher. Sweden also lacks continuous fire training programmes at the GPs.

With regard to administrative security, there are both similarities and differences between the countries. Both countries have the problem of a lack of general information security policies and poor follow-up of security work. However, while England is more advanced in education of security issues based on the Data Protection Act and confidentiality, it has on the other hand deficiencies regarding general education on information security. The users’ security awareness is higher in England, with regard to confidentiality and physical security, but significantly less in relation to other parts of information security.

Concerning patient safety and patient privacy, eight out of nine interviewees agreed that a balance between patient safety and patient privacy is preferred. Nevertheless, five out of nine interviewees claim that in the future, the emphasis will be on privacy since the new program does not seriously take privacy aspects into consideration. There is an obvious fear that privacy will be more neglected in England compared to Sweden. England has chosen a “need to know” approach in their program NPfIT and clearly state that only those involved in the treatment of a patient will have access to the patient information. This will be achieved with strong authentication techniques such as smart cards. Sweden does not generally have that strong an authentication approach, even if similar recommendations exist from the government’s point of view. Nevertheless, England is more conscious about the risks and wants to protect privacy more than Sweden does, although Sweden has a more liberal view of how to protect privacy and how to address authentication techniques.

6.2 Norway and Finland

This section presents the results from the Norwegian and Finish studies respectively, and compares them with a similar Swedish investigation (presented in Chapter 5). The summary is derived from the three main question areas. Section 6.2.1 presents the problems and needs, Section 6.2.2 the positive aspects of information security, and Section 6.2.3 the patient safety and patient privacy aspects. Section 6.2.4 summarizes the comparison between Norway and Finland as well as Sweden.

6.2.1 Problems and Needs

The following technical and administrative security problems as well as needs were highlighted:
Technical Security Problems

- Insufficient authentication and access levels – Norway and Finland
- Integration and interoperability problems – Norway and Finland
- The risk with open hospitals – Norway and Finland
- No logging management tools – Norway
- Deficiencies concerning audit logs - Finland
- No regulation for encryption inside healthcare organizations - Finland
- Lack of knowledge concerning application security level - Finland
- The narrow area of outsourcing – Finland
- Difficult to serve systems in many organizations – Finland

Administrative Security Problems

- Unavailable patient information – Norway
- Lack of resources for information security activities – Norway
- Lack of security routines – Norway
- Employees are the weakest link - Finland
- Lacking security knowledge and behavior - Finland
- System monitoring is too expensive – Finland
- The semantic level of interoperability
- Information overflow – Finland
- How to control access levels – Finland

Technical Needs

- Improve the technical solutions for authorization and authentication – Norway/Finland
- Tools for logging management – Norway
- Support and presenting tools – Norway
- Continuing implementation of EHR – Finland
- 24-hours system monitoring - Finland

Administrative Security Needs

- Focus on risk management – Norway
- Clarify responsibility issues – Norway
- Reorganization of the whole healthcare sector – Finland
- Quality checking tools – Finland
- Standards and service agreements – Finland
- Patients must have control of their own information - Finland.

6.2.2 Positive Aspects

Information security in healthcare is not only associated with problems. The healthcare sector also benefits from several positive aspects of securing its information. Therefore, positive aspects of information security were also investigated, as a complement to the problem perspective. The following positive aspects were highlighted in our study.

- Computerization of patient records – Norway and Finland
• “Power of citizens”
  • Patients are allowed to read their own patient records – Norway and Finland
  • and check their logs – Finland.

6.2.3 Patient Safety and/or Patient Privacy

This group of questions concerns three aspects: the current focus, the desired focus and the probable future focus (noted a, b, and c). Figure 6:2 presents a compilation of the results from the questions concerning the balance between these two concepts. The notation follows the same structure as previous figures (‘A’ refers to respondent A, while ‘a’ refers to the current focus).

Current Focus

Three respondents (one from Norway and both from Finland) claim that the current focus is patient privacy, since legislation is focused on protecting this issue. One Norwegian respondent considers that patient safety dominates healthcare, while patient privacy dominates legislation.

Desired Focus

All respondents state the necessity of achieving a balance between the two concepts, even if two respondents want it to lean more towards safety. It should be possible to achieve a high level of patient safety and a good level of patient privacy.

Probable Future Focus

One respondent from each country claims there needs to be a balance between privacy and safety. The other respondents state that the focus would move towards patient safety in the future. One of the Norwegian respondents adds that even if privacy seems less in focus, in the nearest future the pendulum would probably begin to swing for change in the long-term.

![Figure 6.2. The balance between patient safety and patient privacy (Norway/Finland).](image)
6.2.4 Comparison with the Swedish Study

Similarities between the countries (see Table 6:1) concern problems and needs, positive aspects as well as patient safety versus patient privacy.

**Table 6:1. Similarities between the three countries.**

<table>
<thead>
<tr>
<th>Category</th>
<th>Commonality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems and needs</td>
<td>Lack of authorization techniques (technical security)</td>
</tr>
<tr>
<td></td>
<td>Lack of log management techniques (technical security)</td>
</tr>
<tr>
<td></td>
<td>Too wide availability of patient information (adm. security)</td>
</tr>
<tr>
<td></td>
<td>Incomplete work routines (adm. security)</td>
</tr>
<tr>
<td></td>
<td>Lack of security awareness (adm. security)</td>
</tr>
<tr>
<td></td>
<td>Need for risk analyses (adm. security)</td>
</tr>
<tr>
<td>Positive aspects</td>
<td>Computerization of healthcare records</td>
</tr>
<tr>
<td>Patient safety and patient privacy</td>
<td>No consensus on the current focus in either country</td>
</tr>
<tr>
<td></td>
<td>Legislation is focused on privacy while organizations focus on safety</td>
</tr>
<tr>
<td></td>
<td>Tendency to focus more on safety in the future</td>
</tr>
</tbody>
</table>

The computerization of healthcare records is a main issue in all three countries, resulting in availability of information, improved care flow, and improved quality of care. There are also differences, which are illustrated in Table 6:2.

**Table 6:2 Differences between the three countries.**

<table>
<thead>
<tr>
<th>Differences</th>
<th>Sweden</th>
<th>Norway</th>
<th>Finland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication technique problems</td>
<td>Ongoing pilot project on smart cards</td>
<td>Further advanced with smart cards work, e.g. communications networks.</td>
<td>Further advanced with smart cards work</td>
</tr>
<tr>
<td>Exchange of patient information</td>
<td>Few standards and policies</td>
<td>More standards and policies</td>
<td>More standards and policies</td>
</tr>
<tr>
<td>Patients’ own access to information</td>
<td>Patients lack the right to access logs, means less power to patients</td>
<td>Patients have the right to access logs, means more power to patients</td>
<td>Patients have the right to access logs, means more power to patients</td>
</tr>
<tr>
<td>Patient privacy and Patient safety</td>
<td>No consensus among respondents</td>
<td>Balance is needed</td>
<td>Balance is needed</td>
</tr>
</tbody>
</table>

The top three rows of the table indicate problems and needs, the third row also includes positive aspects, and the fourth concerns the discussion of privacy versus safety. Even though the countries share the problems of authentication techniques, they differ in how advanced they are in addressing them. Information exchange is also in part a common dilemma, but the countries differ here as well in how advanced they are in dealing with the issue. Interestingly, Norway and Finland both allow patients to access logs. The general similarities should allow Sweden to do the same, but this will require legislative changes.
6.2.5 Conclusions

The results show that Norway and Finland as well as Sweden basically have the same problems and needs concerning information security in healthcare. In technical security, they share the problems of authentication techniques, even if Norway is further advanced with their smart cards. All three also lack authorization techniques and tools for log management. In administrative security, the main problems are: too wide availability of patient information, incomplete work routines, lack of security awareness, and lack of risk analyses.

The integration dilemma is also a common problem. Acts must be adjusted according to new requirements, and responsibilities for patient information must be revised. Thus far, Norway and Finland have implemented more standards and policies compared to Sweden, while the Swedish study did identify the need for strategies, policies and standards. In Norway and Finland, patients have the right to access their logs and consequently have more control of their own information. This is currently not possible in Sweden.

Furthermore, the research shows similarities concerning the balance between patient safety and patient privacy, even if the respondents disagree on where the present focus is. They agree that legislation is focused on privacy, while organizations focus on safety. The Norwegian and Finish respondents all state the necessity of achieving a balance between the two concepts. The Swedish respondents are divided: three want a balance while two claim the focus should be on patient safety. The division may depend on the frustration of not having patient information available when needed and hence disregarded patient safety. Another hypothesis is that Swedish citizens trust that the government will protect them and are less obviously concerned that their privacy will be neglected, even if there is apprehension in that area too. In the future, all the countries claim the focus will shift to patient safety, while one also mentioned the importance of privacy.

The next chapter presents the results from the study with the patient in focus. The patient safety and patient privacy aspects are emphasized from the patient’s perspective.
7 The Patient’s View

This chapter presents a brief summary of the results from the patient’s view. The results are described and discussed in more detail in Åhlfeldt and Söderström (2008c) included in Part III (Paper 7). The summary is presented using the structure of the five main question areas in Sections 7.1-7.5.

As mentioned in Chapter 5, we further summarize and classify the results from all the papers in the information security model together with included guidance derived from the studies in Chapter 9.

7.1 The Patients’ Understanding of Patient Safety and Patient Privacy

The interviewees gave the two concepts patient safety and patient privacy the following meanings:

Patient Safety
- as a whole concerns the availability of information
- having a functioning information flow
- patients must own or at least have access to their information and record before one can claim or guarantee patient safety.

Patient Privacy
- no unauthorized persons should have access to patient information
- concerns standing up for one’s principles
- the possibility and the right to choose
- the lack of information implies a lack of knowledge about the patient’s previous medical history, which violates the privacy.

7.2 The Present Risks with These Two Concepts

With regard to patient safety and patient privacy, the following risks are highlighted:

Patient Safety
- The lack of access to patient information.
- The lack of person responsible for the flow of information.
- Lack of resources.
- High rate of work.
- None or inadequate tools for measuring care quality.
- Healthcare does not consider the patients’ whole situation.
- Patients do not have access to their own information and cannot participate in their own care.
- The absence of computerized records.
- Too many limitations in the computerized systems, which increase the risk that the doctor does not acquire the needed information.
Patient Privacy
• Unauthorized people may read patient information not intended for their eyes. This is a major risk with the paper-based systems since they cannot be controlled.
• Significant risk for insight in the computerized records, since most of the systems are wide open. This is not a great problem, however, and it is more important that the information is available when needed.

7.3 The Sensitivity of Patient Information
The following opinions concerning the sensitivity of patient information are illuminated:

• Patient information should not be further sub-divided.
• Healthcare staff involved in the patient’s care must have access to information regardless of organizational appurtenance.
• It is important that the external boundaries between the healthcare organizations and the society are strong.
• It should be possible to further level adjust patient information into one type of general information that is available to all people in healthcare, such as allergies, drugs etc., which should be clearly visible in the record.
• Some kinds of patient information are more sensitive than other kinds, such as psychological illness, alcohol addiction, or sexual orientation.
• Prejudices are preserved if levels of patient information are graduated or set more strictly.

7.4 Security Measures to Achieve Patient Safety and Patient Privacy
With regard to technical as well as administrative security, the following measures are proposed:

Technical Security Measures
• The patient record systems of the different care providers must be integrated in order to deal with the lack of patient information.
• Logging lists, which the patient can access.
• Possibility of making the authorization available to other healthcare organizations, but still maintaining a strong and clear boundary against public access.
• Focus on the design phase when new systems are developed.
• Improved authorization techniques in order to restrict the access levels of external stakeholders and those who should absolutely not have access to information.
Administrative Security Measures

- Synchronization of the legislation - more suitable for the new information society.
- Improve education in all healthcare organizations and for all actors.
- Infrastructure rethinking - three levels; technology, information and function with structures and processes included in all three levels.
- Improve the internal structures with clear and consistent rules.
- Provide patients with responsibility for their own process.
- Higher demands for the provision of tools for measuring care quality.
- Politicians must take their responsibility more seriously and “put their foot down and show what they really want”.
- Clearer professional roles.
- Higher competence at the management level.
- Smaller units responsible with for their resources, and the privatization of hospitals.

7.5 The Balance between the Need of Patient Safety and the Need to Protect the Patient Privacy

This group of questions is three-fold: current focus, desired focus, and probable future focus (noted a, b, and c in the figure). Figure 7:1 presents a compilation of the results from the questions concerning the balance between these two concepts. The notation follows the same structure as in the previous figures ('A' refers to respondent A while ‘a’ refers to the current focus).

Current Focus

Two respondents claimed patient safety is more emphasized today, and two others claimed it is patient privacy. The fifth respondent said that it is not patient safety, but had no clear standpoint on patient privacy.

Desired Focus

Four of five respondents answered that the optimal situation is a balance, while one said patient safety.

Probable Future Focus

Two respondents answered that it will be a balance between safety and privacy in the future as well. One added that even if there was a balance, some emphasis would be on safety. Two out of five answered that only patient safety will be in focus in the future. One of these thought that the rest of society will cherish their privacy, while healthcare would be more focused on patient safety. One out of five claimed patient privacy, because it would take too long to get patient influence in healthcare, and this is a requirement in order to achieve patient safety.
7.6 Conclusions

The results show that the main problems in order to achieve both patient safety and patient privacy from an information security perspective are 1) not having patient information available when needed, which entails a risk of affecting patient safety and 2) having paper-based patient information as well, which entails an obvious risk for the uncontrolled dissemination of patient information – risk for misuse of confidentiality, which can consequently affect patient privacy. Furthermore, the results show that patients do not believe that the healthcare sector lives up to its duties. If it really sets out to achieve patient safety and patient privacy, it must also achieve availability, integrity, confidentiality and accountability of patient information.

The study also shows that the patients focus more on patient safety than on patient privacy. Privacy is an important issue, but should not take place at the expense of patient safety, which the respondents claim is the current situation. Privacy seems to be more important to citizens in countries characterized by having to protect themselves from external threats, or having a regime which does not support democracy. Swedish patients worry more about privacy protection from an individual perspective. An example is protecting their sensitive information from their neighbors or acquaintances, and so on.

Furthermore, it should be noted that the patient representatives really emphasized the patients’ role in their own processes, such as patients owning their information, being more involved in the whole patient process, choosing doctors, and obtaining available information about the course of their illness. However, in the foreseeable future, patients will not be able to own their information even if the opinions are in line with the “National Strategy for eHealth (Ministry of Health and Social Affairs, 2006). According to our research, it is obvious that this perspective is currently far from reality.
8 The Extended Information Security Model

This chapter presents a brief summary of the results from the work extending the information security model. The results are described and discussed in more detail in Åhlfeldt et al. (2007) included in Part III (Paper 8).

As mentioned in Chapter 5, we will further summarize and classify the results from all papers in the information security model together with the included guidance derived from the studies in Chapter 9.

8.1 Elaborating the InfoSec Model

One way to extend the InfoSec model in its administrative part was to use the elements of the TFI-model\(^\text{10}\); formal and informal. This model is a semiotic model and was chosen because of its focus on context-related aspects, such as organizational culture and human behavior, instead of technology. Adopting this view made it possible to better understand all the context specific aspects that otherwise can be difficult to analyze.

Administrative security concerns information security management, which can be both formal and informal. The formal element includes policies, rules controls, standards, and so on, which aim to define an interface between the technological subsystems, while the informal element includes the aspects related to the human behavior. This seems to be in conjunction with the security area too. Björck and Yngström, (2001) have also mentioned this division of information security when they classify some written papers from the security area. The authors divide them into technical, formal and informal parts. They also conclude that information security papers mainly concern technical aspects, while there is a further need for research at the formal level. Above all, they conclude that the informal level has been neglected. One important element at this stage is to make the users security aware. Concerning the formal part, it seems natural to subdivide it into external and internal levels. Each organization is subject to external regulations concerning security issues, for instance, laws, regulations and agreements with other companies. Furthermore, there is an internal formalism for information security management, such as IT-strategies, security policies, educational programs, and so on. According to Lee (1999) this is the level where much of the effort of information security

\(^\text{10}\) The TFI-model adapting the view of an information system as constituted of the technical (T), formal (F) and informal (I) elements.
management is concentrated. Hence, we extended the InfoSec model as depicted in Figure 8:1.

Figure 8:1. Suggestion for an extended InfoSec Model.

8.2 Evaluating the Extended Model

One approach to evaluating the extended InfoSec model was to apply the results from the administrative security part to the results of our earlier research, c.f. Chapter 4, into the model. The result at the administrative security level was classified according to the new levels of administrative security: formal and informal. In addition, the formal issues were further classified as external and internal. The result of this classification is shown in the right part of Figure 8:2 and should be compared with the results from the left side.

Figure 8:2. The left side shows index of problems and needs in healthcare and the right side shows the corresponding indexed results in the extended InfoSec model.

The result shows that the investigations exhibit both formal and informal problems and needs. However, in the formal part, there are no reported problems at the formal external level. This does not imply that there are no problems in this area, however. Other investigations reported in the National Strategy for eHealth (Ministry of Health and Social Affairs, 2006) reveal...
problems at this level concerning, for instance, legislation contradiction. It is reasonable to assume that the problem was not mentioned in our case studies, since other more internal problems impact the respondents’ daily work more directly. Another formal external problem could be e-contracting. In the healthcare area, no such contracting is currently applicable, and therefore no such problems have been identified.

In the informal part, we not only find problems, such as inadequate security awareness and attitudes, but also no measures for compliance and follow up activities. Technical solutions are quite easy to implement. Formal administrative solutions can be considered rigid tasks to perform but are in fact attainable. The main challenge for information security in the future is to implement useful methods to achieve security awareness in organizations.

8.3 Conclusions

Our main contributions include showing how the extended InfoSec model can be of significant use in emphasizing a more holistic view of the information security area, and the administrative security level in particular. The model also visualises, more specifically, within what areas information security measures need to be taken into account.

The results from the study indicated no external problems and needs in the formal part of information security. We do not claim that all external regulations and legislation issues have been taken into account or that there are no problems concerning the external part. However, our investigation did not focus on these issues. In the internal formal part, there is a need for information strategies and information security policies strongly related to context or the type of domains, such as the healthcare, military and business sectors. The internal rules, instructions and education should emerge after defining the policies. In the informal part there is also a need for measures to support the organization in implementing information security awareness. This is not a simple task, but very important in order to reach sufficient information security within the whole organization.

A weakness is that only one single investigation has been used to evaluate the extended InfoSec model. Future work must be conducted to evaluate the model in other studies as well, both theoretically and practically, in order to confirm its usefulness.

The need for formalization in the design phase of information systems development is moving towards the use of semantic technologies and ontologies. Future research should therefore evaluate the extended model in other domains.
The next chapter presents the synthesized results reported in Chapters 4 – 8. The results are further visualized in the extended information security model presented in this chapter.
9 Synthesized Results and Suggested Guidelines and Recommendations

Based on the results reported in Chapters 4 - 8, this chapter synthesizes and visualizes the results in order to provide further answers to the research questions and to fulfill the aim and objectives of the thesis (see also Sections 1.2 and 1.3). The chapter comprises three sections, each relating to one research question: how information security can be better understood (Section 9.1); problems and needs concerning patient information in distributed healthcare (Section 9.2); and suggested security measures needed in order to achieve a reasonable level of information security in healthcare (Section 9.3).

9.1 Improve the Understanding of Information Security

The first research question concerns how information security in healthcare can be better understood, particularly in relation to patient safety and patient privacy. It mainly corresponds to the fourth objective:

Objective no 4: To obtain an increased understanding of administrative security by elaborating this branch of information security. This will contribute to clarifying what measures are needed to ensure a sufficient level of administrative security.

Based on the results, three specific contributions can be highlighted that answer this first question:
1. The creation of the information security model
2. The connection of patient safety and patient privacy to the characterizations of information security, in order to relate information security to the healthcare sector and its main aims.
3. The elaboration of the model in order to extend the administrative part and provide a deeper understanding of its contents.

The remainder of this section discusses these three contributions in more detail.

9.1.1 Creation of the Information Security Model

An information security model was created in the initial phase, c.f. Figure 2:2. This model has been useful in the research process when describing and presenting the information security area to the involved individuals, as well as being a basis for the formulation of questions in the investigations. Moreover, the model has been a useful tool for visualizing problems and needs derived from the case studies.
9.1.2 Connection of Patient Safety and Patient Privacy to the Characterizations of Information Security

Patient safety and patient privacy, the two important aims to achieve when dealing with healthcare information, have been highlighted throughout the thesis. The focus has particularly been on the balance between the concepts and information security. Therefore, we related these concepts to the information security characteristics in order to visualize and clarify the close connection, c.f. Figure 2:7. Furthermore, the question concerning the balance between these concepts was asked in four out of seven case studies. The illustrated connection was also very useful here in order to increase the interviewees’ understanding.

9.1.3 Elaboration of the Information Security Model

The elaboration of the information security model into the extended version was the main research activity conducted in order to fulfil objective 4 and the first research question. The result has been briefly presented in Chapter 8 and published in Paper 8, included in the thesis. The extended model clarifies within which areas information security measures concerning administrative security need to be taken into account. Hence, we use the extended model in Section 9.2 when the synthesized results of problems and needs are described and visualized.

9.2 Identified Information Security Problems and Needs in Distributed Healthcare

The second research question concerns what the particular information security problems and needs concerning patient information are in situations where several healthcare providers and organizations are involved. It corresponds to objectives 1-3:

Objective no 1: To identify problems and needs of information security regarding patient information in distributed healthcare from a national Swedish perspective. In order to relate these problems and needs, an information security model will be compiled.

Objective no 2: To obtain an understanding of how problems and needs identified in Sweden compare to the situation in other countries with similar welfare and living conditions. This will be conducted in an international outlook.

Objective no 3: To bring to light what patients themselves think when it comes to safety and privacy. In what situations they do and do not object to having their information revealed to others, and when safety is more important than privacy and vice versa.

Seven case studies were conducted in order to fulfil objectives 1-3 and the second research question. The results from the studies are presented in
Chapter 4-7 and published Papers 1-7 included in the thesis. The synthesized results concerning problems and needs are described in Section 9.2.1 and visualized in the extended security model. Section 9.2.2 presents the synthesized result concerning the balance between patient safety and patient privacy.

9.2.1 Compilation of Problems and Needs

Figure 9:1 illustrates the compiled result of problems and needs of information security in healthcare presented in Chapter 4-7. For the compilation, the extended information security model was used as a way to further classify problems and needs in the administrative part compared to the previously presented results. The symbols in the Figure 9:1 are noted according to case number, respondent notation (if it existed) and number of the question (e.g. the symbols 4A1a refers to case study number 4, respondent A and question number 1a). We refer to Papers 1-7 for more detailed information concerning the results from each study.

With regard to technical security problems derived from the included studies, the following main problems have been identified:

- **Authentication techniques** (2a, 2c, 3e, 4E1d, 5:4a-b, 6A1d, 6B1d, 6D1d, 7:4c, 7:4e)

  Passwords are still a common approach for accessing patient records as well as communication networks. The healthcare sector is aware of the
weaknesses of password authentication, but is waiting for new regulations and methods for implementing strong authentication techniques. Some projects are in progress, but so far they do not have any decisive power. It is worth noting that according to the law, patient information is defined as sensitive and should be protected with strong authentication as well. It is obvious that the healthcare sector suffers from the inability to act.

- **Authorization techniques (1d, 4B1c, 4B1d, 4C6, 4C8, 4E1d, 5:6, 6A8, 6B1d, 6B8, 6C1a, 6C1d, 6C8, 7:2i, 7:2k)**
  This issue is twofold. Partly, there is a problem with insufficient access levels and consequently, a too wide access of patient records. Our studies show that patient information can be accessed by a wide range of healthcare actors, those involved in the patient care and not. The other side of the problem is that there is a need to increase the accessibility of patient information to involved actors from other healthcare organizations. At present, this is not possible either technically or legally. The obvious risk is that patient information can be revealed to unauthorized individuals while at the same time it is not available to healthcare actors who need information about a patient. Consequently, patient safety and patient privacy are both omitted.

- **System integration (4A3, 4B3, 6A1d, 6A3, 6D4, 7:4a)**
  The present insufficient techniques for patient information exchange constitute a serious security risk for achievement of patient safety. The availability of patient information to authorized healthcare actors is, as mentioned above, a strong requirement in order to provide sufficient care.

- **Absence of logging management tools (3f, 4D1d, 5:10, 6B1d, 6C1a)**
  Common to all the studies is the absence of logging management tools. Depending on what approach the authorization is based on, the importance of checking the logs varies. The results show that mainly a wide range of access levels is used. Hence, log-checking routines must be provided in order to maintain trustworthiness in healthcare. If no tool for logging management is implemented, the risk is obvious, as our results also show, that log-checking will not be provided.

- **Insufficient technical security mechanisms (1e, 2d, 3c, 4A1a, 4A1c-d, 4A4, 4C1c-d, 4D1e, 4D4, 4E1e, 5:3, 5:5, 5:7, 5:8c-d, 5:11, 5:12, 6A-D1c, 6A4, 6B6, 6C6, 6D1a, 6D3, 7:2h, 7:4b, 7:4d)**
  Beside the issues mentioned above, the result also shows the following technical security problems; lack of back-up techniques and routines, insufficient encryption in the patient record systems, no computerized healthcare records, and interruptions in the communication networks.
With regard to physical security, the following issues were identified; theft of equipments and hospitals that are too open.

The main information security problems in healthcare concern the administrative area to which almost all of the technical security problems mentioned above are closely connected. The following main administrative problems are highlighted in our studies:

- **Lack of responsibility-taking and leadership** (4A6, 4B1a-b, 4B3, 4B6, 4B8, 4C3, 4C8, 4D1b, 4D3, 4D8, 4E6, 6A3, 6B3, 6B4, 6C6, 6D8, 7:2c-e, 7:2g, 7:4f, 7:4h, 7:4k-o)
  The results show that the healthcare sector at a national management level is lacking concerning responsibility-taken and leadership, such as lacking political and legally responsibility, different folkways and lacking coordination. The healthcare sector does not know what they actually want.

- **Lack of information security policies and regulations** (1a, 3a-b, 3g, 4A1b, 4A8, 4B1a, 4B4, 4B6, 4C1a, 4D6, 4D8, 4E1b, 5:1, 5:8a, 5:10, 6A4, 6A6, 6B1b, 6A-B8, 6D6, 7:4i)
  Our studies show that security policies and regulations do not exist or are incomplete. Consequently, the foundation of security work is missing, which must be seen as a main reason for the security problems in healthcare.

- **Insufficient security education** (1b, 3h, 4A1b, 5:9, 6B6, 6C1b, 7:4g)
  A lack of security education has been shown in all our studies.

- **Missing compliance and follow-up routines** (1c, 4B1b, 4C1b, 4D1a, 5:8b, 6A1b, 6A7, 6C1a)
  If a healthcare organization has started its security work, it is mostly focused on risk management, policies and regulations. Compliance and follow-up routines are generally non-existent.

- **No clearly identified patient process** (4A3, 4C3, 4E3, 4E8, 6C3, 7:2f, 7:4j)
  One important issue in our studies was the opinion that a comprehensive view of healthcare is missing, and that the healthcare sector does not hence consider the patient’s whole situation. There is a lack of access to patient information and no person responsible for the flow of patient information. The results show that one reason is that no clear patient process has been identified.

- **Inadequate security awareness** (2b-c, 2e-g, 3d, 4D1a, 4D6, 4E4, 4E6, 5:4c, 6A1b, 6C1a-b, 6D1b, 7:2b)
  The individual will always be the weakest link in an organization’s security chain. Healthcare is not an exception. The results show that
healthcare actors as professionals, have an awareness of protecting patient information, but due to the lack of fundamental security structures and management, new technology implementation, and deficient security education, there is a general lack of security awareness.

All technical as well as administrative security problems indirectly affect the four characteristics of information security. However, from the respondents’ point of view, some problems are directly linked to these characteristics. The lack of availability (4A-B1a, 4E1a, 4A-E7, 6A-B1a, 6A-E7, 6C4, 7:2a) of patient information, for instance, is an important security problem. This mainly depends on a lack of technical solutions for transferring patient information between different patient record systems, and organizational structures for efficient patient information management between the healthcare organizations. Furthermore, the results reveal integrity problems (4A1d, 4D4), such as incorrect patient information, as well as confidentiality problems (4B1a, 4E1a, 4C-D4, 6A-B1a, 6B-D7, 7:2j), such as too broad access levels to patient information, which increasingly risk that patient privacy is neglected.

It should be noted that no problems have been identified in the accountability part of the model. This does not mean there are no problems with regard to achieving accountability, but in our investigations no such problem was directly mentioned. However, indirectly it is obvious that accountability will be omitted, for instance, when employees use each other’s logins or group logins are used.

9.2.2 The Balance between Patient Safety and Patient Privacy

Figures 9:2-9:4 presents the compilation result from the issues concerning the balance between patient safety and patient privacy; current focus, desired focus, and probable future focus. The notation follows the same structure as before, the number relates to the case number and the letter relates to the respondent (for instance, 4A – case study number four and respondent A). As previously mentioned, the small square in the patient safety box represents the respondents’ desire to unite the two aims into one, and not to polarize them.

![Figure 9:2. The compilation of the current focus on the balance between patient safety and patient privacy](image-url)
The focus on patient safety and/or patient privacy varies between both countries and among the respondents in the same study. However, in Sweden, the result shows that from the organizations’ view the focus is on patient safety, while the legislation is more focused on privacy. One of the Swedish respondents stated that privacy must not be polarized as its own concept, but must instead be included in the safety concept refusing to separate them. Another respondent had the same opinion, but only emphasized it in “the current focus”.

**Figure 9:3.** The compilation of the desired focus concerning the balance between patient safety and patient privacy

One assumption concerning the desired focus on safety and privacy is that there should be a balance between these concepts. However, only respondents from the international outlook fulfilled that assumption. In Sweden there are more voices expressing a focus on safety than on privacy, also in the desired situation.

**Figure 9:4.** The compilation of probable future focus concerning the balance between patient safety and patient privacy

Comparing the desired focus with the probable future focus, the result shows that from a Scandinavian perspective, patient safety will be more emphasized. On the other hand, the English respondents believe that privacy aspects will be focused on more in the future. It is obvious that Scandinavians have a more naive view of privacy aspects than English people. One reason for the differences is that the UK is at war and therefore subject to obvious threats, not the least of which are those of terrorism. This
implies that the government must implement security measures such as surveillance cameras in public areas, as well as more access to personal data, in order to guarantee the nation’s safety. Sweden has not been at war for two centuries, and Swedish citizens hence trust their government to a greater extent. They have good faith in the government’s ability to protect them, and are less obviously fearful their privacy will be neglected, even if there are concerns in that area too.

9.3 Suggested Security Measures to Improve Information Security in Healthcare

The third research question concerns what security measures are required in order to achieve a reasonable level of information security, taking into account the patient’s need for safety and privacy. It corresponds to objective 5:

**Objective no 5:** *To propose suggestions for security measures that are needed to achieve a reasonable level of security, technical and administrative, by developing a set of guidelines and recommendations.*

In order to come to grips with the problems and needs presented above, a set of guidelines and recommendations has been developed. These guidelines and recommendations are primarily intended for people at the management level of the healthcare sector, for instance, chief security officers, politicians, other authorities, and so on. It has been found that when a lack of security is identified in the working area of the end-users, this depends primarily on information security issues never reaching the management level of organizations. However, these guidelines and recommendations should be useful and of significant interest to people working in healthcare as well, for example, healthcare practitioners, IT-technicians and system developers. Furthermore, it is worth noting that a hundred percent security can never be achieved. The challenge is to reach a level where the business requirements of security, external as well as internal, have been analyzed and estimated. Then again, a reasonable level of security originates from business analysis, current state analysis and risk analysis, in order to determine a suitable level of information security.

The set of guidelines and recommendations has been divided into three main groups. The first group comprises the overall guidelines and recommendations for improving information security in healthcare, while the second and third groups are divided into administrative and technical security guidelines and recommendations.

We propose the following overall guidelines and recommendations:
Identify and proceed from the patient process.

One of the problems identified in our studies is the absence of the patient process analysis. In order to ascertain the needed patient information and how to protect it, the patient processes must be identified and analyzed. This activity is important in order to recognize the IT-solutions necessary for supporting the patient process and achieving good quality healthcare that includes respect for patient privacy. It is not enough to only consider the business processes, even if their importance cannot be underestimated. Business processes should be seen as those supporting the patient process. A generic patient process is hard to identify and probably does not even exist. However, by analyzing real patient processes, specific deficiencies and needs can be identified, which can be further analyzed to subsequently determine generic problems and needs. This is exemplified by the following two situations: one patient’s surgery is canceled due to out-dated X-ray images, which results in a wait of another 2.5 months for the operation; another patient whose husband dies two days before her scheduled surgery must defer the procedure for personal reasons. In the latter case, it took another six months before the surgery was performed. Patient safety was neglected in both cases due to inadequate routines and insufficient communication between the patient and the healthcare organizations. In some sense the patients’ privacy was also neglected because these deficiencies, which result in suffering considerably longer than necessary, imply disrespect towards the patient. Hence both patients safety and patient privacy was neglected. These two examples demonstrate a need to improve routines concerning change of surgery bookings. Furthermore, the patient processes must be identified and analyzed at different levels, at specific units, such as GP, surgery-, medical-, X-ray department, and so on, as well as the cross-border patient process involving different units and organizations. This is an activity intended for people working at various levels of the healthcare sector and the patient as well. Hence, we emphasize that patient process is the most important issue to identify and analyze in order to obtain patient safety and patient privacy.

Introduce a coordination function in cross-border healthcare planning

In order to support the patient process, we suggest the need for a coordination function, which includes a representative who can plead the patient’s cause. It is important to solve the issue of the lack of coordination in healthcare in order to achieve patient safety as well as patient privacy. The responsible healthcare leaders and politicians must take an active part in dealing with this aspect. If collaboration between different caregiver organizations is to function satisfactorily, especially with regard to patient information management, there is a need for, what we have term a “coordinator” with an active responsibility to ensure that
collaboration takes place. This guideline has been published and presented at iSHIMR 2006 conference (cf. Paper 9).

The following administrative security guidelines and recommendations are suggested:

- **Base the information security work on established and well-known standards for information security management.**

  The secure management of patient information must always be a matter of course for the healthcare sector. The best way to reach a sufficient level of information security is to use a structured way of working, and hence, the use of a well-known standard. The international standard, ISO/IEC 27002 (previous ISO/IEC 17799) Code of Practice of Information Security Management (ISO/IEC, 2005b), provides a substantial and practical support for adopting risk analysis, and introducing routines and organization that help to manage information security faithfully. In addition, a healthcare version of ISO/IEC 27002 is under development, which will be entitled: ISO/DIS 27799 Health Informatics — Security Management in Health Using ISO/IEC 17799, (2007). The purpose of this version is to provide guidance to health care organizations and other keepers of personal health information on implementing ISO/IEC 27002 (ISO/IEC 2005b). Furthermore, the implementation of information security standards must be provided at different levels, national as well as regional and local. This guideline is thus intended for managers at all levels.

- **Establish dialogues and informal meetings in order to increase the security awareness**

  This activity can be based, for instance, on incident management outcomes, in order to increase the security awareness of the healthcare actors. The establishment or improvement of formal activities, such as information security education, and so on, does not constitute a guarantee that the security awareness will actually increase, even if the purpose is increased security knowledge. According to the results, an effective way of increasing security awareness is, for instance, when management quickly reacts to an incident and identifies what went wrong and what should have been done instead. Obviously, such reactions increase security knowledge, and in the long-term security awareness as well. The aim, in this instance, is not to blame anyone. Instead it is necessary to stress the incident as a practical example in order to prevent new incidents and to increase security awareness in the organization. This guideline is intended for all the people with some security responsibility in their position.

- **Establish and improve information security education.**

  One of the most important factors in order to spread information security knowledge is education. This is, in general, the most neglected
issue concerning information security and the healthcare sector is not an exception. Resources must be allocated for security education at all levels of the healthcare sector. For example, specific educational programs for information security should be established or improved, and provided at the beginning of employment. Furthermore, continuous security education activities during employment should be established, preferably in combination with other competence increasing activities within the healthcare business. Additionally, implement security features in academic education programs for all kinds of healthcare professionals dealing with patient information. This guideline is intended for people working with education in healthcare, as well as in the academic community.

- *Establish contingent liabilities in order to clarify needed responsibility as derived from the patient process.*

  The issue of responsibility with regard to the distribution of patient information between different healthcare organizations must be clarified. Information “falling between two stools”, due to organizations denying their responsibility should be avoided. Conscious responsible obligations between involved organizations are required. This guideline is intended primarily for politicians and managers in different healthcare organizations.

- *Include all aspects of information security in the continuing work with the National IT Strategy for eHealth.*

  The National IT Strategy for eHealth is under development. According to the status report (National Board of Health and Welfare, 2007b) multiple interaction activities are in proceeding, in order to provide, with an assistance of purposive IT solutions, good and safe care, as well as good level of service for all patients. It is necessary to include information security aspects as an integral part of their whole strategy, not only in the work with the technical IT infrastructure. In this development, there is a superb opportunity to explicitly include the standard ISO/IEC 27002 Code of Practice of Information Security Management (ISO/IEC, 2005b) as a standpoint for further direction. This guideline is primarily intended for the National Board of Health and Welfare that has the responsibility for the implementation of the National IT-strategy for eHealth.

- *Adapt and review existing legislation to better support the patient and the patient process.*

  There is a need to increase the boundaries of confidentiality in the legislation, in order to support the patient process, and it is a necessity to maintain and improve the restrictions for people not involved in the patient’s care. Furthermore, it must be possible for patients to have direct access to their own information, both patient record notes and
logging lists. This is more of a recommendation and is intended for politicians and investigators at the national level.

- **Organize the healthcare sector to better support the patient and the process.**

  If organizational boundaries, such as administration, legislation and financial aspects, prevent the efficient management of the patient process, the healthcare sector must be reorganized, so that it can support patients and their process. This is a recommendation to politicians at the national level.

The following technical security guidelines and recommendations are intended for people working with security technology and for healthcare managers. As mentioned, technical solutions must follow from activities at the administrative security level. Hence, the healthcare managers are responsible for ensuring that sufficient technical solutions are implemented. The technical security guidelines and recommendations suggested comprise:

- **Implement strong authentication techniques**

  Patient information is sensitive information. Strong authentication techniques already exist in the market, and the SITHS project has provided the foundation for such implementation. There are no excuses for not implementing such techniques on a broad front, also in the healthcare sector.

- **Adapt the authorization to support the patient process**

  Introduce access control systems based on a need-to-know model implying that only healthcare actors involved in the patient process would have access to needed patient information. This entails that all healthcare actors involved in the patient process would have access to precisely the patient information he or she needs, as much as possible. The focus must once again be based on the patient process analysis in order to identify which actors really need access to patient information. Remaining actors must, as far as possible, be denied access. A refined need-to-know authority model can be overwhelming, but should be more emphasized compared with the existing wide access levels that ours results have shown.

- **Introduce log management tools**

  This is necessary because we need to be able to identify who actually accesses any particular patient record. Since a stringent authority model will probably never be completely implemented, follow-ups must be managed properly. Our results have shown that there are major deficiencies concerning the following-up of the logs. Log management tools do not exist. In order to achieve trustworthiness for patient
information management in healthcare, an all-out effort for the implementation of log management tools is needed.

- **Introduce encryption to protect sensitive patient information**
  In order to protect sensitive patient information encryption must be implemented in EHR, as well as in other equipment such as facsimiles. Our results have shown that patient information is stored in EHR, to a great extent, and transferred between healthcare organizations with the help of facsimiles without any encryption. Sensitive patient information must be encrypted with well-known and strong encryption algorithms. This is especially necessary when mobile equipment is being used more frequently.

- **Implement communication management tools**
  Communication networks must be managed with automatic tools including, for instance, intrusion detection, virus detection, account management, and log management. It is not acceptable that these activities are managed manually and, as our results have shown, only when something suspicious has already happened.

- **Improve the shell protection concerning buildings and equipment**
  Physical security problems have not been stressed to a great extent in our results. However, they do exist and need to be managed. Hospitals and other large healthcare centers with numerous visitors must improve their fire and shell protection by using, for example, access control, alarm technology, and camera monitoring to a greater extent. Implementing fire practices more frequently is another example. The physical protection in small healthcare units also needs to be emphasized to a greater extent. At what level and to what degree these activities should be implemented must be based on risk analysis and the policy documents. Once again, a management system for information security must be the fundamental starting point.

Figure 9:5 shows how these guidelines and recommendations are structured in the extended information security model.
Synthesized Result and Suggested Guidelines

Figure 9:5 Guidelines and recommendations presented in the extended InfoSec model.

Guidelines and recommendations covering information security as a whole, and hence specifically addressed to the healthcare sector, are placed in the information security box while remaining guidelines and recommendations are located in the respective parts. However, guidelines and recommendations, related to both computer and communication security are located in the IT-security box. It should be noted that the guidelines and recommendations as a whole are derived from the compiled problems and needs presented in Chapter 9. However, all the identified problems and needs do not have one specific connected guideline, because these problems will be managed by guidelines and recommendations from other areas. For example, the problem of communication network interruptions will, to a large extent, be solved by the guideline of implementing standards for information security management.

In summary, since the results presented above have fulfilled the objectives and hence answered the research questions, we claim that the research aim has also been fulfilled. We have identified and elaborated problems and needs regarding information security in distributed healthcare from several viewpoints. Furthermore, we have developed a set of guidelines and recommendations that we consider are well-founded suggestions to be achieved when patient information has to be exchanged between different healthcare organizations.
10 Concluding Discussion and Suggestions for Future Research

This chapter includes a discussion of the research method, the results, and of the thesis contributions (in 10.1 – 10.3). The research quality is discussed and the chapter concludes with directions for future research.

10.1 Method

This work has taken a broad approach by: 1) including the whole information security area, that is, administrative security as well as technical security, 2) focusing on distributed healthcare, 3) investigating the phenomenon of information security in healthcare from several perspectives, and 4) explicitly including the patient. It could be argued that the approach is too wide and thus risks not covering enough details in some areas. As mentioned, however, the broad perspective was an active choice, since the information security area as well as the healthcare sector suffers from stovepipe thinking and a lack of complete solutions. Although it is not possible to cover everything, we still claim that we are on the right track, since the results clearly show a need for a comprehensive view within the area. Despite the fact that the patient is the most important actor in healthcare, it is remarkable that so little patient-centred research has been conducted. This includes research concerning information security in healthcare. However, it is important to have the courage to examine the patient process, and consequently involve several actors, and healthcare organizations to investigate and analyse the phenomenon from different perspectives. Our work does not include all viewpoints and actors, since for example the role “physician” is only involved in our research to a minor degree. The reason for not involving more physicians is that we attempted to use a similar variety of different roles from the various healthcare organizations. The municipalities’ home healthcare units do not have “their own” physicians, but instead patients involved in home healthcare have to contact physicians at the healthcare centre in the same way as other citizens. However, the physicians’ opinions would be of considerable interest to future research as pointed out in Section 10.5.

The private healthcare sector has not been involved either, which depends on the need to delimit the work. In addition, the private sector only constitutes a minor part of the Swedish healthcare system. Furthermore, the main part of the private healthcare business is outsourced from county councils and municipalities. Nevertheless, according to the Health and Medical Service Act (SFS 1982:73), the public health organizations, in their capacity as authorities, still have the responsibility for the care content of the outsourced healthcare business. This area may also be of interest for future research. For example, does the private healthcare sector suffer from the same problems as the public one? Hypothetically, the private sector should be in somewhat better situation according to the results from their minor
Concluding Discussion and Suggestion for Future Research

corresponding to our research in case study 3 (cf. Paper 3). Furthermore, the private sector usually has smaller organizations, which can reach decisions faster and implement changes more easily.

Our work was mainly conducted as an explorative study based on case studies with observations and interviews as data collection techniques. The number of persons that were observed and interviewed in each specific study reflects the intention of spreading the interviewees across different roles in the organizations, in order to include as many healthcare actors as possible. Nevertheless, the choice of who to observe or interview is important for the results. In the first two studies, the selection of participants was made by the organization itself. This may have had a biased impact on the results, since the organization had the possibility of selecting a more favorable respondent from their perspective. However, in healthcare, it is difficult to recruit participants that are both suitable and able to allocate enough time without the influence and approval of the organization itself. In the remaining studies, the author herself contacted the relevant respondents. This was made possible because of their management positions and thus being responsible for their own time. In the study in England, which includes actors working in the field other than managers, the choice of participants was delimited by the healthcare organizations’ unwillingness to supply professionals. It was relatively easy to call managers and ask them for an interview, but requests for interviews with nurses and other actors working in the field, were met with doors as good as closed. Instead, the choice of healthcare actors was provided by contacts leading to other contacts, and the strategy for selecting interviewees from the field can thus be regarded as a bottom up approach. The nurses contacted were very interested to be involved, since they find this area important but neglected. However, it was necessary to assure them that their managers would not be informed about their participation. This might be due to a more hierarchical culture in which field workers have less authority to act on their own without permission from the manager. This circumstance has however, not occurred in the Swedish studies.

The choice of healthcare organizations included primary as well as secondary care and municipal home healthcare units. These three types of healthcare providers represent Swedish public healthcare and were chosen in order to achieve a broad view of how different healthcare providers manage information security. Nevertheless, since these healthcare providers are at a regional level, this may reflect results that do not mirror the whole of Swedish healthcare. However, the geographical area of case studies 1-3 constitutes a central and one of the larger regions of Sweden. It is representative since this region is neither in the frontline nor backline of implementing IT in healthcare. On the other hand, in case study 4, the focus was on a national view from a manager perspective. The authorities and organizations in this study were chosen, because the interviewed persons representing them are known for their knowledge and experience in Swedish
healthcare. The same structure was used in the remaining studies. Concerning the international outlook, study 5 is set-up similarly structured to studies 1-3, in order to cover a broad set of healthcare providers, while study 6 has the same arrangement as study 4, in order to cover a management perspective from a national view.

Furthermore, the participants involved in the case studies can be considered a relevant example of average employees in the healthcare sector. They have considerable experience in their working field of work, since they have been employed for a longer period of time, and they are familiar with information management in healthcare. However, from the patient perspective, it could be possible to discuss the participants involved. When is a relevant sample of patients achieved? We argue that these patient representatives have sufficient experience and knowledge to enable them to present an adequate, clear picture about the status of patient situation. However, further involvement of patients is necessary, as we have already pointed out.

Since several healthcare providers, various healthcare roles, as well as patients are represented and participated in our research, we consider that a comprehensive view of healthcare has been attained. This, together with the broad perspective of the information security area, including both technical and administrative aspects, means that a holistic approach has been achieved.

Taking part in healthcare work through observations and interviews has been regarded as an effective way of obtaining knowledge about a specific phenomenon. Furthermore, the discussions and dialogs with the participants have given rise to new perspectives and ideas for future work (cf. Section 10.5).

Another interesting aspect in this context concerns the positive effect that the meetings with the participants have resulted in. When the results were validated by one unit manager, she said: “Since you were here and made the interview, I have been much more conscious about the security issues and I often think the matter over before I do something in order not to disregard the security”. This example reveals how the interaction with people, for the purpose of investigating some issues, may also generate new knowledge for them. This must be considered a positive aspect, especially since our results point to a lack of user awareness concerning information security.

10.2 Results
This section discusses the results from each of the research questions with respect to their contributions to the fulfillment of the aim. Section 10.2.1 discusses improving the understanding of information security, identified security problems and needs in distributed healthcare (10.2.2), and suggested security measures to improve information security in healthcare (10.2.3).
10.2.1 Improve the Understanding of Information Security

An information security model was created in phase I and further elaborated in Phase II, in order to improve the understanding of the information security concept. Relating the concepts, patient safety and patient privacy, to the characteristics of information security must be seen as a success. It facilitated the understanding of information security when this aspect was presented to the case study participants. The relation also emphasizes that both concepts need to be taken into account, and that it is necessary to address all four characteristics of information security before claiming that information security has been achieved. We do not claim that these connections are absolute, but they do help to connect the information security aspects to the healthcare area.

The extension of the administrative part of information security is another result that improves understanding. The result shows that this division is useful and stresses the formal and informal parts of security problems, and identify what kinds of measures need to be improved. However, it can be discussed if the divisions between formal/informal and external/internal are sufficient. Therefore, the continuing evaluation of the extended InfoSec Model is an activity for future work, see Section 10.5. In this work, we consider that the division has provided a clearer understanding of the administrative problems and needs and hence also what kind of security measures need to be taken into account.

10.2.2 Identify Information Security Problems and Needs in Distributed Healthcare

The respondents identified one common problem, which we also claim is the most important one, that a comprehensive view of the whole area concerning patient information exchange between different healthcare actors is missing. Healthcare work processes and patient processes have to be analyzed in order to determine what kind of patient information is required and by whom, as well as to achieve a high-quality information flow and its protection. This is also in agreement with other findings (National Board of Health and Welfare, 2004; Data Inspection Board, 2005; and SEMA 2005), but there is a need to proceed from talking to acting. From an information security perspective, our research shows that patient participation should be encouraged, since the patient is the only one who can ultimately determine if patient safety and patient privacy have been achieved or not. The healthcare sector still has a long way to go before patients are truly involved in their own processes.

The results also show that there are deficiencies both at the technical and the administrative level of security. At the technical security level, these deficiencies primarily concern authentication, authorization and logging techniques. Vulnerability of communication networks is another main problem. It is notable that the organizations only use passwords as the
authentication technique. The results also reveal that healthcare actors in the field have no intention of changing or improving their techniques in the near future, while the managers know that healthcare needs to proceed in that direction. Different healthcare reports (Carelink, 2007; SOU 2006:82) claim that strong authentication techniques such as “smart cards”, and so on, should be used when, for example, sensitive patient information is managed.

Furthermore, all the Swedish organizations in our research more or less use the parole “Everything that is not forbidden is permitted”, that is, all patient information is available to all users of the systems. The authorization techniques used are insufficient or their requirements are not fulfilled. For the most part, the system administrators decide the authorization level, and not the managers. If the willingness to implement strong authentication techniques is strong enough, there are secure authorization and authentication techniques available on the market.

One of the organizations uses incident management techniques. The others claim they do not have any incidents and consequently do not need such techniques. This is noteworthy, since how can they know that incidents do not exist if they do not use techniques that aid in their discovery? None of the healthcare organizations have techniques to manage the logs. This must be considered a major security risk, particularly with regard to patient privacy. Since they use the logging model to a large extent, the opportunity to adequately check the logs is necessary to achieve trustworthiness in the healthcare and to protect patient privacy.

The communication networks are deficient in functionality and availability. In order to achieve reliability, these networks must be improved in design and infrastructure. A wireless communication infrastructure is needed in the future, but rules and routines for security must first be introduced.

Open hospitals are a problem with regard to stolen equipment and easy access to patient information. Monitors are placed where people pass by, and screens can easily be seen. This has not been considered a major physical security problem in our research, even if the risk of disregarding patient privacy is obvious. England has a higher level of physical security than Sweden, which does not have, for example, the same kind of continuous fire training programmes at the GPs’ units. One reason is that England lives in a state of preparedness in a different way than Sweden, due to the threats of terrorism.

Technical security problems and needs should not be neglected. It is remarkable that in spite of the strong and rapid IT development, technical deficiencies still remain.

At the administrative level, there is a lack of overall security documentation such as IT strategies and information security policies. If they exist, they are
unclear and have not been communicated to the users. This is a major security risk, since healthcare actors cannot possibly know how to manage security if they do not get this information from the managers. Since the strategy documents are inadequate, the overall level of information security is deficient. Other findings, such as deficient compliance and follow-up routines, different regulations for the users to consider, inadequate management of logs, as well as most of the technical security problems, are therefore a consequence of the non-existence of overall strategies and policies. The lack of overall strategies and policies is also mentioned as a major security problem from other research efforts (Gaunt, 1998, 2000; Katsikas, 2000; The National Board of Health and Welfare, 2004; and SEMA, 2005).

Another noteworthy finding is that there are discrepancies concerning internal security knowledge. An insufficient level of security education is of great concern. Different organizational levels view information security in different ways, that is, the overall view is lacking or not anchored in the organization. For instance, network administrators believe that some security measures are managed in the systems, while system administrators believe the network administrators manage these security measures. A similar lack of security education was found in England, Norway and Finland as well, except that England has progressed a step further concerning confidentiality. The healthcare actors in England are very much aware of the Data Protection Act and the privacy issues.

Not everything done in healthcare has a value of its own, but healthcare exists and works for the sake of the patients. The patient perspective is hence a vital aspect of information security in healthcare. Our results show that patients do not believe that the healthcare sector lives up its duties. The present focus is on patient privacy since legislation focuses on protecting this issue, which sometimes hinders patient safety. The trend is that the focus will change depending on the healthcare sector requirements on improved availability of information. From a patient perspective, privacy is important but should not be enforced at the expense of patient safety. However, if the healthcare sector is really determined to achieve patient safety and patient privacy, they must also achieve availability, integrity, confidentiality and accountability of patient information. In the same way that it is necessary to balance the characteristics of information security from given situations, the balance between patient safety and patient privacy is personal, culture and situation-dependent. Therefore, solutions must be flexible to a greater extend and be based on the analysis from different situations.

Regarding the need to distribute patient information about a particular diagnosis between several different healthcare providers, the problems are mainly at a management administrative security level. These problems include imprecise regulations, the need for common terms and concepts, no clear responsibility when the patient is transferred to another actor, and so
on. There is a need for one person, a coordinator, to be primarily responsible for the entire patient process.

To conclude, we have not rated the identified information security problems and needs since they are closely related and integrated to each other. In order to achieve information security in a broad sense, both technical and administrative securities need to be addressed. However, we do claim that the absence of a comprehensive view of patient information management is the one crucial and fundamental reason for the identified security problems and needs in general, and hence the most important one to come to grips with.

10.2.3 Suggested Guidelines and Recommendations to Improve Information Security in Healthcare

The suggested guidelines and recommendations have been formulated from a process of analysis and reasoning with regard to the results. Our research has shown that security problems cannot be isolated, but interact with the whole aspect of the purpose of the healthcare sector. Our research has focused on patient safety and patient privacy and its relation to information security. There is hence a need to emphasize security as a part of the whole business and not as an isolated phenomenon.

The two overall guidelines and recommendations with regard to the patient process and the need for a coordination function in cross-border healthcare are the fundamental ones to apply in order to improve information security concerning patient information exchange between different healthcare actors. The remaining guidelines and recommendations are more generic and concern everyday information security solutions, even if, in our work, they have been specifically developed from the problems and needs identified in our results. The guidelines and recommendations must be implemented internally in one organization and across borders for the purpose of supporting true patient information exchange.

The guidelines and recommendations provided in this thesis are closely relation to ongoing work with the National Strategy of eHealth (Ministry of Health and Social Affairs, 2006). The Swedish approach is, however, vague. Nobody actually has the courage or willingness to put the foot down and direct the way forward. According to the National Board of Health and Welfare (2007b), the principle concerning municipal self-rule requires county councils and municipalities to decide separately how they will implement the strategy. Consequently, the strategy will not reach its full impact within the next 10 years (National Board of Health and Welfare, 2007b). With regard to the use of common security standards, it is remarkable that in the National Strategy of eHealth this kind of security management system is not mentioned. Having a management system for information security would lay the foundation for solving most of the security problems we have identified.
10.3 Contributions

This work has four main contributions areas; 1) an increased understanding of information security by elaborating the information security model; 2) a comprehensive and structured list of information security problems and needs in distributed healthcare; 3) a set of guidelines and recommendations in order to advance information security measures in healthcare, and 4) a comprehensive view of information security in healthcare.

The elaboration of the information security model has increased the understanding of information security by

- providing a more comprehensive view of the information security area, and the administrative security level in particular. The model also visualizes within what areas information security activities need to be taken into account.
- showing the relation between patient safety and patient privacy and the four common characteristics of information security. Information security is an important component when improving patient safety and patient privacy, and consequently in showing the usefulness of information security. This has not been highlighted as extensively in other research.

Identification of information security problems and needs in distributed healthcare contribute in detail by

- pointing out substantial problems in sub-areas of information security and the existing security needs of the healthcare business,
- showing the importance of identifying and analyzing the patient process in order to secure patient information management within as well as between healthcare organizations,
- emphasizing the patient’s role in their own process,
- stressing the need to address the expected lack of administrative security as well as technical security,
- showing that the healthcare sector must manage the identified safety/privacy problems and needs in order to claim that information security has been achieved.

The set of guidelines and recommendations contributes in detail by

- giving rise to solutions to those working with security issues in the distributed healthcare sector,
- stressing the patient process as the main process to identify and analyze in order to achieve patient safety and privacy in healthcare.
- stressing the need for a coordination function that can plead the patient’s cause.

The holistic approach of information security in healthcare taken in this work contributes in detail by

- providing new knowledge for people working with collaboration and overall issues in healthcare by, for instance, bringing the patient process into focus.
Concluding Discussion and Suggestion for Future Research

- showing the importance of such an approach when different authorities and the patient him/herself are involved.

It could be added that the participants’ awareness and level of knowledge has been increased during the studies. This, together with the fact that these contributions have not previously been elaborated to a great extent, we mean that we have provided additional value for the healthcare sector as well as for the research community.

10.4 Scientific Quality

This section reflects on the quality of the research by using the following criteria from Lincoln and Guba (1985): credibility, conformability, dependability, relevance and transferability. The criteria are commonly used for evaluating qualitative research.

10.4.1 Credibility

Research trustworthiness is an important factor related to credibility, according to Lincoln and Guba (1985). Our work uses an empirical approach in close relation to the application field. Problems and needs have been identified from literature, seminars, and case studies in the healthcare sector. The interview notes have, when ever possible, being sent to the respondents for validation. The case study and literature analysis results have furthermore been presented and published, or in two cases received an early accept at peer-reviewed conferences, workshops, and journals. The results have also been discussed at workshops in industrial conferences in the information security community.

The guidelines and recommendations are grounded in the empirical material as well as in findings reported in literature. The guideline pointing to the need for a coordination function in a cross-border healthcare has been presented and published in a peer-reviewed conference proceeding, providing explicit credibility. For the remaining guidelines and recommendations, further explicit validation is suggested as future work. However, the guidelines and recommendations have been implicitly included in the published paper as suggestions to improve information security in healthcare. In this way, the research community has implicitly awarded credibility.

10.4.2 Conformability

Conformability refers to the degree that the results are coherent with and supported by data (Lincoln and Guba, 1985). The research approach, activities and results have all followed a similar structure. Problems have been identified from collected data and classified according to the information security model. Thereafter, suggested solutions and needs have been derived from the identified problems. Furthermore, citations have been
extensively used in the included papers in order to show coherence with respondents’ opinions and conformance of the findings.

10.4.3 Dependability
In qualitative research, it is difficult, if not impossible, to replicate the entire research process. However, reflection concerning dependability is important since it is closely related to credibility (Lincoln and Guba, 1985). Our case studies cannot be fully replicated, since our respondents are anonymous and thus not identifiable. Some have also ended their employments. However, our findings must be considered reliable since they pertain to the entire healthcare sector. Even if other respondents would be chosen for new interviews, the same results, more or less, would be expected. The analysis is straightforward and could easily be replicated. All the interview notes or transcribed interview records and observation protocols are available.

10.4.4 Relevance
We claim our work is highly relevant. The information security area and its impact on the healthcare sector is discussed and debated both in the research field and in the healthcare business. It has been possible to identify new, relevant information and references from both sides. Since the scope of our problem subject is broad, an enclosed background description of the state of the art of information security as well as the healthcare sector was included. When reflecting on the relevance of our results, these different perspectives must be regarded as pertinent since the findings from these activities show different solutions and opinions that are applicable to the suggested guidelines and recommendations. Furthermore, both practitioners and researchers have as mentioned in Section 10.4.1, validated the results. In addition, our findings, together with the suggested guidelines and recommendations, improve the body of knowledge concerning how patient information can securely be managed in healthcare in order to achieve patient safety and patient privacy. Hence, we have answered the research questions and fulfilled the aim of the work, which also show relevance.

10.4.5 Transferability
According to Lincoln and Guba (1985), a researcher on his/her accord cannot claim that transferability has been achieved. Instead, it is up to the world to judge if the work is generalizable and useful. However, we consider that our research is complete enough that a reader from a similar area would be able to judge if our results are transferable. Since our work is focused on healthcare as a specific application area, the results are therefore primarily intended for the healthcare sector, such as the focus on the patient process and the need for a coordination function. The remaining findings of problems and needs, as well as their suggested guidelines and recommendations, concern both healthcare and other areas. One example is the lack of education and security awareness, which relates to every kind of organization managing sensitive information, whether computerized or not.
However, as mentioned in Section 10.4.1, some grounding of the findings has been conducted, implying that a basic step towards transferability has been provided.

10.5 Future Work

In this work, information security in healthcare has been investigated from a broad perspective. In the future, there is a need to investigate some of the outcomes in more specific terms:

- Much effort must be spent to further investigate how the patient process can be identified, modeled and analyzed, in order to advance how information management can be improved and secured for the patient and his/her relatives. The coordination function is another important issue for further research. This role is currently vague, and there is a need to clarify, for instance, responsibilities, assigned activities and appropriate tools and other resources. More work is also needed in identifying guidelines and recommendations and critical success factors for how the balance between patient safety and privacy can be achieved and maintained. This is in correlation with the National Strategy for eHealth (Ministry of Health and Social Affairs, 2006) as well as with the Patient Information Investigation (SOU 2006:82).

- With regard to technical security, there is a need to further study suggested improvements of authentication and authorization techniques, as well as useful tools for communication network management. Examples of questions that need to be studied include: Why is it so hard to implement strong authentication techniques in healthcare? What kinds of tools are needed in order to support a stronger authority model for access levels? And what kind of techniques for managing the logs must be provided in order to maintain the trustworthiness for healthcare?

- In administrative security, which, according to our findings, is the most neglected area so far, research must focus on how existing security standards for improving information security in healthcare can be implemented. This is an important task since underlying security problems are often related to the lack of information security management. Furthermore, security education is an essential area for further research and actions. According to SEMA (2007), “The lack of education in the information security area, is one reason for what could be described as a widespread naivety”. This is a task that both the research community as well as the educational sector need to consider.

- According to our findings, information security standards as well as education should be seen as formal parts of administrative security. However, while the formal parts can be structured in security and
education planning, it is more difficult to achieve the informal needs. Questions for which activities, such as informal dialogs and discussions may be necessary include, for example: How can users become more security conscious? Are formal structures, such as policy documents and educational programs enough?

• As mentioned in Section 8.2, the extended information security model has only been evaluated in one case study. Further research should be conducted in order to evaluate the extended information security model, both theoretically and practically, in order to further establish its usefulness.

• The suggested guidelines and recommendations should be further refined and grounded, both in research and with healthcare practitioners.

Finally, information security aspects, technical as well as administrative, must be an integral part of all IT usage and information management, the healthcare sector included. Security is not something extra. Security is a normal part of doing business.
References


References


References


References


References


References


Part III

Publications

Part III includes nine papers each presenting the results from the different views of the research. Paper 1-3 presents the result from the local view. Paper 4 presents the result from the national perspective. Paper 5 presents the result from the international outlook with England in focus and Paper 6 with Norway and Finland in focus. Paper 7 presents the result from the patient perspective.

<table>
<thead>
<tr>
<th>Paper 1</th>
<th>Information Security in Home Healthcare: A Case Study</th>
<th>Rose-Mharie Åhlfeldt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper 2</td>
<td>Information Security in Electronic Medical Records: A Case Study with the user in focus</td>
<td>Rose-Mharie Åhlfeldt and Lena Ask</td>
</tr>
<tr>
<td>Paper 3</td>
<td>System and Network Security in a Heterogeneous Healthcare Domain: A Case Study</td>
<td>Rose-Mharie Åhlfeldt and Marcus Nohlberg</td>
</tr>
<tr>
<td>Paper 4</td>
<td>Information Security in a Distributed Healthcare Domain: A Case Study</td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
<tr>
<td>Paper 6</td>
<td>Information Security Problems and Needs in Healthcare: A Case Study of Norway and Finland vs Sweden</td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
<tr>
<td>Paper 7</td>
<td>Patient Safety and Patient Privacy in Information Security from the Patient's View: A Case study</td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
<tr>
<td>Paper 8</td>
<td>Improving the Information Security Model by using TFI</td>
<td>Rose-Mharie Åhlfeldt, Paolo Spagnoletti and Guttorm Sindre</td>
</tr>
<tr>
<td>Paper 9</td>
<td>The Need for a Coordinator for Cross-Border Healthcare Planning</td>
<td>Rose-Mharie Åhlfeldt and Eva Söderström</td>
</tr>
</tbody>
</table>
Information Security in Home Healthcare

Rose-Mharie Åhlfeldt

Abstract. Home healthcare is an expanding research area and it has become necessary for municipalities to manage medical information with the same confidentiality as with other care performers. Patient-related information stored in healthcare organizations is defined as sensitive information, and must be managed at a high security level. This paper reports on experiences from a case study in two municipalities of the “Västra Götaland” region in the southwest of Sweden. The research is based on the recommendations and general advice for the processing of personal data compiled by the Data Inspection Board of Sweden. The case study identifies three main deficiencies in the area of information security in home healthcare: 1) It shows the necessity for security training among personnel involved in home healthcare. 2) It also presents the need for elaborate security measures. 3) The extensive use of facsimile transmission for information distribution is another weak point concerning security.

Keywords. Information security, home healthcare, healthcare informatics, personal integrity, secrecy.

Introduction

Healthcare is an information-intensive organization, and a major part of the business includes the exchange of information. It is therefore natural to use the support of computers in order to efficiently improve such an information-intensive organization. The expanding application of computers increases the accessibility of data, especially when modern techniques, such as a network of terminals directly coupled to computers and local area networks, are applied. The unauthorized use of the data is not an illusory danger, and therefore, access to it must be regulated. The fact that not everybody should have access to the data is a logical consequence of the right to privacy. The individual must be able to check what has been registered about him or her and to whom the data are distributed. Consequently, laws protecting privacy have been introduced and information security in healthcare proceeds from laws, practice and ethics (Van Bemmel et al. 1997).

---

Healthcare in Sweden is performed by county councils, municipalities and private care performers. The Swedish reform “Ädelreformen”, which came into force at the turn of 1991/1992, has transferred the major part of home healthcare to the municipalities. These have become liable for all care, except for medical efforts performed by physicians. Consequently, there is never a complete care team in home healthcare. Instead many organizations participate (Augustsson 2001).

In 1998, the Data Inspection Board published a report about the processing of personal data in hospitals (Datainspektionen 1998). In this report they pointed out that considerations of patient’s privacy and protection of secrecy are foundational views in healthcare. This attitude seems to be more important when data is computerized. They also considered the problem of defective management of patient’s data in the computerized area.

Regardless whether if the data is computerized or not, the case study investigates home healthcare in order to examine if it still has the same defective management of patient’s data as the Data Inspection Board identified in hospitals (Åhlfeldt 2001a).

The case study includes observations and interviews in two municipalities of the “Västra Götaland region” in the southwest of Sweden.

The aim of this paper is to present the results and discussions from the case study of information security in home healthcare regarding personal integrity and secrecy. A brief description of information security in healthcare is provided in the next section “Information Security in Healthcare”. The section “Research approach” describes the research method. The result of the observations and interviews is presented in the section “Results” and discussed in section “Discussion”. The conclusion and possible future research is presented in the final section.

**Information Security in Healthcare**

Information Security is a difficult concept to define even for those people working within healthcare. Information in different forms is a necessity for healthcare work, and security is an obvious requirement for almost everything anyone does in healthcare. The demands on handling information in healthcare should be the same regardless whether a computerized or a manual system is used.

There is some related work being conducted in the area of information security in healthcare. SITHS (Secure IT within Healthcare) is a Swedish project with the aim of developing models and methods to realize the basic security functions of IT-support in healthcare. These basic functions are:

- **authentication** – control of the given identity
Paper 1: Information Security in Home Healthcare

- allocation of authority – determination of the access rights
- confidentiality – protection of information against improper insight
- integrity – protection of information against undesired changes, influences or insight
- functions for traceability – possibilities to trace actions and events to a specific user and in this way keep authorized users responsible for their actions.

SITHS defined information security as the collected effect of measures to minimize the risks intended for the accessibility, secrecy, integrity and traceability of information (Lagerlund 1999). The SITHS-project has presented a summary of the basic functions, (see Table 1).

Dahlin and Amesjö (1996) use data security as a security concept for computerized patient records. In order to say that a patient’s record has data security some issues are required:

Table 1. Information security (Björner 1999)

<table>
<thead>
<tr>
<th>Availability</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Accountability</th>
<th>IT-security</th>
<th>Administrative Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>To use resources as</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>required in</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>expected extension</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and within desired</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data must not be</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>accessible or</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unveiled to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>unauthorized people</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection against</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>undesired changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distinctly derive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>performed operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>to an individual</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security obtained</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>with help from</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>related administrated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-repudiation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>with transmission of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>information or</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>steered signal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- data is not able to be lost
- data is not able to fall into the wrong hands
- data is available when needed
- data is reliable

An important element of the information security area is the awareness of the importance of data protection within the organization. Van Bemmel et al. (1997) mean that activities are necessary to make the members of an organization aware of the importance of data protection. The introduction of computers in healthcare has also increased people’s fears that their private lives will be jeopardized. A registered person must be able to check what has been registered about him/her and to whom that data has been distributed (Van Bemmel et al. 1997). The SITHS-project also mentions two models which access information in a computerized system, the authority model and the logging model (Lagerlund 1999). The authority model implies that a user’s access to information is totally managed in advance by the regulated acquisition. The logging model implies that a user has full access to
information on his/her own responsibility and all measures can be checked afterwards. The SITHS-project recommends a combination of the two models. The reason is that an isolated logging model risks minimizing the trustworthiness of the information handling in healthcare, while an isolated authority model probably is overworked because of the extensive administration this model requires (see Figure 1).

Secrecy is another important element in the area of information security. The nursing staff seems to instinctively understand that sensitive information must always be protected against observation, improper access and the possibility of manipulation. At the same time there is an uncertainty among the healthcare staff about the limits allowed in the performance of information handling. This uncertainty has increased by the introduction of IT in healthcare and by new legislation (The Act on Healthcare Record and The Personal Data Act), which has not yet been given its full interpretation and application.

In its third report, the SITHS project declares that the most important element for information security to work in an optimal way is education (Björner 2000). It is through education that existing threats, risks and possibilities can be pointed out. The SITHS-group proclaims that this is the way to build security awareness. Measures of security, no matter how technically advanced they are, can never replace the knowledge of the staff and their attitude to the security work. Furthermore, it is vitally important that ethics and moral are kept at a high level so the trustworthiness of healthcare is enforced (Björner 2000).

Figure 1. The balance between the authority model and logging model (Lagerlund 1999).
In order to realize information security, more is required than just security functions and technology in the system. A structured routine for the security work as a whole is also required. This work must be impelled as a continuing process from the demands of the business to build up and maintain a conscious and adapted level of the information security (Lagerlund 1999).

**Research Approach**

The Data Inspection Board points out in their report that the computerization of Swedish healthcare is widespread (Datainspektionen 1998). Healthcare has traditionally been very concerned with patient privacy, and has defended patient secrecy. Even so, there are still deficiencies in the management of patients’ healthcare data in computerized systems. The examinations of the Data Inspection Board have been intended for the hospitals for which the county councils are the responsible authorities. The research described in this paper focuses on home healthcare with the municipalities as the responsible authority.

According to the recommendations of the Data Inspection Board, the following questions are asked:

- How is the patient’s identity checked?
- What strategies exist to ensure that the strict information requirements enforced by the act are adhered to?
- How are the constitutions and other organizational rules distributed to the staff to ensure that the proper statutes are followed?
- How is unauthorized access to patient records prevented?
- What is needed to improve the protection against unauthorized access in existing and future systems?
- Are there any clearly distinguished levels of access?
- Are there any persons responsible for keeping the authorities up-to-date?
- Are there any routines for following-up the information security of the organization?
- Is there any existing educational program in the organization to instruct the healthcare staff in information security policy?
- Is sensitive information in the system logged?
- How is the log checked and managed?

The study was conducted in the form of interviews with the responsible persons and the home healthcare staff. A field study was also conducted to gain a relevant knowledge of how the management of the personal data functions by following the healthcare staff in their work.

Two municipalities were chosen, one with a computerized system and the other with non-computerized system. Three people, district nurses, staff nurses and nurse’s aids, from each municipality were observed, after which
they had the opportunity to read through the text. The aim was not to provide the observed people the opportunity of change anything, but instead to inform them of the results and to ensure there were no misunderstandings. The interviewees were the observed people. Furthermore, two unit managers and two medically responsible nurses were also interviewed, totally, ten persons, five from each municipality.

The interviews were conducted in a discussion form, and interviewees did not see the questions before the interviews. The interviewer asked the questions and the interviewee answered to the best of his/her ability and these answers were written down. The notes were then rewritten and sent to the interviewed persons for validation.

Results
It should be pointed out that the basic strategies for information security, especially the IT-strategies, are better in the county councils than in the municipalities. Both municipalities included in this study have deficient IT-strategies. In one of the municipalities it has been impossible to access any IT-strategies. According to reports, old strategies that are not relevant anymore exist. New IT-strategies are in process but not yet accessible. In the other municipality, there is a proposal presented to the Municipal Executive Board about developed IT-strategies, but these are very general and more at an all-embracing level, far from any practical guidance for the users of the systems in the daily work.

Whether the systems are intended for care or not, the basic strategies for managing them are deficient or non-existent. This implies that there are already deficiencies in information security at a basic level. Strategies must exist for basic functions such as back-up routines, virus protection, cryptographic techniques, fire security etc.

From the result of the observations and interviews, three main points could be held up as apparent deficiencies in the information security (Åhlfeldt 2001b, 2001c). These points are: education, levels of access profiles and facsimile transmissions as information distributor. These three points are described in more detail in the following subsections.

Education
There is no specific educational program for information security in either of the two municipalities. The municipality with a non-computerized system has the intention of soon introducing a computerized system and they are delighted to include security education in their ordinary educational program. However, at present it is not in the educational plan. The municipality with the computerized system has not either any specific information security educational program. In the education of the computerized system, some questions of security about user names, passwords etc. arose, but it was the
staff themselves who asked these questions since it was not included in the educational program.

Furthermore, for both systems, none of the interviewed people are aware of any following-up routines evaluating the information security. According to the staff, there is no evaluation or following-up of how the information security is managed.

**Access Profile Levels**

In both investigated municipalities, there are clear levels of authorizations between the different parts of the record depending on whether they are regulated by the HSL (a Swedish acronym for the Act of Healthcare) or the SOL (a Swedish acronym for the Act of Social Service). The staff consider that these levels of authorizations are satisfactory. In the computerized system, on the other hand, there are no differences in the levels of authorizations between the occupational groups in that part of record regulated by HSL. The nurses have access to e.g. all of the records of the occupational therapist and vice versa. The levels of authorizations are under consideration and the main problem in this context is the administration of the authorization. The person responsible for the system is in charge of updating the authorizations, and the staff's experience is that this is satisfactory. New employees who have no user names are a greater problem than outdated user names in the systems. Furthermore, deputies and temporary staff generate more administration of authorizations which leads to problems in computerized systems.

In this study, the computerized system practices the logging model, which implies that all the nurses have the same access to all the care-receiver records in the municipality irrespective of the unit they are working in.

**Facsimile as Information Distributor**

During observations the question about the facsimile as an information distributor emerged. Personal data from the municipalities to institutional care is in most cases transferred as a written document sent with the patient. Information from the institutional care to the municipality or the primary care is mainly achieved by facsimile transmission. In some cases, some documents are transferred by the patients themselves or by mail. In both municipalities investigated, these documents are very often transferred by facsimile in a general way without any encryption.

The staff of both municipalities feel that the facsimiles are not encrypted and all personnel groups agree that there are deficiencies. Many transmissions of sensitive information by facsimiles exist and it is unfortunate if this information falls into the wrong hands. There are guidelines and recommendations introduced such as giving a call back when sensitive information is transmitted, but this requirement does not ensure the
information is sent to the right receiver. If the information has gone astray, it is already too late to do something about it.

Discussion

Comparison between the Manual and the Computerized Patient Record System

The difference between a manual system and a computerized one regarding information security is that the risk for deficiencies in information protection increases when the patient record system is computerized. In the computerized system, all nurses have access to the care-receiver records in the whole municipality, which implies that the risk for internal unauthorized access increases. In the manual system, it is only the district nurse who has access to the care-receivers’ records. For this reason the records are not available to other care-performers, thus the spreading of care-receiver records to other places is not a problem. Furthermore, the records are always locked in the district nurse’s office to which no one else has access thus reducing the risk for internal unauthorized entry.

The disadvantage with the manual patient record system is on one hand that it can be difficult to access the patient records accessible when they are needed but also, that patient records can be accessed both by externally and internally unauthorized people. However, this research has shown that the risk for external unauthorized access is not extensive, neither for the manual system nor the computerized one. On the other hand, there is always a risk for internal unauthorized access.

Education

Concerning information security education, there are no direct advantages that will be reflected in the budget. Another set of values than clearly economical ones, must be observed in the first place. If it is difficult to allocate resources for education when economical advantages can be obtained, the question must be asked how important is it to provide information security education, which cannot directly provide such advantages. Since personal privacy and protection of secrecy are emphasized as important parts of the education, there are substantial risks in not providing the necessary allocations of resources for this purpose, despite legislation clearly defining this question and the many recommendations and general advice existing to realize the security routines of the business.

It is not at first hand a question of how the system can support the users. It is a matter of the necessity of resources at a higher level so there are opportunities for education, partly to learn the systems but also instructions in information protection and security awareness in general. These requirements are not dependent on technology but of course the techniques can be used to mediate information to the users about current acts and directions, for example.
This study shows that education clearly falls short with regard to information security in both the computerized and non-computerized systems.

**Access Profile Levels**

As considered before, the computerized system practices the logging model. According to the SITHS-project, it is important for this kind of method that systems and administration to follow-up the logs exist (Björner 1999).

The principal aim is to develop and implement need-to-know access-controls that would protect patients’ healthcare data. The user would only be allowed to access information necessary to complete his or her job (Smith and Eloff, 1999). This is also associated with The Act of Secrecy.

The risk with the logging model is proclaimed to be obvious, which also has been presented in this work. The logging model is used to provide all the users access at their own responsibility while, the lacks of resources, there are still no routines for checking the log file. The computerized record system has been operational for more than two years. However, during the first year the log has only been checked twice (Åhlfeldt 2001c). Considering the sensitiveness of the information managed in patient record systems, the access model is to be preferred despite the amount of administration it requires. Perhaps the best practice would be to have a combination of both models.

The levels of access in the system should be such that provide the users with confidence when using the system. It should not be the user’s responsibility to decide what information he/she has access to. Today, the technology has the opportunity to provide satisfactory support to users, but it needs to be implemented in the systems. The routines that administrate the authorization should be revised. Furthermore, the administration should be analyzed to see how it can be delegated out into the organisation.

**Facsimile as Information Distributor**

According to the transmission of information by the facsimile, these deficiencies can be measured effectively by consciously considering the risks this kind of distribution leads to. If the existing recommendations of The Data Inspection Board are accepted, satisfactory information security can be performed when the facsimile transmits personal data (Datainspektionen 2002).

**Ethics**

Van Bemmel et al (1997) mean that information security in healthcare proceeds from laws, practice and ethics. This study has identified clear deficiencies in information security proceedings from laws and practice in the first hand but also from ethics. From an ethical perspective some questions must be asked. Are we less concerned with finding solutions to
deficiencies derived from ethics than those derived from laws and practice? If information about a patient is lost, or if it has been accessed by unauthorized people, what are the consequences for the organization? From an ethical perspective the question is of utmost importance but from a legal and financial perspective, probably nothing will happen. If we lose our trust in healthcare because, e.g., we use the logging model with deficiencies in its administration and the consequences for the organization are none, the risk must be obvious that in the future information security proceeding from an ethical perspective will be of decreasing importance.

**Conclusion and Further Research**

The aim of the case study was to survey the security problems associated with personal privacy and secrecy in systems managing personal data in home healthcare. The result of the study shows that there are security problems such as inadequate information security education and deficiencies in the levels of access. In addition, the work has illustrated that transmission of information by facsimile is inadequate.

Furthermore, it must be noted since there are no clear IT strategies in the municipalities on which to build information security, the possibility of providing sufficient information security is minimized.

The municipalities do not have adequate experience handling care information and have not kept abreast with the development of systems handling this kind of information. The administration of authorizations is a problem in the municipalities. There is a large turnover of employees as well as different categories of employment positions with variant geographical range. It is unfortunate if choosing a more open strategy for authorization is because the administration is a burden. This is not only a problem for care systems. The administration problem of authorizations also concerns information systems in general.

One interesting future research aspect would be to investigate how the administration of authorization can be facilitated. We must not come to the situation that we build computerized systems to facilitate the ordinary administration and then come to another form of administration, almost with the same burden and performed in a manual way. There should be opportunities investigating if the allocation of authorizations could be delegated out into the organisation so it will not be such a burden for only a few people. Furthermore, the administration of authorization should be automated with the help of computer support in order to increase the administration capacity.

Security is an important part of personal privacy protection. Satisfactory security is a demand according to The Personal Data Act. Security is not something extra. Security is a normal part of doing business.
References


Paper 1: Information Security in Home Healthcare
Information Security in Electronic Medical Records:  
A Case Study with the User in Focus$^{12}$

Rose-Mharie Åhfeldt and Lena Ask

Abstract. Healthcare manages a large amount of information, which represented in different forms is a necessity for healthcare work. Furthermore, security is an obvious requirement for almost everything one does in healthcare. Patient-related information stored in healthcare organizations is defined as sensitive information, and must be managed at a high security level. Today, for employees in healthcare, information is available quicker and easier by means of modern information technology (IT) but IT also entails new demands on information security awareness. It is obvious, from different sources and earlier work in this area, that user behavior is one of the most important reasons for the present shortcomings of information security. These deficiencies can be prevented by establishing information security policies, and by providing information and training to the users when new information systems are deployed in the business. This paper reports on experiences from a case study at a hospital in southwestern Sweden. The aim of the study was to determine how users of electronic medical records (EMR), are affected by the requirements of information security, how they affect the information security, and how well they follow the recommendations and general advice for processing of personal data compiled by the Swedish Data Inspection Board. The result from this study shows that users are indeed affected by, and affect the requirements of information security. This is due to, above all, insufficient knowledge about information security, but also because security policies and routines in the organization are inadequate. Consequently, users are still a critical factor when information security measures are applied in healthcare.

Keywords Information security, healthcare, healthcare informatics, electronic medical record, users, secrecy.

Introduction

Healthcare is in a state of major changes. The economical and demographical conditions change and new forms of healthcare and medical technology are added. Despite this, computer technology’s entry in healthcare has been slow. This is due to the complexity of healthcare with regard to different working forms and organization, but also the conservatism characterizing the healthcare (Hälso- och sjukvårdsinstitutet 1998).

Nevertheless, despite the problems and the conservatism, it is vital to understand that the opportunities offered by IT solutions are important for healthcare since it may improve and facilitate, e.g., documentation, information gathering and decision making. However, one must understand that in the short term, IT investments are costly, but in the long-term, a necessity. IT- support will generate cost savings due to more efficient work

---

$^{12}$ A version of this paper was published in Proceedings of the 2004 Information Resources Management Association International Conference, New Orleans, USA, May, pp 345 – 347.
routines and information management, but most important, it will increase the quality of healthcare (Collste 1997).

Achieving high quality is the cornerstone of healthcare, since humans beings suffering from different ailments are involved. Therefore, all efforts must be optimized and all knowledge and information made available without organizational hindrance, i.e. the right information must be available at the right level of care at the right time (Lagerlund 1999). Furthermore, all information must be documented in a way so that its quality is ensured. Since, healthcare organizations are information-intensive, one third of all resources is related to managing patient information and administration.

Different threat and risk analyses have shown that deficiencies in the staff’s area of responsibility, organization, and knowledge, are the main reasons for malfunctioning IT-systems. Furthermore, analyses also illustrates that the own staff itself is the biggest risk factor for the conscious incorrect management of IT-systems. In addition, it is also shown that the internal personnel commit most security violations (Dahlin & Arnesjö 1996).

To manage information in electronic medical records (EMR), the system must be designed for good readability and it must efficiently support daily work routines, such as the registration of new patient information and the retrieval of existing data (Dahlin and Arnesjö, 1996). According to Lagerlund (1999), healthcare staff inherently know that sensitive information should be protected against illicit insight and unauthorized access. Unfortunately, most healthcare personnel feel insecure about their own authorization with regard to, e.g., what information they are allowed to access and change.

Today, the use of EMR varies between different hospitals in Sweden. Some have just started to introduce EMR while others are as good as computerized with regard to record management. The term ”as good as”, means that some clinics in the same hospital have not yet implemented EMR-systems.

In 1998, the Swedish Data Inspection Board (DIB) published a report about the processing of personal data in hospitals (Datainspektionen 1998). In the report they provide recommendations regarding basic security measures for the control of personal data in healthcare which are as follows.

- The nursing staff must always be vigilant that the processing of sensitive personal data onto another national registration number does not occur. The patient’s identity must always be ensured through some form of checking.
- Since the Act on Healthcare Records has come into force, every controller of personal data must, without delay, develop strategies, which according to the Act, fulfil the strict demands of information security.
The controller of personal data must ensure that applicable regulations and rules are distributed within the organization so the statutes can be followed.

Workstations in use must never be left without control. It is impossible to enforce any form of IT-security if workstations in use are left unattended. The encroachment of patient record systems and other systems of sensitive data can easily occur with unsuspected consequences.

All users of the computer system should always and only use their own password and ensure that others never use it.

Computer screens with sensitive information should not be placed in the direct view of passers-by.

The access-control manager must establish checking routines to ensure that ex-members of staff do not retain access to the system.

The controller of personal data must establish regular routines for checking the IT-security in the organization.

All users of the computer system should be educated in IT-security continuously.

Every acquisition of collection of personal data including sensitive information ought to be logged. The log should continuously be controlled.

From these recommendations and the basic functions of authentication, allocation of authorization, secrecy, integrity, non-repudiation and traceability, it is important to investigate how the users follow these recommendations in order to guarantee the information security. In addition, various authors (Furnell et al. 1996; Lagerlund 1999) claim that users constitute the biggest risk concerning information security.

The aim of the study was to determine how users of electronic medical records (EMR), are affected by the requirements of information security, how they affect the information security and how they follow the recommendations and general advice from the DIB.

Research Approach
The work was conducted as a case study which included observations and interviews with healthcare staff at a hospital in the “Västra Götaland” region in the southwest of Sweden.

The study was conducted with a limited group of Swedish healthcare employees and took the form of observations and interviews. The observations took place at a hospital in southwestern Sweden. The observed people used EMR and they shared the same computer. During three days of observations at three different sections, users of EMR sharing the same computer were observed. Different levels of the staff, including staff nurses, nurses, unit manager, doctors and occupational therapists used the
computers. Relevant events of the staffs work routines at the nurses’ office were entered in an observation scheme.

The interview questions issued from the recommendations and general advice for the processing of personal data compiled by the DIB. Some questions resulted from the staff observation. Five employees were interviewed; one system administrator and four nurses. The interviews lasted from thirty minutes to one and a half hours. The aim of the system administrator's interview was to gather knowledge about how and to what extent the users obtain information about the policies, statutes and training of information security. The interviews were tape-recorded and after transcription each interview was sent to the respondent for validation.

In this paper, the results from the case study are presented and discussed. The paper includes the following outline: Firstly, a brief description of information security in healthcare is provided. Thereafter, the results of the case study are presented in the section “Results” and discussed in the section “Discussion”. Finally, some concluding remarks and possible future research topics are presented.

Information Security in Healthcare
Information Security is a difficult concept to define even for those people working within healthcare. Information in different forms is a necessity for healthcare work, and security is an obvious requirement for almost every aspect of its management. The security demands should be the same regardless if the patient information is being managed by a computerized or non-computerized system.

Some related work in the area of information security in healthcare is currently in progress. SITHS (Secure IT within Healthcare) is a Swedish project with the aim of developing models and methods that realize basic security functions of IT-support in healthcare. These basic functions are:

- **authentication** – control of the given identity
- allocation of **authority** – determination of the access rights
- **secrecy** – protection of information against improper insight
- **integrity** – protection of information against undesired changes, influences or insight
- functions for **traceability** – possibilities of tracing actions and events to a specific user and thus making authorized users responsible for their actions.

SITHS defines information security as the collected effect of measures to minimize the risks intended for the accessibility, secrecy, integrity and traceability of information (Lagerlund 1999). The SITHS-project presents a summary of the basic functions, (cf. Table 1).
Dahlin and Arnesjö, (1996) use data security as a security concept for computerized patient records. To claim that a patient’s record is data secure requires that some issues are fulfilled. 
- the data does not go astray
- the data cannot fall into the wrong hands
- the data is available when needed
- the data is reliable

Secrecy is another important element in the area of information security. The nursing staff normally has an instinctive feeling that sensitive information must always be protected against observation, improper access and the possibilities of manipulation. At the same time there is uncertainty among the healthcare staff concerning the limits allowed in the performance of information handling. This uncertainty has increased by the introduction of IT in healthcare and by new legislation (SFS 1998:544; SFS 1998:204), which have not yet fully interpreted and applied.

To achieve adequate information security, only through security functions and technology in the system is not enough. A structured routine for the security measures as a whole is required. The routine must be impelled as a continuous process arising from the demands of the business in order to build up and maintain a conscious and adapted level of information security (Lagerlund 1999).

Healthcare is controlled by a considerable number of acts, orders and statutes. A brief description of the most important acts that cause an impact on the use of IT in healthcare is provided below.

**The Patient Record Act** (SFS 1985:562) concerns information recorded on paper, or in any other form or medium. The act uses the term journal documentation, which implies everything pertaining to medical information. It is vital for the credibility of healthcare that security is guaranteed and that no recorded data can be accessed by unauthorized persons.
The Secrecy Act (SFS 1980:100) regulates the obligation to observe professional secrecy in public business and prohibit the distribution of public documents. In the Act, the primary purpose of secrecy is to protect people’s privacy. In healthcare, secrecy applies to information about the state of health or other private circumstances of individuals where it is unclear that revealing the information could be disadvantageous to the private person or someone close to him/her.

The Personal Data Act (SFS 1998:204) contains provisions to protect people against their personal integrity being violated by the processing of personal data. The Act, which is adapted to the EU rules, applies to personal data that is transmitted, disseminated or made available by other means.

The Act on Healthcare Records (SFS 1998:544) concerns care according to healthcare, dental care, psychiatric compulsion care, legal psychiatric care, and care in infection protection. In the Act, the data, which is described as sensitive by the Personal Data Act, cannot be used as searchable terms in the healthcare record. On the other hand, data regarding ailments and a patient’s state of health can be used. Only those who need access to the data, in order to perform their work can have direct use of the data in the healthcare record.

The Users and Factors Related to Information Security
The user employs the IT-system as a support tool in the business. The region of Västra Götaland claims that the user is the person who has the most contact with the system and therefore the best person to judge if the IT-system is useful. In addition, the user is responsible for looking after and reporting how well the IT-systems function. The user is also obligated to report incidents.

Concerning information security, Gaunt and Roger-France (1996) claim it is essential that the healthcare staff really understand why it is so important to maintain a secure environment for the information they store about the patients, the care and how it is organized. The best way to achieve this is to have well structured training programs which involve the whole staff.

Sägänger and Utbult (1998) claims that every third record is not available when it is needed for meetings with patients, but opposite can also be the case. The user has too much available information and not enough time to read all that is required for the patient meeting. The healthcare staff use at least 30 % of their working time managing information (Sägänger and Utbult 1998).

Gratte (1996) claims that the main security problems, are caused by human error. To all appearances, this is due to on users’ deficient training and documentation that is hard to understand and insufficient. The most
effective solution would be to provide all users with sufficient knowledge and encourage them to change their attitudes, because these are often the problem. Users often fail to understand the importance of the information. Instead they manage information stored in computers in different way to corresponding paper based information. Gratte (1996) claims that 80% of all security deficiencies can be related to the healthcare staff. Causes of the security deficiencies can be irresponsibility and lack of understanding and knowledge.

Even the DIB (1998) reports that carelessness in security frequently occurs. One reason can be that security measures are perceived as another burden in an already difficult work situation. Training in information security has been tremendously neglected in many care units. Also, motivation for positive security thinking within the staff is missing (Datanspektitionen 1998).

One secrecy problem is when a user fails to log out from the system and the next user can see information without access authorization. There is also a risk that employees reveal their passwords to individuals who may use it for crime (Sågänger and Utbult 1998). According to Furnell et al. (2000), 26% of users must remember passwords and user names for five or more applications. It is a problem for users to remember so many passwords. Consequently, users choose simple and well-known names which are easy to remember. Dowland, et al. (1999) mentioned in their paper that 29% of the people interviewed in their investigation admitted that other people know their passwords. If any employee is suspected of having exceeded their authority to sensitive information, it is possible to obtain the user name from the logging register to check if the employee has done something wrong (Sågänger and Utbult 1998). Furthermore, 75% of employees who use computers in their work utilize the equipment for non-working related activities.

Information security in healthcare should be an important part in the daily work of the staff, in order to prevent unauthorized people accessing information about the patients. Information security is also a vital aspect for the staff because they must have correct information in order to provide the patients the medical treatment they need. The availability of information in EMR has increased which makes high demands on different routines and protection measures in healthcare. To obtain a secure environment, it is necessary that the staff understands and is aware of the contents of information security. Therefore, users of all information systems in healthcare should be adequately educated in information security in order to comply with the security demands. It is also crucial that acts concerning information handling in healthcare are followed so that patients can have confidence in healthcare working staff.
**Results**

In this section, a conclusion of the observations study and a summary of the conducted interviews will be provided. A more detailed description of the observations and interviews can be found in Ask (2002).

**Observations**

When users log-on to the system, they employ a user name and a password to access the server. Moreover, depending on the program to be used, they must once again use their user name and password. These passwords can be the same. The users remember their passwords and it seems that they do not need any support for the memory. Sometimes when the users start the computer and log-on to the system they complain that this procedure takes too much time. Especially, when they are going to write just a simple note in the EMR, the log-on procedure takes most of the time. Furthermore, the users are often interrupted when they are going to write notes in the record and must leave their work place for other tasks. This way of working demonstrates that the users are not taking the responsibility for the log-out procedure in a suitable way. During the time when the user is still logged on to the system but not working with the computer, both unauthorized employees and outsiders could have access to patient information. This is inconsistent with the recommendation and general advice from the DIB.

During the observations, users allowed other users to employ their identity and authorization. It seems obvious that some users do not really understand why the log-on procedures and authority control systems exist. Furthermore, when users write notes about the patients they do not use any support for the memory. As previously mentioned, they are often interrupted by the telephone or patients who need help. Therefore, the users’ ability to remember everything is a challenging task when they are managing information about several patients at the same time.

Patient information was available in various places at the nurses’ office, besides the computerized patient records. There are medical lists, admission notes etc. which can easily be accessed for unauthorized people. On the other hand, the computer screens were placed away from passers-by who could thus not see sensitive information without entering the office. This follows DIB recommendations.

Facsimiles are frequently used to transmit patient information to other care units. This information is not encrypted and only on some occasions unidentified. The staff calls the receivers before transmissions and then receives an acknowledgment that the message has reached the right person.

**Interviews**

There is no specific training program for information security in the organization. When people begin their employment they receive an introductory document from the system administrator which includes some
security advice. Furthermore, the organization does not follow up that the advice is obeyed. The staff want more continuous security information since they do not really understand their obligations concerning log-on functions etc.

Several of the interviewed persons used someone else’s identity when making notes in the record. In various situations it happened that they thought they had logged on to the system correctly, but discovered when they were going to sign the record note, that this was not the case. Another example of such a situation is when users have too much work to do. The organization has no routines for checking that if the users employ their own user names or not. Instead, the staff is responsible for the written information in the EMR or other applications which is signed with their own identity.

In the EMR no indication is provided that users must change their passwords, but in the network system they must change it every sixteenth day. The employees have various passwords to remember. The interviewed persons use 3-4 passwords and they all, except for one user, referred to relatives or similar and then combined with numbers.

Every transaction in the system is logged. The administrator has a computerized application to check the log file, but there are no routines for managing the logging procedure and the log file has never been checked.

When the availability to EMR is interrupted, it causes irritation and frustration to the staff. The interviewed nurses claimed that it can be chaos. An interruption causes a lot of problems since they do not have the information they need. If they are warned of an interruption, they replicate all necessary records and put them in a cover, recording new notes in the EMR afterwards. All nurses claimed that this is not a suitable way of working.

**Discussion**

Managing information should be done in a way which generates more security for the patient. Moreover, this would allow the healthcare staff to spend more time taking care of and treating the patients, which are their primary tasks.

From the aim of this work, i.e. how users of EMR are affected by the requirements of information security and how they themselves affect information security, the following issues can be discussed.

The result reveals that necessary actions from an information security perspective are not taken, because there are deficiencies in the staff’s way of working. According to France (2001) most of the staff is not aware of how
to manage the EMR and common information security problems when they arise. The result from this work shows the same.

Users are affected by the requirements of information security when

- the log-on function does not work satisfactorily, for example, the log-on routine is not compatible to the users’ way of working, the password-exchange routine in the system is inadequate, the log-on and log-out routines take too much time, and the users’ problem remembering the passwords.
- the users are not aware of or have inadequate knowledge of information security issues, for example, the various regulations and statutes, different functions in the systems, as well as the risks and threats.
- they use the log-on and log-out routines of the system, in order to support traceability.
- interruption to EMR occurs.

Users can, as a result of ignorance concerning information security and computers, and due to the practice of sending facsimile messages, be affected negatively since they do not understand that they are acting incorrectly. They can be responsible for taking part in an incorrect action without knowing that it is wrong and without understanding they may be made responsible.

Users are unaware that IT-systems in healthcare are logged and how the organization manages and checks the log. According to Engström (2002) users have the right to training and information about the routines of the organization concerning how they manage and check the log file and also what kind of data is stored. Users are positive to having the system logged, partly, because they want the patients’ trust for the work they perform and partly for their own protection. This implies that users understand the existing reasons for logging sensitive information in healthcare systems.

The result also shows that there is a problem remembering several different passwords. This results in the use of simple passwords often relating to relatives’ names. This is also confirmed by Furnell et al. (2000). Furthermore, the users do not have any indication from the EMR telling them that it is time to change their passwords. Consequently, this safeguard is often overlooked.

When the availability of EMR is interrupted, the users are negatively affected. Interruptions convey more work for the staff since they are forced to duplicate registrations of patient information. However, the staff is positive to EMR and compared to paper based records, the availability of patient information has improved.

The user affects the information security in EMR among other things when
the log-on and log-out functions do not work satisfactorily, for example, the user leaves the computer for other tasks without logging out from the system. Also, other users’ identities and authorities are used.

information is handled and registered incorrectly, for example, users leave printouts at the printer; they do not check the receiver’s authority to access information; they register information on wrong patients or send patient information by facsimiles without removing the identity of the information.

deficiencies in and inadequate knowledge about applying application and that information is registered in several places in the EMR, routines for implementing the sign-technique, and the use of simple passwords often associated with relatives’ name.

The EMR’s requirement for users to log-on and log-out with their user identity is not followed every time. The users are not always aware of the risks when they do not log out from the system or leave their own identity to another employee. The attitude of not logging out from the system because it is impractical must be changed. If not, deficiencies will increase. Training is one way of changing the inadequate log-on routines, but the management of the organization is responsible for allocating time for the users and providing them with information about the existing security routines. Furthermore, simple and secure log-on and log-out techniques must be purchased and implemented in the organization. The DIB (1998) point out in their report that the systems must not contribute to the unsuitable use of an authority control system by slow and complicated log-on and log-out procedures.

The study also shows that an adequate and continuous training program concerning information security is needed. Security can only be implemented if the whole staff understands and accepts necessary security measures. Appropriate security training and attention is necessary in order for the staff to understand the consequences of their actions thus avoiding unnecessary risks (Furnell et al. 2001; Björner 2000).

The results indicate that users are still a major risk factor concerning information security because the requirements on how information security is achieved are not always followed by them. The users are in continuous need of information and training about information security in order to be aware of existing risks and threats when managing sensitive information. The log-on and log-out functions should as far as possible support the users’ way of working, instead of constituting obstruction. Furthermore, users should be aware of their own responsibility when they are exposed to more information than they need when treating the patient. In order to preserve and reinforce patient confidence, healthcare should strive for security aware users.
Conclusion and Further Research

The aim with this work was to determine how users of electronic medical records (EMR), are affected by the requirements of information security and how users themselves affect information security.

From the result above, it can be concluded that users are affected by, and affect the requirements of information security. This is due to, above all, insufficient knowledge of information security, but also to the inadequacy of security policies and routines in the organization. Consequently, users are still a critical factor when information security measures are applied in healthcare.

The question must be asked why it is so difficult to commit resources to training programs etc. for the staff. Even if various sources, both from national agencies (Datainspektionen 1998; Björner 2000) and research communities (Gratte 1996; Faulkner 2000; Furnell et al. 2001) have illuminated these facts for several years, this study shows that the situation is still the same. Concerning training, there are no direct gains that immediately appear in the budget. In contrast there is another set of values than the obviously economical ones that must be observed. If it is difficult to allocate resources for education when there are clear economical gains, it seems to be even more so when there are no such direct advantages (Åhlfeldt 2001).

From the above, it may be claimed that it is important to conduct further research on the resources needed for the staff to be able to acquire sufficient knowledge about information security matters. Furthermore, if we imagine an ideal world in which these resources are available for staff training, would that naturally lead to a sufficient awareness of information security or are there other factors that also come into play?

Another possible future research issue would be to investigate how and why it is so difficult to implement simple and effective log-on and log-out functions, for example, smart cards, single sign-on techniques etc, although they clearly facilitates the daily work for the staff.

It would also be interesting to compare our results with experience from other countries in similar areas of healthcare, for example, to compare Swedish regulations to the HIPAA standards and the users’ role in it.

Information security in EMR is a part of the whole information security aspects of healthcare. Satisfactory security as a whole is a demand according to national regulations. To fulfil this demand, the users must be taken into account.
References


System and Network Security in a Heterogeneous Healthcare Domain

Rose-Mharie Åhlfeldt and Marcus Nohlberg

Abstract. Healthcare organizations manage sensitive information in their computerized healthcare records. When the need for communication between different healthcare performers increases in order to improve the quality of patient care, the security requirements also increase in digital medical records and network systems. This paper shows the findings from a security activity in the research project VITA Nova Hemma, which aims to develop a methodology for, and to investigate the potential use of process manager technology in healthcare. The focus is on home healthcare using mobile devices, which will communicate with IT systems via a process manager. The aim of the security activity was to carry out a system and network analysis in the existing systems where the involved medical record systems and networks were analyzed from different security aspects.

The results show major variances at the level of information security in the different medical record systems and networks of the investigated healthcare organizations. Examples are: the organizations’ security requirements of the system; the organizations’ existing policy documents; security mechanisms such as automatic functions for managing user accounts and signing techniques, and common security awareness in the organization, for instance, managing passwords, system logs etc. The variances are especially located in the medical record systems even if they also exist in the network systems, for instance, the organizations view of authentication, security in mobile devices; and the management of logs.

The results also indicate that further research of security issues is necessary when different healthcare performers want to exchange sensitive patient information in a distributed healthcare environment.

Introduction

Security issues have a high priority when patient information is to be exchanged between different care performers in the healthcare sector. Healthcare has in the last decades processed from manually managed to computer based patient records. Even if this development has been slow, the IT-age has also reached the healthcare area. There are many advantages with computer based patient record systems. Van Bemmel and Musen (1997) mention advantages such as simultaneous access from multiple locations, legibility, variety of views on data, support of structured data entry, decision support etc. However, it is important to preserve the rigorous security requirements of sensitive information, such as patient information, even in computer-based systems. Furthermore, new security requirements related to

---

13 A version of this paper was published in CD ROM Proceedings of the 4th Security Conference, Las Vegas, USA, May 2005.
digitalized systems must be added and managed (Van Bemmel and Musen, 1997).

Access to patient information is not only necessary for a specific unit in a specific healthcare organization. Instead, patient information is exchanged between different care units and care performers in order to improve and provide the patient necessary care. This implies that information is not only exchanged between different units of the same organization. Communication and information exchange must also be performed between different external performers of primary, secondary, and home healthcare in order to fulfil patient care. This places rigorous demands not only on the possibilities of information exchange between different healthcare performers but also requires a new holistic view of the patients care process. In this paper the term “the care process” is defined as the process whereby various healthcare providers interact with and for the patient in order to increase his or her quality of life (Vissers, 1998). When information is exchanged between various care performers it becomes more dispersive. Therefore, new security demands, both technical and administrative, must be managed (Blobel, 1997).

This paper aims to provide a report from the security activities of the project VITA Nova Hemma which is being conducted mid west region of Sweden, and is based upon an earlier project called VITA Nova. The healthcare units involved include two municipal home healthcares, a regional primary care, a hospital and a laboratory company.

The first project, VITA Nova (acronym for the Swedish ”Vårdens IT-Arkitektur i Ny belysning”), was carried out between 2002-07-01 and 2003-09-30. Its aim was to develop a methodology for, and to investigate the potential of, process manager technology in healthcare. In the project, a prototype system based on the process manager technology (Visuera Process Manager) was built, integrating the work of the various healthcare units along a limited patient process (the leg ulcer process).

The second project, VITA Nova Hemma began 2003-11-01 and concludes in 2006-06-01. The focus is on home healthcare using mobile devices, which communicate with IT systems via a process manager. The prototype created in the first project will be further improved to include real integration of IT systems. The participants of the two projects, besides the healthcare units include the University of Skövde and Stockholm University/Royal Institute of Technology, the technology providers, Visuera Integration AB, Unicome Care (only the VITA Nova project) as well as Alkit Communication AB and Guide Konsult i Göteborg AB (only Vita Nova Hemma project). For more information about these projects we refer to the related papers (Wangler et al., 2003; Perjons et al., 2004) and the project’s home page (VITA Nova Hemma, 2004)
The Investigation

In the VITA Nova project, different security aspects of the involved healthcare systems were analyzed. Interviews were conducted with system administrators of the respective healthcare systems. In VITA Nova Hemma, further studies of the involved healthcare organizations’ systems and networks were done. Additionally, the suppliers of the patient record systems and those responsibly for the networks in the involved healthcare organizations were interviewed.

The basis for the questions in the security analysis were the ISO-standard ISO/IEC 17799 Information Security Management (ISO, 2000). From this standard, different questions related to system and network security were devised and reformulated for the interviews with the participants from the suppliers and healthcare organizations. These interviews were conducted in a semi structured discussion form manner without strictly formal questions. Further queries were added during the interviews.

The main points chosen from the ISO-standard are as follows:

System security
- Business requirements for access control
- Access control policy
- Access control rules
- Monitoring system access use
- Encryption and signing

Network security
- Policy, rules, compliance and continuity
- Technical security measures and routines

Results

A summary of the results from the interviews is provided below. The suppliers and the healthcare organizations are numbered 1 – 3.

System Security

Below is a summary of the results regarding system security.

Business Policy and Requirements

The level of defined general business requirements from the organizations, regarding access control varies. Supplier 1 had well defined documents from the customer organization while supplier 2 had only received some verbal instructions. Supplier 3 had received some documentation but relied mostly on verbal instructions or their earlier experiences.

None of the suppliers have any support for information classification in their systems. This could mean that the suppliers view of all the information as
being at the same level and should be protected with the same principles. Another interpretation is that the suppliers did not receive any requirements to classify the information from the organizations. Hence, this function has not been implemented.

Furthermore, the results concerning the suppliers’ consideration to legislation vary. Suppliers 1 and 3 argue that they have taken the legislation into consideration, while supplier 2 admits there are laws and rules they have not studied and complied to fully with the existing systems.

In summary, it can be argued that there are insufficiencies concerning policies and requirements from the healthcare organizations, especially between supplier 2 and the collaborated healthcare organization. One interesting question is in what way the organization itself is conscious of this problem and how it will affect the system security in the long-term.

**Rules for Access Controls**

All the suppliers and their systems are homogenous in the way they have designed access control. In their systems they have clear rules for access control even if they all use the principle ”everything is allowed which is not explicitly forbidden”. This implies that it is the local system administrator that has the main responsibility for detailed access control.

None of the interviewed organizations have clear rules for acceptance of, or signing for the system administrators or another technical person. This can increase the security vulnerability because when new rules are introduced they could conflict with other established regulations and thus reduce the safeguards.

**User Access Control**

Concerning users access control of the systems, all three suppliers have similar functions in their systems, which both increase security and others, which in the authors’ opinion decrease it. For instance, none of the systems have a function which automatically log the use of user accounts and provide an alarm when a user’s account has not been used during a specific time period. Furthermore, there is no other verification technique for the identification of the users than passwords. According to one of the suppliers, “there is no interest to implement any other verification technique in the near future”. The other suppliers concern with this opinion.

This is notable since both the research and security industries have pointed out that sufficient control over authentication techniques for access to sensitive information should be managed by a two part solution (Protect Data 2004), something you have and something you know. Also healthcare area projects such as SITHS, (Secure IT in Healthcare, (SITHS, 2000)) have declared that not only a two part solution for authentication is necessary, they also argue for strong authentication.
Another interesting detail to be noted is that two of the suppliers have a function which forces the users to change their password in a specific time period, while the third supplier has made an explicit choice not to use this kind of measure because they argue that “it will violate the users’ privacy”. This is an interesting aspect in the discussion about managing passwords since more or less all recommendations from the security community emphasize that information systems must have a function that force users to change their passwords in a specified time period. Another discussion concerns how many users have a fair knowledge in the field of password management and also the ability to choose new “good” passwords. A forcing function can often reduce the security instead of increasing it, which was its actual purpose. It is also important to ask in what way forced password changes are violations of privacy for the user since studies still show the users’ inability to change to and choose good passwords (ProtectData, 2004).

The possibilities of users’ to disregard protections in the system also varied. Supplier 1 means that there are no backdoors in their system while supplier 2 maintains that there will always be backdoors in systems for the programmers and others to use. If a user has adequate knowledge of computers, he/she can always gain entry to the system. Supplier 3 has a more liberal view maintaining that even if there is no possibility today to gain entry to the system, this cannot be guaranteed. These disparate answers could result from different levels of knowledge about software development, but could also depend on what kind of security protection level the supplier uses in the system.

**Monitoring System Control**

According to ISO/IEC 17799 (2000), monitoring consists of routines for recording user identity, date and time for log in and log out, terminal identity and terminal placing, recording of successful and unsuccessful system authentication, as well as registering of successful and unsuccessful access of data and other resources. The interviews show that all the systems record the user identity, date and time for log in and log out. System 2 does not record successful and unsuccessful system authentication which the other systems do. The limited logging procedures of successful and unsuccessful system authentication in system 2 and the lack of records for terminal identity and terminal placing can be considered a security deficiency. Probably, both system suppliers and the healthcare organizations consider that follow-up routines of unauthorized system control are unnecessary in a broader sense, since there are no business requirements to store this kind of information.

Nonetheless, there is no possibility to automatically store divergences in logs to secondary logs or to store the logs on separate devices.

Since the principle choice is “Everything is available …” it is notable that the logging does not have a high priority. If there is to be any possibility of
proving computer intrusion it is necessary to store logs in which you can be found records of system authentication, data access, terminal identity and terminal placing, and also features that provide possibilities of controlling logs and storing them in a reliable way.

**Encryption and Signing**

Within encryption and signing there are notable differences between the suppliers. Only supplier 1 encrypts all information in the database. The other suppliers only encrypt the passwords. Also, the selection of encryption algorithms differs between the suppliers. While supplier 1 could not provide an answer to what kind of algorithm they use, supplier 2 uses an algorithm they developed themselves, and supplier 3 has an old “dependable” symmetric encryption algorithm that they do not recall the name of.

Encryption is an advanced mathematical technique and encryption algorithms have been developed and tested during many years and in different stages and paradigms. It is a clear security risk to use an encryption algorithm that has not been sufficiently tested, since research has yet to study whether this algorithm is secure or not.

Signing is used in all systems. However, none of the suppliers use digital signatures, i.e. strong signing. Instead, they use the authentication technique as a signing technique, i.e. the user who has logged in to the system is the person who signs the record. This can be achieved in two ways. Either the records are signed automatically with the log-on password as by supplier 2 or the password can be used once again to sign the record. This last method can be used in supplier 3’s software, but required by supplier 1.

The lack of a strong signing technique must be considered an obvious security risk since previous studies (Åhlfeldt and Ask, 2004) have shown that in some cases other users’ log-on and passwords are used in order to avoid a new log-on procedure which is considered too time consuming. Furthermore, the use of accountability and tracing techniques is far more difficult if the signing technique is inadequate.

It is also interesting to note that none of the suppliers have any intention in the near future of implementing a strong signing technique, for instance smart cards, in spite of different research and other projects (SITHS, 2000) declaring and recommending this kind of infrastructure for healthcare in the future.

**Network Security**

A summary of the results regarding network security is provided below.
Policies
None of the organizations have been actively working with the SS-ISO/IEC 17799-standard. In a majority of the cases, it is not certain if the interviewees were at all familiar with the standard.

Both buyer number 1 and 2 lack a clear security policy. On the other hand there were policies that dealt with computer usage and network policies, and they are presently working on developing a new policy. Buyer 3 has a security policy that every employee must sign.

“There are examples of people being fired for browsing in the wrong places, or storing the wrong kind of pictures. This is one of the reasons why we want to have regulations; our actions tend to attract a lot of attention.” Buyer 3

Buyer 3 considers their policy to be improvable.

All the buyers have the possibility of investigate suspicions of abuse, foremost of e-mail and Internet, but this is predominantly done manually.

None of the organizations have any real continuous security education. Buyer number 1 is the only one that has any kind of continuous training, as they send out reminders on which viruses, Trojans etc that are currently active. It has been almost 10 years since buyer 2 held any security education for all their users.

“There is no further training, every new employee gets a one day education, in which 30 minutes to an hour is spent on IT, after that there are no more education” Buyer 3

There is a feeling of inherited slowness within the organizations that makes it difficult for them to actually ensure security consciousness in the users. Even if the users all feel that they have good support in their security work from the management, the lack of continuous education indicates that the investment in security is actually one that aims to use as little as possible of the users’ resources.

It also seems that the main focus is on securing user activities, such as surveillance of Internet use and e-mail, rather than monitoring for example information theft. While the internal risk in organizations is not a threat to take lightly, there are signs that they primarily want to protect the organizations against unproductive/disloyal employees.

Notably, most of the organizations do have security deficiencies if which they are aware and regard as slight, but have been unable to remove, for some reason. These deficiencies can, in some cases, be several years old. They include for instance, unencrypted wireless networks, or computers
owned by independent consultancy firms that have external connections straight into the organizations networks.

**Protective Measures and Routines**

In general, the organizations have a good understanding of their physical security requirements. Buyers 1 and 2 have a good level of protection today. Buyer 3 is well aware of what is lacking in the present solution, and has an approved budget for improvement.

Routines for continuous controls that security flaws have been corrected, updates have been installed and equipment is accurately configured are missing for buyer 1, where the controls are performed after an informal reading of relevant web pages. Buyers 2 and 3 have a more formally distributed responsibility to different groups that to some extent have liabilities.

The organizations that have experienced the need for incident report software have them. It is notable that buyer 1 does not have a system, as they believe there has not been a need for it. They might have found a need if they indeed had used a system to gather such information.

"There have not been that many incidents. Our users are very kind, so we have not noted that any users have misbehaved. It is hard to know for sure, though." *Buyer 1*

All the organizations are well aware of the possible internal threats. No one has any automatic functions for surveillance and instead look through logs etc. as needs may arise. This is probably an ineffective activity, as buyers 1 and 3 do not actually store their logs at all.

From a technical perspective the networks are all built around switches. This provides a very basic level of security. For buyers 2 and 3, whose needs for confidentiality are higher than for buyer 1, the network traffic that needs to be protected is done by encryption, either of the communication line, or the files themselves.

The protection against computer viruses are well designed and thoroughly implemented by all the buyers. The computers, servers and portable computers have anti virus software. Even if certain elements of the virus protection would benefit from improvements, first and foremost more frequent updates of all computers, the organizations are well aware of the necessity for protection against viruses. A continuous improvement process is being undertaken by all of the buyers. This could be because viruses are common, result in clear and easily understood damages, as well as providing management, users and specialists with simple risk estimations.
The use of portable computers tends to be a risk, e.g., as they are often vulnerable outside of the protected internal networks, while at the same time they are granted privileges when connected to the internal network again. Portable computer can also be easily stolen. This is something the buyers are aware of, but apart from anti virus software, there is little protection for the portable computers. For instance, not one of the organizations seems to use firewalls on the laptops. One organization that actually uses disc encryption, buyer 2, regards it as working poorly, implying it is often not used. The inadequate protection of the laptops suggests that there are major risks for the organizations as a whole and for confidential data in particular. This is an area that should be improved.

The buyers are using central firewalls, and there is a certain degree of freedom for the users to open ports in these if the need should arise. Only buyer 1 has knowledge about what kind of services are run in the DMZ. Buyers 2 and 3 are not responsible for the DMZ and consequently do not have that knowledge.

Authentication of the users poses a complex problem for the organizations. The problems arise because there are often large numbers of legacy systems in the organizations. There are many users with different user names and passwords in various subsystems. Although, there are plans for migrating all the accounts into a central authentication system, the buyers fear that it will take a long time before those systems will be ready. Furthermore, there are plans for more secure authentication using smart cards, biometry or similar solutions, but these seem to be hindered by the lack of a central authentication system, and the fact that the management has not yet requested them.

Passwords are used for authentication in all organizations while the demands of the password policy vary, then generally seem more to be functions within the systems than within the organizational policy where password length or quality is not regulated in detail. The systems require that the passwords must be changed regularly, often after 90 days. The users should then change to a new password that is not the same as those previously used. These demands of frequent changes of passwords are perceived by the buyers as facilitating users to use the same password in several systems. The users simply change all the passwords at once, to the same, new, password.

"The length of the password is not regulated, but there is a requirement to change password after 90 days. If we have too few days, the users will stick a post-it with their passwords under the keyboards, and if there are too many days the [network] system will be insecure.” Buyer 2

For large organizations, it is a complex and costly process to manage users in an efficient manner. There are good opportunities to speed up the
implementation of a central authentication system by working towards
general demands for the implementation of, for instance, smart cards. This
will not only make the systems safer, but the management of users and
authentication will also be improved. Internal routines for removing users
who have left the organizations should be automated to a greater extent,
both to improve security and to reduce licensing costs.

The logging of user activity, most importantly log-in, and network traffic etc.,
varies considerably between the organizations. Buyer 2 has very good control
over their logs, and regularly performs backups of them. Buyer 1 does not
archive their logs, and generally logs very little. Buyer 3 has made the explicit
choice of logging as little as possible, in order to prevent to providing
information to, for instance, reporters. Furthermore, the little logging they
actually do is not archived.

“We tend to log as little as possible, to avoid problems with
reporters requesting information. This is a good way to avoid that
problem [with the media], but it makes it hard to have any kind
of traceability in the [network] systems.” Buyer 3

Logging the use of the system, and archiving these logs in such way make
them difficult to modify is of the greatest importance in order to achieve
some kind of accountability and to enable the tracing of the sequence of
events in the event of an incident. Logs are often needed even to know if
something has happened. This is an area where improvement is critical.

This lack of accountability in the systems is made even more obvious as
there are no administrative duties that require they are done by more than
one administrator simultaneously. Every administrator can do pretty much
everything within the systems. All organizations are working towards
removing all shared administrator accounts, which is good.

Backups are performed automatically in all the organizations, and reasonably
extensively. It is not clear to what extent data is backed up to external
systems, stored at a different location than the servers, but the general
knowledge of backup security seems to be good.

**Conclusion and Discussing**
The results show major variances in the level of information security of the
different medical record systems and networks of the investigated healthcare
organizations. These variances are especially located in the medical record
systems even if they also exist in the network system.

The following deficiencies concerning system security were found:
- The organizations’ security requirements on the system are missing
- Missing policy documents
Security mechanisms as automatic functions for managing user accounts and signing techniques.
- Common security awareness in the organization, for instance, managing passwords, logs etc.

In the healthcare area where sensitive patient information is managed it is important to implement a high level of security solutions which must be based on different organizational as well as legal security frameworks, (Blobel, 1997; Datainspektionen, 1998). From the results above it is obvious that there are deficiencies both of technical and organizational level of security. The lack of security requirements from healthcare organizations to system developers and the absence of policy documents are at the organizational level and have higher abstraction and in some cases also more importance, since the holistic view of information security is not present (Gaunt, 1998; Katsikas, 2000).

Furthermore, the deficiencies found at the technical level must be considered a high security risk in the healthcare domain. Managing user accounts in a secure way is of crucial importance for the trustworthiness of healthcare when processing patient information. In addition, the signing technique should be based on strong signing, as is recommended by both research and the security industry (Blobel, 2001; ProtectData 2004). Blobel (2001) has pointed out that in the healthcare domain the highest digital signature level is often mandated. Obviously, this has not been implemented in the healthcare domain as a whole.

The following major deficiencies concerning network security were found:
- The organizations’ view of authentication & passwords
- Security in mobile devices
- Managing the logs
- Education of the users

Regarding the networks, the buyers all have rather good security awareness. They are conscious of the network deficiencies, but the variances lie within whether they are taken seriously or not. The organizations seem to believe that a security risk is not real if it is known. There are also some deficiencies in their routines for authentication, leading to problems with passwords. The handling of portable computers and the management of logging etc. are other problems. Some of these problems are the result of political policies, some of budgetary limitations, but others are based on the attitude towards security. Perhaps one of the major issues is the fact that the education of the users with regard to security comprises a maximum of a couple of hours, and is a one-time event. Continuous education is crucial for maintaining up a good level of security.

It is interesting to note that there are also differences of attitude to security within the organizations, i.e. the overall view is missing, or is not totally
anchored in the organization. There are network administrators who argue and believe that certain security measures are not required in the network, as they maintain that the systems take care of them, but after talking to the system administrators the contrary has been revealed. They believe that these security measures are dealt with in the networks.

Another noteworthy conclusion is that security seems to mean different things to different people, perhaps due to their place in the hierarchy of the organization. Some policies seem to be written more to ensure productivity by limiting the use of e-mail and access to places that users can surf to, than to achieve actual security. Could the outspoken interest in security from management be not only the result of the need for information security, but also to the desire for more efficient organizations, where security is a powerful tool used to enforce stricter work procedures?

It is important that the security issues achieve a higher level of abstraction. Since there are differences in the security levels between the healthcare performers in both systems and networks, questions must be raised how security will be managed when the systems are to interact with each other. Is it necessary to negotiate a reliable minimal level of security in the healthcare providers system and networks in order to maintain an acceptable security level of system integration? What kind of security mechanisms and measures are needed in integration tools, for instance a process manager, to maintain and preferably also improve the existing security level in systems and networks.

The results also indicate a lack of IT-competence when the healthcare organization orders or develops a new IT-system. Who decides the competence need for the participants to be included in healthcare IT-projects? Is there enough IT-proficiency and especially knowledge of information security within the ordering organization or is it necessary to consult expertise externally? According to Gaunt (2000) security education is necessary for the user of the IT-systems in healthcare. But it is also necessary to ensure a high level of security education for healthcare persons involved in different IT-projects. If the organization does not have sufficient security competence they would benefit from involving other security experts when they create requirement specifications in order to achieve the successful implementation of new systems in healthcare.

Security aspects are crucial for our future work in the VITA Nova Hemma project but they are also important for the distributed healthcare domain as a whole. This paper has shown that further research of security issues is necessary when different healthcare performers exchange sensitive patient information.
References


Paper 3: System and Network Security in a Heterogeneous Healthcare Domain
Information Security in a Distributed Healthcare Domain: A Case Study

Rose-Mharie Åhfeldt and Eva Söderström

Abstract. Accessibility to the right patient information at the right time is a necessity in order to provide the best possible care for a patient. This is a complex undertaking, in particular since healthcare is increasingly characterized by diversity, distributed care givers, and extended use of IT. Patient information is sensitive, and must be handled correctly and safely in this setting. This paper takes a national perspective and investigates the problems and needs concerning information security in a highly distributed healthcare domain. A small field study of five interviews was conducted to collect data. Results show that problems exist primarily in administrative security, but also that the balance between patient privacy and patient safety is difficult to maintain. Required security measures are pointed out, and the need for a holistic view is highlighted.

Introduction

Information is a valuable asset in the information society, particularly in the healthcare sector where access to patient information is one of the most important factors for safety and quality. The information must be correct and accountable. Patient information qualifies as sensitive, and is therefore classified as confidential. Consequently, information security is important to achieve and must be taken into account in the healthcare sector in order to achieve both patient safety and patient privacy [1], [2].

Swedish healthcare has been slow in implementing IT despite demands for more effective care and awareness about how it could be achieved, for instance with the help of IT. Many patients do not receive care from only one healthcare provider. Instead, they can visit their “own” healthcare centre he/she normally uses, while at the same time require, for instance, special care at the hospital, the municipality’s home healthcare or health service, or contact with the pharmacy and other actors in the healthcare business. In order to get a clear holistic view of the patient’s health, relevant information about the patient must be available when needed [3]. There is hence a great need to transfer patient information between several healthcare providers in order to support a sufficient care chain where the patient is in focus.

At present, patient information based on digitalized techniques between different healthcare providers in the Swedish healthcare system is hardly integrated at all. Much work is on-going, but implementation is slow since we must be able to protect patient information from being misused. Information security in a distributed healthcare domain is a critical factor when IT-solutions of patient information are applied [4], [5].

The aim of this paper is to present the results from a case study applied in the Swedish healthcare system in order to identify problems and needs concerning information security in a distributed healthcare domain. An information security model has been used to achieve a broad perspective. Our contribution is a holistic view of information security, which is necessary to be able to survey problems and needs as desired in the future when the transmission of patient information between different healthcare providers becomes more common.

The paper is structured as follows: Information security and the Info Sec model are presented in the following section. Thereafter, the case study and the results are presented in separately sections. Some concluding remarks are made in the final section.

**Information Security Model**

Information security concerns security issues in all kinds of information processing and includes the characteristics: availability, confidentiality, integrity and accountability. According to SIS [6] information security is defined as the protection of information assets, aiming to maintain confidentiality, integrity, availability and accountability of information.

Both technical and administrative security measures are required to achieve these four characteristics. Administrative security concerns the management of information security; strategies, policies, risk assessments etc. Planning and implementation in security work requires a structured way of working. This part of the overall security is thus at an organizational level and concerns the business as a whole. It is positioned towards what the overall security requirements should be. Technical security concerns measures to be taken in order to achieve the overall requirements. Technical security is subdivided into physical security and IT security. Physical security concerns the physical protection of information, for instance, fire protection and alarm. IT-security refers to security for information in technical information systems. IT-security can then be subdivided into computer- and communication security. Computer Security relates to the protection of hardware and its contents while Communication Security involves the protection of networks and other media that communicate information between computers.

In order to provide a more understandable view of how these characteristics and the security measures relate to one another, an information security
model has been created (Figure 1). The aim of the model is to describe, in a simple way, what information security represents. The model combines the definitions and descriptions mentioned above.

The main concept, information security, is situated in the middle. The four characteristics are placed at the top, and together represent information security. Only fulfilling parts of them is not enough, all must be included for information security to be achieved. The lower part of the model presents the different security measures in a hierarchical structure. These are gathered directly from the SIS conceptual classification [6], cf. Figure 2. Required security measures include both Technical and Administrative security.

**Information Security in Healthcare**

Swedish healthcare is currently undergoing extensive changes. It is, to some extent, moving out from the hospitals and is instead being carried out in other forms and locations. Patients with complex care needs can, for instance, obtain extensive care activities in their homes. They have contact with several different healthcare providers, both within municipalities and county councils. These changes increase the requirements for secure communication and cooperation between several different organizations and authorities.

Proper functions controlling unauthorized access to patient information are still missing when IT-systems are extended to more and more users. The
Data Inspection Board declares in its report that in practice county councils have little or no control of who has access to information about specific patients [7]. When using an open authorization, e.g. the logging model, additional and stronger security measures, such as regular and systematic follow-up routines of logs, are required. The Data Inspection Board [7] also claims that “thresholds” should exist in the systems in order to force the users to make active choices when accessing sensitive data about a specific patient.

In its report [8] The National Board of Welfare identifies cooperation and information transmission between different healthcare providers as a risk area for patient safety. This not only concerns computerized systems. Instead, all media useful for patient information transmission between different healthcare providers are risk factors. The connection between the systems and the use of different media does not yet work satisfactorily. Furthermore, the board claims that the healthcare providers must offer systematic measures in order to achieve sufficient routines for patient information exchange [8].

The demands mentioned above are not unique for Swedish healthcare compared to other countries. Even if traditions and legal aspects differ between countries, the main problems are the same. Strong authentications, derived services as authorisation, access controls, accountability, integrity and confidentiality are impertunate demands to achieve [9], [10], [11], [12], [13].

In a distributed healthcare domain, there is also a particular need for a process-oriented approach [14]. In this case study, the patient process was in focus since it is expanding beyond the boundaries of one organization, and consequently leads to patient information being available to additional healthcare providers as well. There is a need for better awareness, improved procedures, improved software, and a more centralised approach and systems management [15].

The main purpose of information security in healthcare is to achieve two important aims. The first is to achieve a high level of patient safety, i.e. to provide patients with the opportunities for the best care with the right information at the right time. The other aim is to achieve a high level of patient privacy; i.e. to protect sensitive patient information being distributed

15 Open authorization refers to an extensive use of authorization implying that various healthcare roles and organizations have access to information without any specific restrictions in the authorization control systems.
to unauthorized persons. Achieving both these aims simultaneously is
difficult. Often either one or the other aim is compromised. For that reason,
a balance between these aims is necessary when the work of information
security within healthcare is discussed [2].

In order to relate the two main aims to the characteristics of information
security, we associate patient safety more to availability and integrity, while
patient privacy is related more to confidentiality and accountability. These
relation boundaries are not static, but depend on each other. In the result
section, the relationship between patient safety/patient privacy and the
information security characteristics are presented together with the results
from the investigation.

The Case Study
The study has been constructed as a small field study with 5 interviews. This
chapter introduces the respondents and approach used.

Aim of the study
The aims of the case study were twofold: to firstly investigate how healthcare
business management\(^ {16}\) perceive current information security from their
holistic perspective; and secondly, to explore their view of information
security when patient information is to be exchanged between different
healthcare providers. The study was performed from a national Swedish
perspective.

The investigation focused on three different groups of questions:
What main problems and needs, alternatively positive effects of information
security, exist in healthcare from a national perspective?
What problems and needs, alternatively positive effects, exist when patient
information is being exchanged between different healthcare providers?
How can the present balance between patient safety and patient privacy be
recognised, and what tendency can be discerned for the future?

Case study respondents
Two governmental institutions (The National Board of Health and Welfare
and The Data Inspection Board) and one special interest organization

\(^{16}\) Healthcare business management refers to governments/organisations of interests with a
national responsibility for healthcare and information security responsible actors within
regions and county councils.
(Carelink) were chosen. Furthermore, two information security managers were selected from two of the largest regions and county councils in Sweden. The National Board of Health and Welfare is the Swedish national expert and supervisory authority for the social services, public health, infectious diseases prevention and the health services. The Board seeks to ensure that efforts in these areas are of good quality and are distributed according to need [16]. The Data Inspection Board is a public authority and their task is to protect the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology [17]. Carelink is a member organization for Swedish county councils, municipalities and private healthcare providers. Through this cooperation Carelink contributes to the development of IT within Swedish health and welfare [18]. These three authorities/organizations were chosen since the interviewed persons representing them are known for their knowledge and experience of Swedish healthcare. Two persons from The National Board of Health and Welfare were interviewed together. One is a technical person responsible for the technical security issues in healthcare, and the other is a legal expert with focus on security aspects in healthcare. They are both involved in several national healthcare projects. In a similar manner, two persons were interviewed from the Data Inspection Board. One of them is involved in the Board’s regular inspections concerning the healthcare sector. The other is a legal expert with focus on security aspects in healthcare. This person is also involved in national projects with a focus on healthcare, and holds a position as information security manager. No one else in the organization has his kind of information security knowledge. The choice of the two information security managers was based on their broad knowledge in the area of information security within their region and county council respectively. Both hold a position as information security managers in the organizations and have the best knowledge concerning these issues in the organization respectively. The region was chosen because it is one of the largest regions in Sweden and previous research has been done therein. The county council was chosen because it is in the front line in the development of IT support and future commitments to IT in healthcare.

It should not be assumed that these interviewed persons can provide a total picture of the Swedish conditions concerning the observed area. But, it should be noted that these selected individuals have such experiences and knowledge that they can present an adequate clear picture about the status of the nation’s standpoint in the area and from the results, draw relevant conclusions.

**Approach**

The study was conducted by semi-structured interviews, i.e. the interviews were based on a number of main questions. These questions often generated new questions, and the interview was more of a discussion or conversation between the interviewer and the interviewee [19]. The basis for the questions has been the Info Sec model. From this model, questions were constructed
about information security partly from a holistic view of healthcare, partly concerning the exchange of patient information between different healthcare providers, and partly the balance between the need of availability of patient information and the protection of patient privacy.

The interviews were performed during a period of two working months and were recorded and transcribed. Afterwards, the transcriptions were sent to the interviewed persons to be read and commented on. The answers were analysed with the help of structuring and categorising them in a table, and then according to the Info Sec model in order to visualise the existing problems and needs, Figure 2.

Nine questions numbered from 1 to 9 were asked. The first question is subdivided into four parts, 1a to 1d. The five interviews were noted as A – E. The answers from the first question and interview organization A have the notation A1a, A1b and so on. All answers are structured in a similar manner.

**Results**

This chapter presents a summary of the results from the three main question areas stated in the applied case study.

**Problems and Needs**

The answers from the questions 1, 3, 4, 6, 7 and 8 concerning problems and needs have been classified and visualised into the Info Sec in Figure 2. Single numbers imply that all the interviewed persons have answers related to the same area.

According to the structure of the questions asked during the interviews, general problems and needs were addressed first, before the specific questions regarding security during patient information exchange. We followed this structure when accounting for the results.
Technical security problems primarily concern vulnerability of communication networks. These networks often lack both functionality and availability. One respondent mentioned the need for wireless networks, while also referring to their potential security problems.

"There is no control on what kind of wireless networks they have and so on. Very much is built upon own initiatives at a specific ward, where someone has installed a wireless network and the IT-unit does not even know of its existence." (respondent B)

There are also insufficient tools for log management, deficient techniques for access levels and authentication. Physical security problems primarily concern theft of equipment. None of the interviewed persons claimed that patient information had ever been stolen. However, one of them indicated that patient information can be lost due to insufficient or the lack of back-up routines. The interviewed persons consistently consider administrative security characteristics as a main problem area in information security in healthcare. Three out of five answers claimed deficiencies of availability of patient information as the main problem source. Other administrative security problems are the absence of information security policies and regulations, incomplete working routines, insufficient education and deficient compliance and follow up routines.

"We have done 40 risk analyses now and they show that mostly there are deficiencies concerning organizational issues and unclear responsible issues" (respondent D)

In technical information security, increased availability of patient information brings a need for new and improved authorization techniques. To keep patient integrity at an appropriate level, authority must be provided that depends on the healthcare actors’ need for patient information. Each healthcare provider also has its own information system for keeping patient information, and sometimes even different such systems in its own
organization. These are not connected, since they are old legacy systems that are not technically possible to integrate. Administrative security is, not surprisingly, regarded as the main problem also when exchanging patient information between different caregivers. Imprecise regulations were emphasized, but the need for common terms and concepts was also highlighted. A key problem is the necessity of dealing with different actors and their respective responsibility for the patients. Each actor takes on responsibility while the patient is with him or her, but there is no clear responsibility when the patient is being transferred to another actor. There is a need for one person to be primarily responsible for the entire patient process, taking the good of the patient as the primary concern (also highlighted in a study by Åhlfeldt and Söderström, [20]). In addition, there is no clear and identified business-level process, which was indicated by several of the respondents.

Some aspects that concern both technical and administrative security were also mentioned. One example is that the healthcare sector must raise its competence level for how to formulate and put forward requirements for information security. All actors must know what they want and be able to formulate it. This requires both organizational routines and education of staff, as well as technical insight. Furthermore, more risk analyses and regulations are needed, which should support the processes and define how much patient information is really needed. Consequently, the need of many-to-many relation concerning availability of patient information may not be necessary. Such analyses and regulations may concern both technical and administrative aspects.

The respondents were also asked to look into the future and comment on possible security problems lying ahead, given a situation when the availability of patient information is improved. Once again, the administrative security problems dominated, for example, that vulnerability will increase and patient integrity risks being reduced. The volume of information is ever increasing, and one respondent therefore fears that healthcare will never get away from its weakest link in the security chain – the individual him-/herself. Interestingly, one respondent showed great faith in legislation, when saying,

“the legalization and regulations will be reviewed in such a way that with a proper complied legalization the security will in the future be fulfilled” (respondent B).

This would imply that legislation will include all aspects of information security, including the informal parts, for instance, individual aspects such as user awareness.

Positive Aspects
Answers from question 2 concerning the existing positive aspects are presented in Figure 3. Concerning question 5, positives aspects in the future when patient information is going to be exchanged, the answers were at such
an abstract level that it could not be classified specifically in the information security model. This is interesting since if we can achieve a good level of information security in the future, then security issues can be what they are meant to be; support for the whole business. The answers from question 5 are presented in the text below.

This section follows the same structure as the previous one in terms of first presenting the results in the Figure 3, addressing general positive aspects, before going into the specifics concerning the exchange of patient information.

![Figure 3. Results from question 2 concerning the positive aspects](image)

It is worth noting that one respondent took the discussion up one level and argued from a society perspective. The respondent claimed that since society has changed its perception of the importance of information security, this view brings positive implications for the healthcare sector as a whole. Much remains to be done and work is ongoing, but even small improvement steps increase the gain of security considerably. There are also unifying projects to develop common standards and regulations. One such example is the ongoing Commission of Inquiry on Patient Information in Sweden [21].

The results show positive aspects in the administrative security area, for instance, having improved the number of risk analyzes, increased the common view on security requirements. Furthermore, the results show positive aspects to achieving confidentiality and accountability even if there is still a lot of work to do in this area.

A common positive technical aspect from the respondents was their positive attitude to having patient information computer based compared with the paper based patient records.

The need for patient information exchange between the healthcare providers has clear positive aspects, even though the answers are stated at a rather abstract level. Care flows (the whole of the patient process) will be more efficient, and the quality of care and patient safety will be improved. Patients
also stand a better chance of recovering earlier than expected, which implies an improved quality of care. These improvements in efficiency are very important from a national perspective, both in terms of quality, and cost savings. Yet another positive aspect is the possibility of using new technology developments to obtain help from experts in other countries, for example during operations and when providing care from a distance. Thus, when patient information availability increases, it is also possible to increase the availability of expertise input to help care for the patient.

**Patient safety and/or patient privacy?**

Answers from question 9 are classified to the items patient safety and patient privacy. The upper part of the Info Sec model has been extended with the objects patient safety and patient privacy; and relates them to the four characteristics of information security, cf. Figure 4.

The results from question 9 show how the aims, patient safety and patient privacy, often contradict one another. However, the results also show a desire to balance them. The two concepts were debated and viewed differently by the interviewed persons, when asked about the current state of the relationship between them. Two respondents claim that the current focus is patient privacy, since legislation focuses on protecting this very issue. Sometimes, patient privacy legislation is so strict it almost hinders patient safety. Two respondents claimed there should not be a polarisation between the two aims, but that privacy is a part of safety. The fifth respondent considers that patient safety dominates the practise of healthcare, while patient privacy dominates legislation.

Concerning the desired state of the relationship between patient privacy and patient safety, three of the interviewed persons stated the necessity of achieving a balance between the two. It should be possible to achieve a high level of patient safety as well as achieving a good level of patient privacy. One respondent expressed a desire to unite the two aims into one, and not to polarise them. The final respondent wanted the focus to be on patient safety, even though patient privacy should be protected as well. The question here is if all respondents actually mean the same thing when discussing the

![Figure 4. Result from question 9 concerning the balance between patient safety and patient privacy](image-url)
issue. In order to achieve a balance between the two concepts, they must be clustered and complement each other.

For future developments, two respondents claim that there will be a balance between privacy and safety. The other three respondents stated that the focus will change depending on the healthcare sector requirements on improved availability of information. This requirement will change the focus to patient safety with the risk of decreasing the roll of patient privacy.

Discussion and Conclusion
Since society as a whole pays greater attention to information security, it becomes more and more important in healthcare as well. However, there are still clear deficiencies. Our case study shows deficiencies primarily in administrative security. For example, clear regulations are missing, both legally and organizationally. These deficiencies seem to be more obvious when looking at the need for cross border patient information exchange between several healthcare organisations. However, the positive effects of such an opportunity are great enough for the healthcare sector to proceed in that direction, not the least with respect to available resources but also to increase the quality of care. However, the technical problems and needs should not be neglected. It is remarkable that in spite of the strong and rapid developments in this area, technical deficiencies still remain. Sufficient secure authorisation and authentication techniques exist in the market place, if the willingness to implement them is strong enough. Furthermore, techniques for managing communication networks, for instance, for checking logs, also exist.

Our study shows apprehensions from some of the respondents that patient privacy will be set aside in the need of making patient information available to more healthcare providers. The openness of availability depends on the difficulty of creating and implementing adequate technical solutions for the sufficient level of access techniques. Quoting one respondent:

“increasing availability to patient information could also imply that patients do not search for care depending on that they don’t want to have their information available to everyone … that the healthcare personnel are not willing to make complete notes in the records because they are afraid of writing too much since so many other people can read it … this is what people have contacted us about” (respondent B)

The quote shows an interesting point, that a technically increased availability may imply a decrease in the willingness to make necessary notes in the documentation.

Table 1 presents needed security measures for the future, as a summary of the information security needs according to our respondents.
Table 1 Security needs

<table>
<thead>
<tr>
<th>Administrative security</th>
<th>Technical security</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Clear regulations, both legally and from the healthcare sector itself.</td>
<td></td>
</tr>
<tr>
<td>- Focus on risk management</td>
<td></td>
</tr>
<tr>
<td>- Continuous working with strategies and policies</td>
<td></td>
</tr>
<tr>
<td>- Awareness</td>
<td></td>
</tr>
<tr>
<td>- Communication and dialogs between actors and individuals</td>
<td></td>
</tr>
<tr>
<td>- The healthcare business must take their responsibility</td>
<td></td>
</tr>
<tr>
<td>- Survey the healthcare business processes</td>
<td></td>
</tr>
<tr>
<td>- Improve the technical solutions for authorization and authentication</td>
<td></td>
</tr>
<tr>
<td>- Logging management</td>
<td></td>
</tr>
</tbody>
</table>

Our respondents posed one common requirement, that a holistic view of the whole area concerning patient information exchange between different healthcare actors is needed. Politicians, legalisation and the healthcare sector must all take on the responsibility here. Healthcare processes have to be analysed in order to obtain both good information flow and protection. Supplementary innovations of technical solutions for logging management, access control and authentication for the healthcare sector are needed as well. Furthermore, it is of great importance for the healthcare business to obtain sufficient follow up routines for compliance and education of users in order to achieve a high level of security awareness in the healthcare business. The investigation also confirms the need of more research in the area.

References


Rose-Mharie Åhlfeldt and Eva Söderström

Abstract. In healthcare, the right information at the right time is a necessity in order to provide the best possible care for a patient. Patient information must also be protected from unauthorized access in order to protect patient privacy. Furthermore, patients visit more than one healthcare provider, which implies the need for cross-border healthcare and a focus on the patient process. Different countries are at different stages of development with regard to information security problems and needs in healthcare, and this paper focuses on two of them. A small case study of nine interviews was conducted to collect data from the UK (mainly England). The results were compared to a similar study in Sweden and show that the UK is more focused on confidentiality issues while Sweden is more concerned about the availability to patient information. Consequently, the focuses on patient safety and patient privacy differ between these two countries.

Keywords. Information security, healthcare informatics, patient safety, patient privacy.

1 Introduction

Information security has always been an important issue in the healthcare sector, in order to ensure that patient information is correct as well as available when needed. In other words, that the right information is available at the right time. Furthermore, patient information must be protected from unauthorized access in order to protect patient privacy. The computerization of patient records has been a necessary step in order to achieve these important concepts. However, since the focus has been on technology, the problems and risks of the management of patient information have not been addressed. In a world where society, organizations and individuals are changing rapidly, the advancement of reality is thus often hard to handle. Nowadays, patients can visit not only one healthcare provider, but an illness can include contact with different types of such providers. There is an obvious need for cross-border healthcare, which consequently includes the cross-border transfer of patient information. Different countries are at different stages in their development and management of cross-border patient information. Some countries are aiming to implement one record for each patient, while others are attempting to integrate different electronic healthcare records (EHR) in order to make important patient information

17 A version of this paper is submitted and has an early accept to the Health Informatics Journal.
available. In addition, the countries can also differ in their approaches towards sufficient protection of patient information.

The aim of this paper is to identify problems and needs of information security in a distributed healthcare domain. We do so by, firstly, presenting the results from a case study applied to healthcare in England, where different types of healthcare providers were examined: hospitals, general practitioners (GPs) and home visitor units. Furthermore, different roles from each healthcare provider were included: managers, system administrators, and healthcare staff. In addition, an information security model was used to achieve a broad perspective. The results from the study were subsequently compared to a similar study in Sweden (see for example: Åhlfeldt, 2002; Åhlfeldt and Ask 2004; Åhlfeldt and Nohlberg 2005 and Åhlfeldt, 2006). The contribution from the study and the comparison constitutes a comprehensive view of information security. This is necessary to be able to prepare for and alleviate problems and needs in the future, when transfer of patient information between different healthcare providers becomes more common.

The paper is structured as follows; Section 2 presents a background of existing problems with regard to the management of patient information when it is exchanged between different healthcare organizations. The chapter also includes a description of the patient process and its way through different healthcare organizations, and illustrates the lack of information following the patient through his/her care chain. While Section 3 provides the research approach, Section 4 presents the results of the study. In Section 5 the results are compared to the Swedish study and finally, Section 6 includes a summary of the results, as well as a discussion of future work.

2 Background

The healthcare sector has, more or less, always faced great challenges since it operates in a changing and demanding society. This applies especially to the past decades, when the information society evolved, and the age of computerization began. Nevertheless, the computerization of patient records in healthcare has taken a long time to implement. One reason among others is that patient information is sensitive and thus must be managed securely. Nowadays, the demands on healthcare have increased due to patients being able to move around more and needing help irrespective of where they are located and when they become ill. Furthermore, citizens in developed countries have a longer life span, due to higher living standards and healthcare. This raises new demands on evolved resources for healthcare. IT can be used to support information management in addressing these new requirements. However, its slow implementation has meant that many healthcare units still keep patient record systems that do not communicate with each other. As a consequence, transferring patient information between
different healthcare providers is problematic. Many patients also suffer from several diagnoses (multi-sick patients), and need contact with a number of healthcare providers. The problems of this situation include that there is no holistic view of the illness in the patient information and no one is responsible for the patients’ whole care process. This patient process constitutes the care chain a patient follows throughout all the phases of the disease, whether care is provided by one or by several healthcare actors.

In Sweden, different projects have started to reach a solution concerning how patient information should be transferred across healthcare borders in a straightforward and secure way. A National Strategy for IT in Healthcare (SKR 2005/06: 139, 2006) has been established, which states that Sweden will create an infrastructure for information as well as communication. The information infrastructure aims to establish a common view of terms and concepts in order to help the healthcare sector with the kinds of concepts to use. The communication infrastructure aims to technically enable the exchange of patient information between different healthcare organizations. In addition, the IT strategy aims to synchronize healthcare sector legislation to avoid the contradiction that exists today. An overview of various acts related to healthcare will be established, compiling those dealing with new requirements and techniques (SOU, 2006:82). Otherwise, it is the responsibility of the county councils and municipalities to achieve integrated systems for exchanging patient information. Furthermore, a common project titled “National Patient Overview” (Carelink, 2007), which is under development, aims to establish a common structure for the most important patient information needed in cross-border healthcare, for example, information about drugs, allergies and so on (Carelink, 2007).

The UK has more or less the same problems as Sweden, but to a greater extent. The healthcare sector in England, for example, has over 5000 computer systems of varying quality and age. It is currently not possible to nationally transfer patient information efficiently, securely and confidentially from one National Health Service (NHS, 2007a) organization to another. England has over 50 million patients and over 500 000 employees in the healthcare sector. The country’s strategy to address the problems is somewhat different compared to Sweden. England will implement the National Program for IT (NPfIT), an initiative from the NHS towards an electronic care record for patients and towards connecting 30 000 GPs to 300 hospitals. The vision is manifold (NHS, 2007b):

• more choice and control for patients over their health and care
• a health service designed around the patient
• modern, integrated IT-systems, throughout the NHS, connecting over 100,000 doctors, 380,000 nurses and 50,000 other healthcare professionals;
• secure, up-to-date, accurate information to all care providers for diagnosis, treatment and care of the patient;
• easier access to their own health information for patients; and
According to Connecting for Health, this is the world's largest civil IT program (Ferrar, 2006). The aim is to provide secure and audited access to records by authorized healthcare professionals (NHS, 2007b). NPfIT includes different deliverables, of which the NHS Care Record Services (NHS CRS) is one. The project has been heavily criticized, mainly for inadequate attention to security and patient privacy (Wikipedia, 2007).

According to the NHS (2007b), patient information will be secured by allowing only authorized NHS professionals involved in a patient's care to access his/her records. Furthermore, access will be on a “need to know” basis according to job role, and patient information will only be shared in the interest of patient care. The NHS also claims that an audit trail ascertaining where, when and by whom patient records were accessed will help to assure confidentiality.

There is hence a vision, in both Sweden and England, of achieving a seamless healthcare sector through the use of IT. However a vision is one thing, making it work in practice is something entirely different. The questions that must be asked are; how well established is information security concerning patient information today, and what is needed in the future to realize the vision?

Previous research in Sweden has shown considerable deficiencies in the management of patient information (Åhlfeldt, 2006). There are shortcomings in technical security concerning authentication techniques, access control systems, unstable communication networks and insecure communication equipment. But the most significant deficiencies reside in administrative security, for instance, in terms of a lack of routines, no information security policies, lack of education, low security awareness of the users, and so on. These problems are so extensive, that simply introducing new technology will not improve the situation, even if the vision is commenable and the work is proceeding in the right direction.

In order to compare the problems of Sweden and UK in this context, a study was conducted to identify how different healthcare providers in the NHS manage information security concerning patient information in practice. Furthermore, the results from this study were compared to those of the previous Swedish study (see Section 5).

3 The Field Study Approach
The qualitative field study was conducted in collaboration with the EU-sponsored Network of Excellence “INTEROP”. INTEROP provided contacts with a university in the southeast of England, the area in which the study was conducted at the end of 2006. Three types of healthcare
professionals, comprising managers, nurses and system administrators, were interviewed. In addition, they all represented different NHS organizations; hospitals, GPs, and a representative (a security manager) from NPfIT, NHS. A total of nine deep interviews with four managers, three nurses and two system administrators were carried out (see Table 1).

Table 1. The involved healthcare organizations and the roles of the interviewed persons.

<table>
<thead>
<tr>
<th></th>
<th>Manager</th>
<th>System Adm</th>
<th>Nurse</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hospital</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>GP</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>NHS</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The interview questions were mainly derived from the Swedish study, which had a similar approach (see Åhlfeldt, 2006). These in turn were based on general advice and guidance from the Swedish Data Inspection Board (DIB, 1998; 2002). The Swedish DIB is a supervisory authority aiming to protect personal data from being revealed. Some questions were also based on the international information security standard ISO/IEC 17799 (ISO/IEC, 2000), and focused on system and network security issues therein.

The questions were semistructured, meaning, for example, that one main question was asked initially to start the discussion. Depending on the answer, the discussion stimulated further and deeper questions in order to achieve an overview of the context. Each interview, which lasted between 1.5 and 2 hours, was recorded, transcribed, and analyzed by coding the answers and writing them into a matrix.

The information security model (InfoSec) was used to visualize the results. This model combines four common characteristics of information security: availability, confidentiality, integrity and accountability; with a model for security measures required to achieve the characteristics. The latest version of the model was presented in the Handbook of Terminology by the Swedish Institute for Standardization (SIS) (SIS, 2003). The InfoSec model was used in the Swedish study to visualize problems and needs concerning patient information transfer in a distributed healthcare domain (Åhlfeldt, 2006). Hence, InfoSec facilitated the comparison between the Swedish and English results.

4 Results

The results are structured according to the main question used to initiate the discussion, as described in Chapter 3. Section 4.1 presents questions 1-12 concerning problems and needs in the information security area and these questions are compiled in section 4.2. Included in section 4.3, is question 13 concerning NPfIT and section 4.4 presents the answers to question 14, which are compiled in section 4.5.
4.1 Problems and Needs Concerning Information Security in Healthcare

4.1.1 Education
In the UK, NHS numbers are now used to identify the patients. The number is given to the citizen at birth. However, NHS numbers are quite unknown to most people in the UK, and they are not easily remembered or used when identifying the patients. Instead, the healthcare staff uses such identifiers as name, birthday and address. Almost all the interviewed persons admitted that errors in patient identification have been occurred due to deficient verification techniques. Only one said this could probably happen but did not think it had in the own care unit.

4.1.2 Strategies to Ensure Information Requirements by the Directive 95/46/EC (Data Protection Act, 1998)
All the interviewees were very conscious of the Data Protection Act. Furthermore, they also had some kind of educational program to inform and update the staff on the Act’s context and news. One unit did so on a mandatory basis. According to another of the managers, “They are very, very, very conscious of data protection”.

4.1.3 Distribution of Security Information
Most of the security information dealt with the Data Protection Act and confidentiality, while it was more difficult to obtain other types of security information. Nearly all of the interviewees were unaware of other security types, but assumed they exist and were available on the Intranet. The Intranet also seems to be the way information security is distributed within the organizations.

4.1.4 Managing Protection of Unauthorized Access – Authentication
The most commonly used authentication technique, for example, in all local systems, is the password. Although they have smart cards in the national system, these are only used it in the booking system, so far (“Chose and Book”). Home visitors have not yet computerized their patient records, which implies that the physical security protection of the records seems to be regarded as more important. According to the interviewed home visitor, there are major deficiencies in the management of the physical security. Although staff use a pin-code to lock the doors, this is badly handled, for example, the pin-code can be revealed to others, and doors have been left open, because it is difficult to remember the pin-code. Some of the managers also state that humans are a weak point. “I don’t think the staff realizes how quite important it is.” or “It is as good as it can be, but human behavior will always be a weak point”.

4.1.5 Encryption and Signing
None of the managers knew if the patient information in the databases was encrypted. One said it is in the national system, but probably not in the local
ones. The hospital system administrator said that the information is not encrypted, while the GP system administrator thinks it is, but did not know.

According to the hospital system administrator, signing is accomplished with the help of passwords in the systems, while at the GPs, it is handled with the help of the login-process. Smart cards are used in the national system, otherwise passwords are the most common signing technique.

4.1.6 Levels of Access Profiles

In the local systems, it seems the access levels are rarely used even if the systems allow that kind of function. It is only at the GPs that these kinds of access levels have been implemented in the local system, which are then integrated with the national one. Otherwise, all the actors have access to all the patient information. According to the hospital system administrator, access control in the national system is role-based. How it works still depends on the respective allotment of each unit’s system administrator. Since there is no specific policy for this issue, it is mainly responsibility of the administrators to decide how the levels of access should be implemented. Opinions differ whether this is acceptable or not. Many managers declared that the staff works closely together, and it is therefore important that everyone involved in the patient’s care has access to the information. Several nurses stated that other actors, such as receptionists, do not need any medical information concerning the patients, and consequently, should not have access to that information. The information should therefore be clearly divided into different access levels. There are clear deficiencies in the manual system as exemplified by the interviewed home visitor: “The receptionist shouldn’t see the notes but seems to know everything about the patients”.

4.1.7 Networks

In this area of England, the NHS-net, which is an infrastructure included in NPfIT, has already been implemented. This is a unique network separated from the Internet and everything, including e-mail, goes through it. It is known that e-mail is sometimes used to transfer patient information, even if this is not allowed. Remote connections to the patient record system can also be made, although this is not part of the NHS-net. The system administrators are hesitant about how many doctors really use this function. No wireless networks are used according to the system administrators.

4.1.8 Follow up Routines and Monitoring System Access Use

Although there is no prescribed information security policy, everyone has a kind of Data Protection policy or the like. There are some national standards for NPfIT, which are adhered to in the implementation process. Follow up actions of policies or other security routines are rare, but can occur. When it does, the follow up is done as a hazard activity or in response to suspicions that something has happened. Although some audit trails are made, these also occur as a hazard activity. No follow up activities are carried out on a
regular basis. According to one manager and the system administrators, there are no resources for these kinds of activities.

According to the system administrators, there is no intrusion detection system (IDS), and logs are not checked on a regular basis. Instead, the new system with smart cards is trusted, and there is complete confidence in this kind of protection.

4.1.9 Educational Program of Information Security

The two hospitals use different approaches to educational programs of information security. At the first hospital, the manager stated that they only have security education when the systems are changed. The nurses at the other hospital claim they are provided with continuous information about security in a broad sense, including physical security. The GPs seem to share a common view of security education, even if the time intervals between their efforts vary. Security education can be organized on yearly basis, when new systems are introduced, or as a part of regular meetings. However, the nurse working as a home care visitor said that they do not have much security education at all: “We have incidents and we are aware but we don’t do anything about it”.

4.1.10 Log Management

Only one of the managers (GP) claimed to possess knowledge about the logging process, what they log, and that logs can be checked when needed. The other managers have no knowledge about logs, what they include, or in what way they are checked and instead, they claim this is not done at all.

4.1.11 Technical Security Measures and Routines

The physical security can be assumed to be sufficient, even if older hospitals have deficiencies compared to the newer ones. In the latter case, hospital security is already dealt with in the designing phase in order to ensure protection from intrusion, fire, and so on. The hospitals’ sensitive equipment must also be protected. At the GPs, the fire system, alarm systems and emergency items are checked every week. In addition, the access to the building is also checked and recorded by keeping staff lists and building plans. Furthermore, the hospitals have regular updates of their virus protection. At the GPs, the system administrator thinks this is an automatic process, but is unsure. Although mobile equipment is used in the hospitals, it is the person managing the security who decides if mobile equipment should be used, but no specific regulations for mobile equipment exist.

4.1.12 Distribution of Patient Information

The transfer of patient information between different healthcare providers is done by regular mail, fax and internal mail systems or by the patient him/herself. Some patient information is sent via “Recording Delivery” (Assurance), and sometimes by e-mail. Furthermore, some information is now being sent via the national system, but so far only on a small scale. The
interviewees do see the possibility of improving the distribution of patient information to other healthcare units with the help of the national system. However, all interviewees consider that the security of transferring patient information is deficient. They assume that the right person is on the receiving end of the fax, or that the person delivering the internal mail has not seen the information, but they do not really know. There are no specified routines for this matter, neither at the GPs nor at the hospitals. At the home visitors centre, the staff often transfer the information to the GP or the hospital themselves, since they have a close working relationship. In other situations, they use “Recording Delivery”.

In “Chose and Book”, the hospital does not have access to patient information until the patient has made an actual appointment, and the letter has been sent by the GP. Only then is the information transferred and the hospital can access it in the system.

4.2 Interview Result Compilation Questions 1-12
This section compiles the results from Section 4.1, the main questions 1 – 12, classifies them in terms of the information security model and visualizes them in the information security model (cf. Figure 1).

1. Managing patient identity – **Administrative security**
2. Strategies to ensure information requirements by the Directive 95/46/EC (Data Protection Act) - Good, no specific problems
3. Distribution of security information – **IT-Security**
4. Managing protection of unauthorized access
   a. Weak authentication in the local system – only passwords – **Computer Security**
   b. Weak physical protection in the manual system, but good level at the GPs. - **Physical Security**
   c. Human behavior – **Administrative Security**
5. Encryption and signing – **Computer Security**
6. Levels of access profiles- **Computer Security**
7. Networks
   Remote access – **Communication Security**
8. Follow up – routines and monitoring system access use.
   a. No prescribed information security policies apart from the national standards and those of the Data Protection Act – **Administrative Security**
   b. Poor follow-up of the security work - **Administrative Security**
   c. No regular audits. – **IT Security**
   d. No IDS – **Communication Security**
9. Education program of information security
   - Generally good education concerning the Data Protection Act and confidentiality. Information Security education in a broad sense is lacking. Very weak education at the home visitors centre – **Administrative Security**
10. Log management
   - Also in the national system it seems logging management does not function. They trust the “need to know”- model very much -

   **Administrative Security**

11. Technical security measures and routines
   - Mobile equipment – **IT Security**

12. Distribution of patient information
   - Fax, mail, - **Communication Security**

![Figure 1. Visualizing the problems from the first twelve areas. No 2 is excluded since no specific problems were identified.](image)

**4.3 National Program for IT**

The interviewed persons’ opinions about the new national system, NPfIT, were varied, for example, the managers said: “Fantastic. You won’t have a lot of notes floating around. You will have all the notes in the system. I think it should be wonderful”. “Excellent idea, but very poor introduction” (Manager GP1). “I think it is a disaster. Anything that has a top-down approach will always cost a lot more money and never works as well as a bottom-up approach, because systems work best when they are tailored around where people work” (Manager GP2). “If you spend a million pounds on a system, you have to spend close of that on training. You can’t put in a million pounds into a system where 50 pounds went on training, it doesn’t work” (Manager GP2). The system administrators also had different points of view: “A lot has been put on hospitals to achieve in a very short space of time. It would have been better if the system had been implemented in more than one piece to achieve it nationally” (System admin hospital). “Good for the patients. According to the exchange of information it is excellent and for the working staff it is good” (System admin GP).

The answers also differ with regard to how information security will be improved in the new national system. One manager believes that the support of different access levels for the staff will be an improvement. The information will not float around in the office. Another manager says that she will not have her own patient information in the new system for two
reasons: 1) the number of people she believes may be able to view that record; and 2) the lack of a clear definition of what is available to whom. The nurses believe that security will improve compared with the current situation, above all with regard to the levels of access. However, the nurse claims it will not make any difference for some special units at the hospital. The hospital system administrator considers the smart card process and the role-based access will improve the overall security, but that it is administratively overwhelming. The GP system administrator really does not know how security could be further improved in the new system.

The main risks of the new national program are considered to be the structure of a great number of people, the levels of access together with the risk of hacker attacks, a central database and risks concerning new functions that are not adaptable to the healthcare domain, and so on. However, according to the system administrators, delaying the program constitutes the greatest risk, but at the same time they consider that implementation must not proceed too quickly, nor be too ambitious.

4.4 Patient Safety and Patient Privacy
All the interviewed nurses, as well as one manager and one system administrator considered patient safety and patient privacy to be equally important, while two of managers and one system administrator stated that patient safety is more important than patient privacy.

Their opinions differed with regard to how these concepts are emphasized in their daily work. One nurse favored patient safety, while another favored patient privacy, and yet a third believed both should be emphasized. One of the managers asserted that patient privacy is important for the patients, while patient safety is more important for the organization. Another manager favored patient safety, and yet a third said both. The system administrators stated they do not differentiate between the concepts in their daily work. Sometimes privacy is more emphasized, since patient safety is taken for granted, but it is not a subject they discuss. The GP administrator claimed that the concepts cannot be separated.

All the interviewees claimed that the two concepts can be balanced, but not at 100 percent. However, it is something to strive for. If a choice must be made, two of the interviewees said that patient safety should be prioritized because this is the most important aspect for healthcare.

Furthermore, all the interviewees believed that when NPfIT has been implemented, more emphasis will be on privacy from a patient perspective. The motivation was that they all considered patient privacy was being neglected in the National Programme. Hence, from both the organizational and the NHS perspectives, patient safety will be more prioritized than it is today.
4.4 Interview Result Compilation Question 14

This section compiles the results from the main question 14, by visualizing them in Figure 2. The first subquestion (a), concerning the present focus is distributed over the area with a small dominance in patient safety. The second subquestion (b), concerning the optimal situation is dominant in the balance area. The third subquestions (c), concerning where the focus will be in the future, are realistically dominant in the patient privacy area,

![Figure 2. The results from the main question no 14.](image)

5 Discussion and Comparison of the Results with the Swedish study

In this chapter, the results from the studies in Sweden and England are compared and analyzed. The analysis is organized in the categories: Managing patient information, strategies concerning the Data Protection Act, technical security, administrative security, patient record systems, and patient safety and patient privacy.

5.1 Managing Patient Information

The method of identifying patients in England and in the whole of the UK is interesting, but clearly less efficient compared to Swedish conditions. Sweden utilizes a personal number system (social numbers), which allocates every Swedish citizen his/her own unique identification number. It is consequently much easier to be certain that the right patient is being treated. The results show that in England errors in patient identification can occur due to the lack of a unique identifier. However, there can be problems with unique identifiers as well. Incidents have occurred in Sweden where patients’ identification was incorrect, which usually depends on a failure to check the all of the 10 digits (6 + 4) in the personal number (Socialstyrelsen, 2007). The risk with a unique identifier is that it is easier to access information from other systems or databases that are irrelevant to the care situation, since the same identifier is used in every national system. Examples of such systems include the car registry, social insurance register, tax registry and other allowance/funding registries. This is also the reason why many other countries do not use this type of identifier. From a security perspective, it is very important that a person receives the correct, designated care. According
to the interviewees, there have not yet been any serious consequences, although one said that incidents have occurred.

5.2 Strategies concerning the Data Protection Act

One interesting finding was that the interviewees all knew of the Data Protection Act and the importance of confidentiality. None considered themselves ignorant of this Act, and all stated they were very conscious of these issues and had continuous education in order to further improve their knowledge. On the other hand, there were clear shortcomings concerning knowledge about other types of information security characteristics; availability, integrity and accountability. These aspects were not considered as important as confidentiality, which can be deduced from the interpretation of the answers. During the interviews, the interviewer had to clarify several times that information security concerns all four characteristics. Many of the interviewees believed that security and confidentiality were one and the same concept.

5.3 Technical Security

The problems and needs of technical security are similar in England and Sweden (for Swedish results, see Åhlfeldt, 2002; Åhlfeldt and Ask, 2003, Åhlfeldt and Nohlberg 2004): weak authentication techniques, wide access levels, integration problems between different systems, no encryption of sensitive information, weak signing techniques, and so on. In England, they currently have a special situation because they are implementing the new national system NPfIT, while still using the old patient record systems. For obvious reasons, they will not address the technical weaknesses since they are awaiting the new system. However, it should be emphasized that implementing a new system does not automatically solve all the problems. The study shows that although the old local systems have functions that the new one does not have, the new system is still needed. The question must be asked if the users will have to use the inadequate security solutions of the local systems or if the old functions can be integrated with the new system. The NHS-net has already been implemented, which implies that the security levels of communication security have increased considerably. It should be noted, however, that not all information is sent via the NHS-net. Some information is still managed manually to other units. The transfer of information from remote areas is not included either, which must be seen as a major shortcoming since in the long-term it could impact the patient safety if the healthcare staff cannot access patient information from other places than from a specific healthcare unit.

The level of physical security varies. At the new hospital and at GPs, the level of physical security is sufficient. The interviewer was, without any prior knowledge, allowed to participate and observe fire training during the period the interviews were being conducted. On the other hand, the physical security level at the home visitor unit is weak. Although the staff seems to be
aware of the problem, this is primarily a management problem. If we compare the physical security levels to Swedish conditions, England’s level of physical security is higher. Sweden does not have continuous fire training programmes at the GPs in the same way as in England. One reason is that England lives in a state of preparedness, which is different than in Sweden due to the threats of terrorism.

5.4 Administrative Security
Concerning administrative security, there are both similarities and differences between the countries. Both countries experience problems due to the lack of general information security policies and inadequate follow-up of security work. However, England is further advanced in education on security issues in the Data Protection Act and confidentiality. On the other hand, England has deficiencies regarding general education on information security. The security awareness of users is higher in England with regard to confidentiality and physical security, but significantly less in other parts of information security.

5.5 Patient Record Systems
The expectations from the NPfIT program are very high, especially with regard to information security. But the question is if it can solve all the existing problems. The aims and vision of the program which are based on the international standard of information security, ISO/IEC 17799 are impressive. Since this standard originates from England, it is natural to base this kind of gigantic project on the standard, according to a representative from the NHS. Furthermore, there is also the ambition to implement strong authentication techniques, such as smart cards. It is also very interesting that the program will apply a strong authorization “need to know” model as a primary task. Both the NHS and the interviewees really want access levels that only include those, and only those, who are involved with the patients’ care. The drawback of such a model is that it is administratively very overwhelming, and the question must therefore be asked if this is practically viable in a long-term sense. Despite this ambition, the project has received strong criticism concerning the neglect of patient privacy, since the information about all patients is contained in only one database. The criticism comes from actors within healthcare as well as from patients and the general public.

5.6 Patient Safety and Patient Privacy
Eight out of nine interviewees agreed that a balance between patient safety and patient privacy is preferred. However, five out of nine interviewees believe that the emphasis will be on privacy in the future, since the new program does not seriously take privacy aspects into consideration. There is an obvious fear that privacy will be more neglected in England than in Sweden. One reason for the differences is that the UK is a country at war and is therefore subject to obvious threats, not at least of which are those of
terrorism. This implies that the government must implement security measures, such as surveillance cameras in public areas, as well as more access to personal data, in order to guarantee the nation’s safety. One consequence is that ordinary people feel threatened and consequently want to protect their privacy. Sweden has not been at war for several centuries, and Swedish citizens hence trust their government to a greater extent. They trust the government to protect them and are less obviously fearful that their privacy will be neglected, even if there are concerns in that area too.

Another interesting finding is that NPfIT has chosen a “need to know” approach in their program, which clearly states that only those involved in the treatment of a patient will have access to the patient information. This will be achieved with strong authentication techniques such as smart cards. Sweden does not generally have such a strong authentication approach, even if similar recommendations from the government’s point of view exist. Nevertheless, England is more conscious about the risks and wants to protect privacy more than Sweden does, although Sweden has a more liberal view of how to protect privacy and address authentication techniques.

### 6 Summary and Future Work

The aim of this paper, in which different types of healthcare providers were studied, is to identify problems and needs concerning information security in a distributed healthcare domain. We addressed the aim by conducting a study in England and comparing the results to a pre-existing Swedish study, thereby achieving a more holistic, international overview of problems and needs. We present and classify the results according to the information security model, and emphasize the need to relate and analyse the important issues of patient safety and patient privacy to the area of information security. Furthermore, the holistic view of information security is also manifested by emphasizing both technical and administrative aspects of information security.

Based on the analysis in Section 5, the two studies, in Sweden and England respectively, show the following similarities and differences between the countries:

- **Managing patient information**: the UK uses NHS numbers, while Sweden uses personal numbers. In both countries, patients’ identities have been mixed up.
- **Strategies concerning the Data Protection Act**: The UK is more focused on these strategies than Sweden.
- **Technical security**: the UK has implemented NHS-net for all NHS Trusts. In Sweden, Sjunet has only voluntary membership except for county councils. Both countries have weak authentication techniques, wide access levels, system integration problems, and weak signing
techniques. The two communication networks (NHS-net and Sjunet) are similar, but cannot be used for all types of patient information.

- **Administrative security**: The UK has more focus on education concerning confidentiality, and as thus a more heightened awareness of this aspect than Sweden. Both countries lack a general security policy, having inadequate follow up security work routines, and lack in information security awareness.

- **Patient record systems**: the UK solves the system integration problems with a top-down approach – NPfIT, which means the use of one patient record system in the whole of England. Sweden uses a bottom-up approach, in which 21 county councils and regions have different patient record systems. They attempt to solve the problem with an integration platform for general patient information.

- **Patient safety and patient privacy**: the UK emphasizes patient privacy, while Sweden focuses on patient safety.

A future work could be to reconduct this investigation in a couple of years when NPfIT has been implemented. It would be interesting to study if the identified problems and this investigation have been solved or if they still exist, find out what healthcare actors as well as patients think about the privacy aspect. Furthermore, such a future study should also cover if the healthcare sectors of England and Sweden have succeeded with their ambitions to follow the patients in their care process and transfer patient information between different healthcare providers with the aim to obtaining patient safety as well as patient privacy.

**References**


Paper 5: Information Security Problems and Needs in Healthcare: 
A Case study of England vs Sweden
Information Security Problems and Needs in Healthcare: A Case study of Norway and Finland vs Sweden

Rose-Mharie Åhlfeldt and Eva Söderström

Abstract. In healthcare, the right information at the right time is a necessity in order to provide the best possible care for a patient. Patient information must also be protected from unauthorized access in order to protect patient privacy. It is also common for patients to visit more than one healthcare provider, which implies the need for cross-border healthcare and a focus on the patient process. Countries work differently with these issues. This paper is focused on three Scandinavian countries, Norway, Sweden and Finland, and their information security problems and needs in healthcare. Data was collected via case studies, and the results were compared to show both similarities and differences between these countries. Similarities include the too wide availability of patient information, an obvious need for risk analysis, and a tendency to focus more on patient safety than on patient privacy. Patients being involved in their own care, and the approach of exchanging patient information are examples of differences.

Keywords. Information security, healthcare informatics, patient safety, patient privacy.

1 Introduction

Information Technology (IT) in healthcare has the potential to increase the welfare of the citizens as well as improve the efficiency of the healthcare organizations. The demands on the healthcare sector in the Nordic countries come from: an aging population, a need for seamless service processes, an increasing demand of care in the patients’ homes, a demand for more information and participation, etc. [1]. Even if the Nordic countries are at the forefront with regard to the use of IT and the Internet in the society as a whole, the implementation of IT in healthcare has been slow [1]. When IT solutions are applied in healthcare, especially in a distributed fashion, information security is a critical issue [2], [3].

The aim of this paper is to identify similarities and differences concerning the problems and needs of information security in a distributed healthcare domain. The research method used was two minor case studies in Norway and Finland. The results were compared with a previous, similar study in Sweden [4], also incorporating an existing information security model. The contribution is a holistic view of information security, which is necessary when preparing for and

18 A version of this paper will be published in the International Conference Proceedings on Interoperability of Enterprise Software and Application (I-ESA’2008), Berlin, Germany, March 2008.
alleviating problems and needs in the future. In particular, the holistic view is a necessary contribution when patient information is transferred between different healthcare providers.

The paper is structured as follows: Information security and the Info Sec model are presented in Chapter 2, while Chapter 3 introduces the state-of-the-art information security in healthcare. Chapter 4 includes the research approach, and Chapter 5 presents the results of the study. Chapter 6 discusses and compares the results with the Swedish study. A summarizing discussion is given in Chapter 7.

2 Information Security Model

Information security concerns security issues in all kinds of information processing. According to SIS [5], information security is defined as the protection of information assets, and its aim is to maintain confidentiality, integrity, availability and accountability of information. In order to achieve the four characteristics, both technical and administrative security measures are required. Administrative security concerns the management of information security; strategies, policies, risk assessments etc. It includes structured planning and implementation of security work, and concerns the organizational level and thus the organization as a whole. Technical security concerns measures to be taken in order to achieve the overall requirements. It is subdivided into physical security (physical protection of information) and IT security (security for information in technical information systems). IT-security is further divided into computer security (protection of hardware and its contents) and communication security (protection of networks and media used for communication). A visual overview of the characteristics and security measures is presented in an information security model (Figure 1). The model combines the mentioned concepts.

![Information Security Model](image)

With information security in the middle, the four characteristics are at the top, and the security measures are at the bottom. The latter ones are gathered directly from the SIS conceptual classification [5].

192
3 Information Security in Healthcare

Swedish healthcare is currently undergoing extensive changes. It is to some extent moving out of the hospitals and is instead being carried out in other forms and locations. Patients with complex care needs acquire extensive care activities, for instance, in their homes. They have contact with several different healthcare providers, both within municipalities and county councils. These changes increase the requirements for secure communication, as well as cooperation between several different organizations and authorities.

The National Board of Welfare [6] identifies cooperation and information transfer between different healthcare providers as a risk area for patient safety. Computerized systems as well as all media useful for patient information transmission between different healthcare providers constitute risk factors. The Board claims that healthcare providers must offer systematic measures in order to achieve sufficiently secure routines for the exchange of patient information [6].

IT-systems are extended to more and more users, but proper functions that control unauthorized access to patient information are still lacking. The Swedish Data Inspection Board declares in its report that county councils, in practice, have little or no control of who has access to information about specific patients [7]. Depending on the authorization method used, various additional measures and routines may be required to force the users into making active choices when accessing sensitive data about a specific patient.

These demands are not unique for Swedish healthcare. Even if traditions and legal aspects differ between countries, the main problems are the same. Strong authentication, derived services such as authorization, access controls, accountability, integrity and confidentiality are importunate demands to achieve [8], [9], [10]. In a distributed healthcare domain, there is also a particular need for a process-oriented approach [11]. Our research is focused on the patient process, since it expands beyond the boundaries of one organization, and consequently leads to patient information being available to more actors. There is a need for better awareness, improved procedures, improved software, and so on [12].

The main purpose of information security in healthcare is twofold: to achieve a high level of patient safety, i.e. to provide patients with the best care with the right information at the right time; and to achieve a high level of patient privacy; i.e. to protect sensitive patient information from unauthorized access. It is difficult to achieve both aims simultaneously, and one of them is often compromised. Hence, a balance between them is necessary in healthcare [13]. Patient safety is here related to availability and integrity, while patient privacy is related to confidentiality and accountability. We return to the relationship between the two concepts in the results.
4 The Case Studies
The research was constructed as two minor case studies with a total of four interviews.

The aim of the case studies was twofold: to investigate how healthcare management perceives current information security from a holistic perspective, and to explore their view of information security when patient information is exchanged. The studies were conducted at a national level in Norway and Finland. Three groups were in focus: 1) What main problems and needs, alternatively positive effects of information security, exist in healthcare from a national perspective? 2) What problems and needs, alternatively positive effects, exist when patient information is being exchanged between different healthcare providers? 3) How can the present balance between patient safety and patient privacy be recognized and what tendency can be discerned for the future?

From each country, one interest organization (In Norway KITH – The Norwegian Centre for Informatics in Health and Social Care [14], in Finland STAKES – The National Research and Development Centre for Welfare and Health [15]) and one information security manager from a large hospital were selected. The respondents were selected for their good knowledge and experience of Norwegian and Finnish healthcare respectively.

The studies used semi-structured interviews and were based on a set of main questions. Nine questions, derived from the Info Sec model, concern information security from a holistic view, the exchange of patient information between different healthcare providers, as well as the balance between the need for availability of patient information and protecting patient privacy.

The questions are numbered from 1 to 9. The first one is divided into four parts: 1a - 1d. The four respondents were noted as A – D, with A and B from Norway, and C and D from Finland. The answers from A and the first question are hence noted as A1a, A1b and so on in Figure 2. All the answers are structured in a similar manner.

5 Results
This chapter presents a summary of the results from the three main questions stated in the applied case study.

5.1 Problems and Needs
The questions were structured to address general problems and needs first, before the specific questions about security during patient information exchange. We follow this structure when accounting for the results. The answers from the questions 1, 3, 4, 6, 7 and 8 concerning problems and needs have been classified and illustrated into the Info Sec Model in Figure 2.
1a Information Security Problems – spontaneous
Both Norwegian respondents mentioned the problem of unavailable patient information, within as well as across organizations. They also emphasized that only those who need the information should have access to it.

Respondent C identified employees as the weakest link, but that this is difficult to define. There are too many deficiencies concerning, for example, audit logs, regulations for encryption of information inside healthcare provider organizations, and medical doctors being reluctant to ask for consent. Respondent D claimed that the major problem is a lack of knowledge concerning the applications’ security level. Suppliers may have said one thing, but the reality is something else.

1b Information Security problems – administratively
The respondents mentioned that lack of knowledge, human behavior and comprehension are the main administrative problems. There is a lack of resources for information security activities and insufficient routines to meet the security requirements. Furthermore, systems monitoring is also a problem. It is too expensive to have 24-hour monitoring, although this really is necessary.

1c Information Security problems – physical security
“Open” hospitals are a major physical security problem in both Norway and Finland. Although new hospitals in Norway equip their entrances with cameras etc., it is still very easy to enter the wards, where much information is visible, both physically and on screens, according to respondent B.

Hospitals in Finland use group logins to buildings, and computers have been stolen from the central store, according to respondent D. Respondent C pointed out that physical security in small and medium size healthcare centers is not adequate.
1d Information Security problems – IT security
Authentication and access level problems are obvious in both Norway and Finland. Norway has implemented smart cards for the network, but it is an expensive technique with usability problems, such as users forgetting the cards at home, and not bringing them to other computers. Norway also lacks an automatic tool for checking logs, which is unacceptable since the access levels are too wide according to respondent B.

Respondent C claims that their whole password system is not very secure at all. Outsourcing is also a narrow area: “You cannot easily see what you can outsource. You can outsource the technology but you cannot outsource the rest of the responsibility. It has to be included in the contract” (respondent C). Respondent D mentioned problems such as too many uncontrolled output sockets in the systems and external partner access to the systems.

3 Present substantial security problems with cross border healthcare information from a patient process view
In Norway, the information is attached to one organization and almost limited for legal reasons. Technically, systems are hard to integrate, and structured information is difficult to transfer between the systems. According to respondent B, although they can transfer information, this is not allowed according to their legislation. In one region, all healthcare organizations (except municipalities) have the same system, making it easy to transfer information between them.

Finland also has interoperability problems, which are technical in a short-term sense. The main problems are semantic, according to respondent C. Respondent D claims that sending information between hospitals and healthcare centers is a minor problem. Instead, the main problem is serving the systems of the many organizations.

4 and 6 Future substantial security problems with cross border healthcare information from a patient process view and the security measures for solutions
The Norwegian respondents agree on the importance of the technology working and being thought through from the start. Risk analysis is needed for the whole healthcare sector, and consequences should be dealt with. The main problem is the daily work for the ordinary co-operators according to respondent A: “It is important to find a balance”. Responsibility issues are also important for the future, such as: obtained consent, documentation and information duty, and distribution to the research community.

In Finland, respondent C states that the next generation of health record systems will be more consistent and more accessible, but changing IT will take more than one generation. According to respondent C, finding one general definition of merging data is too difficult. Information overflow is another problem: “The medical doctors still have a maximum of 15 minutes for the patient and five minutes for discussion. They do not have time to check all the information” (respondent C). Respondent D also mentioned the problem with a high service level agreement.
To solve these problems, Norwegian respondents suggested supporting as well as presenting tools, improved analysis tools for checking logs, and more education concerning network applications. The Finnish respondents emphasized the need for electronic healthcare information, and respondent C suggested a reorganization of the whole healthcare sector. Furthermore, tools for checking quality will be more common and useful as well as necessary for the healthcare sector in order to improve the quality of care. Respondent D suggested the need for standards and service agreements.

**7 and 8 Future security problems concerning availability of health information and measures for solutions**

Confidentiality aspects are a common risk factor concerning the availability of healthcare information for all respondents. The Norwegians stress that the availability of many patients' health records is too broad, revealing a need to revise authorization allowance. Respondent A pointed out the risk for criminal blackmail, particularly for well-known persons: "At present, we have a peaceful regime both in Norway and Sweden, but in other types of political regimes, our openness can be of great importance and be misused".

The Finnish respondents also worry about how to control access levels, for example: "We have to think about how we control the access to patient information and other data because the access is very wide" (respondent C). The political situation was also considered: "Political situations outside Scandinavia, health and fitness records and of course the access, is controlled by law, but we have seen that a law can be changed in some weeks like in the UK" (respondent C).

The Norwegian respondents suggest the solution of maintaining basic principals concerning privacy and data protection. The access control systems must be improved: "We must implement a “need-to-know-model” even if it is administratively both intensive and expensive" (respondent A); and "We have to do risk analyses in order to set requirements for privacy" (respondent B).

In Finland, respondent D emphasizes that patients must have control over their own records, while respondent C is more focused on technical issues: "New technology must be implemented, for instance the new generation of PKI."

**5.2 Positive Aspects**

This section follows the same structure as the previous one in terms of first presenting the results in Figure 3, addressing general positive aspects, before proceeding with the specifics about the exchange of patient information. The answers from questions 2 and 5 concerning the positives aspects are presented in Figure 3.
2 Present positive aspects of information security in healthcare
In both Norway and Finland, patients are allowed to read their own patient records, implying: “power of citizens” (respondent C). When paper-based records were used, patients did not have this opportunity. The computerization of patient records is the most positive aspect of information security in healthcare according to all the respondents: “More people can have access to information quickly and simultaneously, and depending on IT, we can log everyone who has accessed the record and compared with the paper based system, this is very positive” (respondent B); “People cannot do whatever they want, with IT you have more orderliness” (respondent D).

5 Future positive aspects of information security in healthcare
Future positive aspects will be more or less the same as previously mentioned. Even though improvements are still needed, there is a sense of faith that the healthcare sector will succeed. Information is available for healthcare actors who really need it, both internally and externally. The duty of information is improved and easier to implement with IT than paper-based systems. Hence, IT development must continue in healthcare.

5.3 Patient Safety and/or Patient Privacy
Answers from question 9 are classified according to patient safety and patient privacy regulations. These concepts have extended the upper part of the Info Sec model and become related to the upper four characteristics of information security (Figure 4). The results indicate how patient safety and patient integrity often contradict one another, but also the desire to balance them. Three respondents claim the current focus priority is on patient privacy, since legislation is focused on protecting this issue. One respondent considers that patient safety dominates healthcare, while patient privacy dominates legislation.
All the respondents state the necessity of achieving a balance between the two concepts, even if two of the respondents want it to lean more towards safety. It should be possible to achieve a high level of patient safety and an acceptable level of patient privacy.

Respondents A and D claim that in the future there will be a balance between privacy and safety: “We must try to find the right way. Sometimes we have to focus more on patient safety and sometimes on patient privacy” (respondent A); and “Patient safety is more technically focused and therefore easier to solve. The privacy part is more complex” (respondent D). Respondents B and C state that the focus would move towards patient safety in the future: “Safety and quality is coming and will be measured” (respondent C). Respondent B adds that even if privacy seems to be less in focus at the present time, in the near future, the pendulum will probably swing back.

6 Discussion and Comparison with the Swedish Study

The results from the case studies are now compared to a similar study in Sweden. For details about the Swedish study, we refer to [4]. The analysis is organized according to the categories: information security problems and needs, positive aspects of information security in healthcare, and patient safety and patient privacy.

6.1 Problems and Needs

The three countries have approximately the same social structure. They also basically have the same problems and needs concerning information security in healthcare. With regard to technical security, they share the problems concerning authentication techniques, even if Norway is somewhat further advanced with their smart cards. All three countries also lack authorization techniques and tools for log management. In administrative security, the main problems are: a too wide availability of patient information, incomplete work routines, a lack of security awareness and a lack of risk analyses.

The integration dilemma is also a common problem. Legislation must be adapted to the new requirements, and the responsibilities for patient information must be revised. Thus far, Norway and Finland have implemented more
standards and policies than Sweden, while the Swedish study did identify the need for strategies, policies and standards. In Norway and Finland, patients have the right to access their logs and consequently have more control of their own information. This is currently not possible in Sweden, but the proposed “Data Protection Act” will enable patients to be admitted access to their logs if possible, but they will not have the right to claim them.

6.2 Positive Aspects

All countries agree that the most positive aspect concerning information security in healthcare is the computerization of healthcare records. Security issues still remain, but the positive aspects are clear; information availability for healthcare staff both internally and externally, more efficient care flow, and improved quality of care and patient safety. Norway and Finland emphasize the positive aspect of more power to the patients, but this is – as mentioned – not possible in Sweden.

6.3 Patient Safety and Patient Privacy

Our research shows similarities concerning the balance between patient safety and patient privacy, even though the respondents disagree on which one the present focus is directed. They agree that legislation is focused on privacy, while organizations focus on safety. The Norwegian and Finnish respondents all state the necessity of achieving a balance between the two concepts. The Swedish respondents are divided; three want a balance while two claim the focus should be on patient safety. All the countries claim that in the future the focus will shift to patient safety, while one also mentioned the importance of privacy.

6.4 Comparison Summary

The similarities between the countries concern problems and needs, positive aspects, as well as patient safety versus patient privacy, which is illustrated in Table 1.

<table>
<thead>
<tr>
<th>Category</th>
<th>Similarities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problems and needs</td>
<td>Lack of an authorization techniques (technical security)</td>
</tr>
<tr>
<td></td>
<td>Lack of log management techniques (technical security)</td>
</tr>
<tr>
<td></td>
<td>Too wide availability of patient information (adm. security)</td>
</tr>
<tr>
<td></td>
<td>Incomplete work routines (adm. security)</td>
</tr>
<tr>
<td></td>
<td>Lack of security awareness (adm security)</td>
</tr>
<tr>
<td></td>
<td>Need for risk analyses (adm security)</td>
</tr>
<tr>
<td>Positive aspects</td>
<td>Computerization of healthcare records</td>
</tr>
<tr>
<td>Patient safety and patient privacy</td>
<td>No consensus on the current focus between the countries</td>
</tr>
<tr>
<td></td>
<td>Legislation is focused on privacy while organisations emphasize safety</td>
</tr>
<tr>
<td></td>
<td>Tendency to focus more on safety in the future</td>
</tr>
</tbody>
</table>

The computerization of healthcare records, which is a main issue in all three countries, results in availability of information, better care flow, and improved quality of care. There are also differences, illustrated in Table 2.
Table 2. Differences between the three countries.

<table>
<thead>
<tr>
<th>Differences</th>
<th>Sweden</th>
<th>Norway</th>
<th>Finland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication technique problems</td>
<td>Ongoing pilot project with smart cards</td>
<td>Further advanced with smart cards implementation, e.g. communications networks.</td>
<td>Further advanced with smart cards implementation</td>
</tr>
<tr>
<td>Exchange of patient information</td>
<td>Few standards and policies</td>
<td>More standards and policies</td>
<td>More standards and policies</td>
</tr>
<tr>
<td>Patients’ own access to information</td>
<td>Patients lack the right to access their logs, thus little power to patients</td>
<td>Patients have the right to access their logs, thus more power to patients</td>
<td>Patients have the right to access their logs, thus more power to patients</td>
</tr>
<tr>
<td>Patient privacy and Patient safety</td>
<td>No consensus among respondents</td>
<td>Balance is needed</td>
<td>Balance is needed</td>
</tr>
</tbody>
</table>

The first three rows of the table indicate problems and needs, the third row includes positive aspects, and the fourth concerns the discussion of privacy versus safety. Even though the countries share the problems of authentication techniques, they differ in how far advanced they are addressing them. Information exchange is also, in part, a common dilemma, but here the countries differ as well in how advanced they are in dealing with the issue. Interestingly, Norway and Finland both allow patients to access their logs. The general similarities should allow Sweden to do the same, but as mentioned, this will require legislative changes.

7 Summarizing Discussion

The aim of this paper is to identify problems and needs concerning information security in a distributed healthcare domain. Two minor case studies were conducted in Norway and Finland, and the results were compared to a similar pre-existing Swedish study. Consequently, this research provides a more holistic, international overview. The results were presented and classified according to the Info Sec model. Furthermore, the need to relate and analyze patient safety and patient privacy was also emphasized. There are many similarities between the Norway, Finland and Sweden. The differences are mainly found at a more abstract level. Sweden has only recently conducted a National Strategy for IT in Healthcare, while both Norway and Finland have worked in a more structured way for a longer period of time. Both Norway and Finland are more centralized in their healthcare IT-development. Another interesting difference is the lack of patient involvement in Sweden compared to both Norway and Finland. The respondents claim that patient involvement is a useful preventive measure to protect patient privacy. When patients have the right to see who has accessed their records, the healthcare staff is more careful about avoiding misuse. However, protecting privacy is a very individual task, because people have different attitudes about the matter of privacy and even personal opinions can change depending on the situation. The involvement of patients could therefore be a good complement to the protection of their own privacy. This is a challenge for all three countries, but particularly for Sweden since it does not
allow patients to access their records in the same way as in Norway and Finland. Patient safety and patient privacy in healthcare must be accomplished in order to achieve good quality of care and maintain the trust of the patients. This implies that information security must be taken seriously and the balance between these two concepts should be given careful consideration. However, the healthcare sector in general needs to look at and implement, more extensively, the existing security standards, framework and best practice, such as ISO/IEC 17799 [16] and ITIL [17]. Ongoing work to incorporate the ISO/IEC 17799 into the healthcare sector (ISO 27799) exists, but further efforts are needed to adopt other frameworks into the sector as well. Furthermore, future research needs to follow the developments in how the countries address both the problems and differences, nationally, as well as in how they collaborate to identify common solutions. In addition, guidelines and recommendations for establishing and achieving successful collaboration across national borders should be developed, which can also help establish better links with other countries as well. Such activities will be useful not the least since the mobility of students, the workforce and organizations keeps increasing.

References

8 CEN TC 251, prENV 13729, 1999 Health Inormatics Secure User Identification - Strong Authentication using Microprocessor Cards (SEC-ID/CARDS), 1999.


Patient Safety and Patient Privacy in Information Security from the patient’s view: A Case Study

Rose-Mari Åhfeldt and Eva Söderström

Abstract. The patient is the most important actor in healthcare and it is an obligation for healthcare to operate so that it fulfils the requirements of good care, i.e. provide patients with both patient safety and patient privacy. Furthermore, patients visit more than one healthcare provider, which implies the need for cross-border healthcare and a focus on the patient process. In order to manage sensitive patient information, IT solutions are required and the need of information security in healthcare is obvious. This paper presents the results from a case study in Swedish healthcare aiming to identify problems and needs concerning patient safety and patient privacy from a patient view. We also present how patient safety and patient privacy relate to the information security area, and emphasize the patient’s view on these issues when the transfer of patient information between different healthcare providers becomes more common in the future. The results show that patients focus more on patient safety than on patient privacy, and that their role in their own process must be highlighted.

Keywords. Information security, healthcare informatics, patient safety, patient privacy patient process.

1 Introduction

In healthcare, the patient is the most important actor. According to the Health and Medical Service Act (SFS, 1982:763), the aim of healthcare is to provide citizens with good health. The healthcare has to be provided with respect for the equality of all human beings and the dignity of the individual. Healthcare has to be operated so that it fulfils the requirements of good care (SFS, 1982:763). This implies, among other things, that healthcare has to be of good quality, safe and secure for the patients, easily accessible, based on respect for the patient’s self-determination and privacy, and promote good relationships between the patients and the healthcare actors (SOU 2006:82). Healthcare has to, as far as possible, be conducted and implemented after consultation with the patients. Furthermore, the healthcare must satisfy the patients’ need of continuity and safety in healthcare, and different activities for the patient must be coordinated in an appropriate way (SOU 2006:82). This implies that the patient is the actor for whom healthcare works, and thus the purpose of its aims. Hence, the healthcare sector has to provide patients with both patient safety and patient privacy.

19 A version of this paper is submitted and has an early accept to the Journal of Information System Security (JISS).
In order to fulfil the aims, good medical knowledge and good management of patient information is required. The implementation of IT in healthcare has been slow, but is taking a step in the right direction. The future work aims to involve IT as a support for good and efficient information management within healthcare. This is necessary, not the least since patients can be required to visit more than one healthcare provider. One illness can require visits to several different healthcare providers, which means that the patient information has to follow the patient’s progress through the treatment, that is, the patient process.

Earlier research has shown significant deficiencies concerning information security when patient information has to be exchanged between different healthcare organizations. (Åhlfeldt and Söderström, 2007; Åhlfeldt 2006). Hence, since the patient is an important actor it is of considerable interest to investigate the patient’s view concerning how the healthcare sector fulfils the aims of patient safety and patient privacy. The aim of this paper is therefore to present the results of a case study applied to Swedish healthcare in order to identify problems and needs concerning patient safety and patient privacy from the patients’ perspective. The overall focus is on information security concerning these two concepts. Furthermore, we present and describe the patient process and its importance in a distributed healthcare domain. Our contributions show how patient safety and patient privacy relate to the information security area. Furthermore, our contributions emphasize the patient's view on these issues when the transmission of patient information between different healthcare providers becomes more common in the future.

The paper is structured as follows: The concepts, patient safety and patient privacy together with the patient process, are described in the Section, 2 and 3. Thereafter, the case study and the results are presented in Sections 4 and 5. Some concluding remarks are made in the final section.

2 Patient Safety and Patient Privacy

One main aim of healthcare, as mentioned, is to achieve both patient security and patient privacy. According to Utbult et. al. (2004), the aim of patient safety is to provide the patient with the best care, based on care decisions resulting from the right information at the right time. The lack of information must not lead to for example, the wrong treatment or unnecessary care activities, such as extra patient visits to the doctors due to on unavailable patient information from different healthcare organizations. The keyword here is integration. In addition, the aim of patient privacy is to protect sensitive patient information from being distributed to unauthorized persons. More formally, SOSFS (2005:12) says that patient safety is defined as protection against care harm, that is, the result of measures against risks, incidents and negative events which provide protection against care harm. There is no similar formal definition of patient privacy, but NE (2007) defines integrity and privacy as the right to have one’s personal individuality and internal sphere respected and not to have one’s dignity violated.
With regard to the area of information security and its four characteristics (availability, integrity, confidentiality and accountability), patient safety is clearly related to availability and integrity. Patient information must be available and correct; the right information at the right time. Patient privacy, on the other hand, is related to confidentiality and accountability. It should not be possible for unauthorized people to access sensitive information and it should be possible to trace who accessed what information afterwards. Figure 1 shows how patient safety and patient privacy relate to the information security model. For further descriptions of the model, we refer, for example, Åhlfeldt and Söderström, (2007) and Åhlfeldt et al., (2007).

3 The Patient Process
The patient process is the process that follows the patient during an event of illness. In simple diseases, the patient only has contact with one healthcare provider. When diagnoses become more complicated, however, the patient has to visit different healthcare specialists and actors during one disease event. This means that important patient information must follow the patient in order to secure good quality of care. We therefore need to transfer patient information, not only in one within one healthcare organization, but to several types. For instance, a patient first visits a healthcare center (primary care) where they establish one diagnosis, which requires treatment from a specialist. The patient is then referred to a hospital (secondary care) for further treatment. When the patient has finished the treatment at the hospital, he/she may still need help dealing with the daily tasks of life. The patient can then receive care from the municipality’s home healthcare unit. It should also be noted that many private healthcare actors within the healthcare sector, with which the patient may be in contact also exist. One current problem is that there are no adequate IT-tools supporting this patient process. Each healthcare organization has its own systems, which cannot communicate with each other. This is a risk for the patient safety. Furthermore, when IT tools are developed in healthcare, security
measures must be implemented in order to protect the sensitive patient information, that is, achieve patient privacy. One example of a patient process and its involved care providers is shown in Figure 2.

Figure 2 provides an overview of a real patient process, and illustrates how many care providers can be involved and their connections in what seems a not so complicated patient process. A patient visits a doctor for pain in the left foot. It appears to be a “ganglion” and has to be removed. Four different healthcare organizations are involved in this example. Furthermore, at each healthcare organization, two-three different units are involved. In total, we have eight different care providers who need patient information in order to provide a good quality of care.

One problem is that no one has seriously modeled and analyzed the patient process. Some research projects have pointed out the need for this kind of work, and have done such process modeling (VITA Nova Hemma, 2007; S@ms, 2007 and Mobis@ms, 2007). However, in healthcare, they only model business processes internally in the organization. A holistic view of the patient process from the patient’s view does hence not exist. Consequently, the patient may be disregarded, which usually jeopardizes both patient safety and patient privacy.

4 The Case Study
The study comprises a small case study of 5 interviews. This section introduces the respondents and the approach used.

4.1 Aim of the Studies
The aim of the case study was to investigate the patients’ view of patient safety and patient privacy with focus on patient information exchange between several healthcare providers.
4.2 Case Study Respondents

Conducting an investigation from a patient perspective is important, but complicated. For time limitation reasons, a questionnaire for many patients could not be used, although it would have been preferable in order to reach as broad a spectrum of patients as possible. Instead, five patient representatives were chosen. These persons are all previous patients who have continued their interest in patient issues in different ways. Two of them work in patient organizations while the other three try to plead the patients’ cause in different interest organizations, projects and investigations.

We do not claim that these individuals provide a total picture of the patients’ view of the observed area. However, their experiences and knowledge mean that they can provide an adequate, clear picture of the status of the patient situation. Relevant conclusions can be drawn from the results, which can then be used to encourage further studies.

4.3 Approach

The study was conducted in semi-structured interviews, that is, the interviews were based on a number of main questions. These questions often generate new ones, which means the interview is more of a discussion or conversation between the interviewer and the interviewed person (Darke and Shanks, 2002). The basis for the questions has been the Info Sec model and its relation to the two concepts; patient safety and patient privacy. From this model, questions were formulated about patient safety and patient privacy based on a holistic view of healthcare. The investigation focused on five groups of questions:

- The patients’ understanding of patient safety and patient privacy
- The present risks with these two concepts
- The sensitivity of patient information
- Security measures to achieve patient safety and patient privacy
- The balance between the need of availability of patient information and the protection the patient privacy.

Seven questions, numbered from 1 to 7 and grouped into five main question areas were asked. The fifth and seventh questions are subdivided into three parts, 1a to 1c. In addition, the five interviews are noted as A – E. The answers from the first question and interview person A have the notion A1a, A1b and so on. All the answers are structured in a similar manner.

The interviews were recorded and transcribed during a period of two working months. All the answers were subsequently analyzed as well as structured and categorizing them in a table. Since question 7 is the main focus of the study, the answers are illustrated in Figure 3 to illuminate the patient’s view of the much-disputed balance between patient safety and patient privacy.
5 Results
This section presents a summary of the results from the five main question areas stated in the applied case study.

5.1 The Patient’s Understanding of Patient Safety and Patient Privacy

Patient Safety
Each of the interviewees agreed that the content of patient safety, as a whole, concerns availability of information.Primarily, when information is available, correct and secure care can be provided. One of the interviewed patients claimed that it also concerns having a functioning information flow. In addition three interviewees also asserted that the patients should own their information or at least have access to it before one can claim or guarantee patient safety.

Patient Privacy
All the interviewees agreed that privacy means no unauthorized person should have access to patient information. One of the interviewees also claimed that privacy is about standing up for one’s principles: “Healthcare doesn’t do that today and it impacts the patient privacy” according to respondent C. Furthermore, two of the interviewees maintained that privacy also concerns the possibility and right to choose. Another stated that the lack of information, which implies a lack of knowledge concerning the patient’s previous medical history, violates the privacy.

5.2 The Present Risk with these two Concepts

Patient Safety
All the interviewed patients agreed that the lack of access to patient information constitutes the greatest risk concerning patient safety. This implies that conditions for providing good and secure care have been removed. The lack of a person responsible for the flow of information, insufficient resources, high work rate, as well as none or deficient tools for measuring care quality are other factors mentioned. One interviewee said that healthcare does not look at the patients’ whole situation, adding that each organization only takes responsibility for its own part. Another mentioned that as a patient it is impossible to know who to go when visiting the healthcare centre, since there is no ranking of the staff:

“You have to be pleased with the doctor working that day and his level of competence is unknown for the patient” (respondent D).

Furthermore, one interviewee considered it remarkable that the same requirements do not apply to patient information systems that apply to other medical equipment. For example, the same kind of testing need not be applied when controlling that the systems are working. There is, however, an upcoming proposal, which will take this issue into account.
Another issue mentioned by several interviewees is that patients do not have access to their own information and cannot participate in their own care:

“It is self-evident that patient must have access to their own information and be informed, partly to check the sayings and doings, but also to be a part of their own care” (respondent B).

One interviewee claimed that the absence of computerized records implies great risks in healthcare concerning patient security:

“Everything can be better if we digitalize our systems. So far we still have paper based records, we have no control of information and the risk is obvious that important information is missing when patient’s health is evaluated.” (respondent E).

Another patient also mentioned the risk of having too many limitations in the computerized systems, which increase the possibility of the doctor not acquiring the needed information.

**Patient privacy**

All the interviewees agreed that the greatest privacy risk concerns the possibility of unauthorized people reading patient information not intended for their eyes. They claim that this continues to be a risk, because the paper-based systems still remaining today cannot be controlled. Unauthorized personnel can read records without logging, and many records are also lost. In the computerized systems, there is also considerable risk for insight of the records, since most of the systems are wide open, according to the interviewees. However, all said they did not consider this a great problem, because from a patient perspective, it is more important that the information is available when needed to those who need it.

“The opportunity to abuse the vulnerability is not much exploited. If so, the healthcare sector would have been reacting earlier” (respondent A).

**5.3 The Sensitivity of Patient Information**

Three respondents consider that even if patient information is sensitive, it cannot be further sub-divided:

“... what kind of information is sensitive is very individual, so that all information needs to be managed carefully” (respondent B).

The interviewees believe this not merely reflects their own opinions, but that they speak for all patient groups. Two respondents said that the healthcare sector could be more generous with levels of authority. Above all, healthcare staff involved in the patient’s care must have access to information regardless of organizational role. Nevertheless, the external boundaries between the healthcare organizations and the society must be very strong. The interviewees mention, for example, insurance companies, employers, and so on. Two of them believe it should be possible to level adjust the information further into one type
of information that is available to all people in healthcare, which should be clearly marked in the record. This kind of information, for example, about allergies, drugs, and so on, can be life-saving for the patient.

One common argument is that some kinds of patient information are more sensitive than other kinds, such as psychological illness, alcohol addiction, or a patient’s sexual orientation. Two respondents believe that prejudices are preserved if levels of patient information are graduated or set more strictly.

5.4 Security Measures to Achieve Patient Safety and Patient Privacy

One common attitude among the interviewees was that the patient record systems at the different care providers must be integrated in order to deal with the lack of patient information. Respondents B and C mentioned the need for synchronized legislation that is more suitable for the new information society. Two respondents stated the need of logging lists, which the patients themselves can access. This would minimize the suspicion that unauthorized people could have access to and read sensitive patient information. If the patient could access the logging lists to check who has read the records, the situation would be less dramatic. However, if the patient discovered something suspicious, he/she could take action to identify the intruder. Another possibility mentioned was to open up the authorization to other healthcare organizations, but still have a strong and clear boundary against the society. The respondents claimed that patient safety will decline unless important patient information can cross care providers’ boundaries. On the other hand, there must also be a strong barrier against society in order to achieve trustworthiness concerning patient privacy: “freaks will always be there but they should not put spikes in the wheel for everyone else” (respondent A).

Some more general measures were also mentioned. For example, education is needed in all healthcare organizations and actors. One respondent maintained that it is necessary to rethink and start again by creating an infrastructure of three levels; technology, information and function. According to respondent A, it is necessary to consider structures and processes in all three levels. Another respondent stated that the internal structures must be improved by clear and consistent rules. One argued for the need of patients’ responsibility for their own process. “It is a betrayal to exclude the patient in the way they are doing today” (respondent C). Although there are patients who may be too sick to take this responsibility, they can have representatives pleading for them.

Concerning technical issues, one respondent pointed out that technical matters do not have to come first. The present problems are not technical. Instead there must be a focus on the design phase when new systems are developed. Another respondent declared the need for improved authorization techniques in order to restrict the access levels against external stakeholders, and to those who absolutely should not have access to information. At the same time, care providers boundaries must be opened to those who actually need access to information. “This is Alpha and Omega for patient safety” (respondent E).
Another respondent pointed out that politicians must take their responsibility more seriously and “put their foot down and show what they really want” (respondent C). It is not possible to let each county council/region or municipality reinvent the wheel over and over according to respondent C. A clearer course of demands and power of action are requested from the politicians.

Setting higher demands for obtaining tools to measure care quality is another initiative to improve patient safety. Although this may seem self-evident, the present situation is far from it according to one respondent. Respondent D requested clearer professional roles, claiming that a doctor must be a doctor and nothing else. A secretary should take care of administrative tasks instead of the doctors, because is more important for the doctor to spend the time with the patients. Furthermore, higher competence at the management level is required: “At the moment you can be promoted by faithful work, not because of improved competence in that area” (respondent D).

Other suggestions from the respondents included smaller units responsible for their own resources and the privatization of hospitals. There would be more benefits for the patients with private hospitals due to higher quality according to the respondent.

5.5 The Balance between the Need of Availability of Patient Information and the Need to Protect the Patient Privacy

The questions related to this were three fold: which concept is emphasized, which should be emphasized, and what will the situation be in the future. Two respondents claimed patient safety is more emphasized today, and two others said patient privacy. The fifth answered that it is not patient safety but had no clear standpoint on patient privacy.

Concerning which of the concepts should be emphasized, four answered that the optimal situation is a balance, while one said patient safety. Two interviewees answered the final question concerning future emphasis when all patient record are computerized and integrated by saying that it will be a balance between safety and privacy in the future as well. One added that even if there was a balance, some emphasis would be on safety, while two answered that only patient safety will be focused on in the future. One of these thought that the rest of society will cherish their privacy while healthcare would be more focused on patient safety. Another claimed patient privacy, because it would take too long for patients to influence healthcare, which is a requirement in order to achieve patient safety.

Figure 3 presents a compilation of the results from the questions concerning the balance between these two concepts.
6 Discussion and Conclusion
The aim with this paper is to present the results from a case study conducted from a patient view in order to identify problems and needs of information security in healthcare. Focus has been on the main concepts and aims of patient safety and patient privacy. Our results contribute in particular to demonstrating how patient safety and patient privacy relate to information security, and what view patients have on these issues.

In order to achieve both patient safety and patient privacy from an information security perspective, it is important to manage the kinds of problems identified in this study which include:
1. not having patient information available when needed, which risks affecting patient safety, and
2. continued use of paper-based patient information as well, which increases an obvious risk for the uncontrolled distribution of patient information – the risk of confidentiality misuse and consequently affecting patient privacy

The National Board for Health and Welfare in Sweden expresses the duties of healthcare in the following way: "Care providers must be obligated to have security systems and routines which guarantee the patient safety in case of unforeseen interruptions and disturbances, and that these are known for the users ... the actual care and treatment situation must be governed for the users access and supply the patient’s right to confidentiality protection and integrity" (National Board of Health and Welfare, 2004, pp. 5-6). Our results show that patients do not believe that the healthcare sector lives up to these duties. If the healthcare sector really sets out to achieve patient safety and patient privacy, they must also achieve availability, integrity, confidentiality and accountability of patient information. Our research contributes by clearly showing the relation between the patient safety/patient privacy and the four common characteristics of information security (safety to availability and integrity, and privacy to confidentiality and accountability). This has not been highlighted in previous research to a great extent. These relations are not absolute, however, since there are situations where confidentiality and accountability are needed in order to achieve patient safety, and availability and integrity are needed to achieve patient privacy. One example is when false
information about a patient’s sexual preferences is recorded and revealed to others. The patient’s privacy is affected, but not necessarily his/her safety. Unavailable patient information can affect patient privacy and safety, since the respect for the patient can be questioned. For example, a surgeon discovers that the x-ray images he/she needed before a surgery are too old, resulting in the cancellation of the surgery the day before its scheduled time. This affects both the patient’s privacy and safety. The contribution of our research highlights the relation between patient safety, privacy and information security, and consequently shows that the healthcare sector must manage the identified safety/privacy problems and needs in order to claim that information security has been achieved.

Our study also shows that the patient representatives focus more on patient safety than on patient privacy. Privacy is an important issue, but should not take place at the expense of patient safety, which the respondents claim is the current situation. Although this is a small study, the results correspond to our previous research in Swedish healthcare (Åhlfeldt and Söderström, 2007). Swedish patients seem rather unconcerned about the possibility of their patient information being revealed to others. One reason may be that Swedish citizens trust their government and confident their information will not be misused by the national authorities. This trust could depend on Sweden’s centuries-long peacetime situation. Privacy is more important for citizens in countries that have to protect themselves from external threats or with regimes, which do not support democracy. Swedish patients are more concerned about privacy protection from an individual perspective, for example, ensuring that their sensitive information is not made known to their neighbors or acquaintances, and so on. Future work must therefore be directed more towards identifying guidelines and critical success factors about how the balance between patient safety and privacy can be achieved and maintained.

Furthermore, it should be noted that the respondents really emphasized the patients’ role in their own processes, such as the right: to own their information, be more involved in the whole patient process, to choose doctors, and be provided with available information about the course of their illness. However, in the near foreseeable future, patients will not be able to own their information even if the opinions are in line with the “National Strategy for eHealth (Ministry of Health and Social Affairs, 2006). According to our research, it is obvious that this perspective is currently far from reality. The healthcare sector still has a long way to go before patients are truly involved in their own processes. It should be noted that the patients themselves rarely take initiatives in this direction. Few patients choose doctors, even when the option is available to them. The National Strategy for eHealth is being implemented via various projects, but patient involvement is only partly in focus. The priorities in this area are to make it easy for citizens to access information about different services for health and healthcare via a web portal, and to provide arrangements for booking appointments and coordinating booking systems in healthcare (Ministry of Health and Social Affairs, 2006). From an information security perspective, our
research shows that patient participation should be encouraged, since the patient is ultimately the only one who can tell if patient safety and patient privacy have been achieved or not. In future research, more patient groups should be included, and a more extensive study should be undertaken to detail these results.

As mentioned in the paper, the aim of healthcare is to provide citizens with good health (SFS, 1982). Consequently, the patient is the most important actor in the healthcare sector. If it is not for the patient’s best that healthcare is working, then who is it working for? To quote one respondent: “Who is there for whom” (respondent C). The patient process must be further clarified and the lack of information management and information security measures must be elucidated. There is a need to clarify the patient process in order to accomplish a comprehensive view, not the least when patient information is to be exchanged between different care providers. However, the question is if patients can manage these aspects themselves. Respondent C mentioned the need of a representative who can plead the patient’s cause, a need which we pointed out in our previous research as well (Åhlfeldt and Söderström, 2006).

The Swedish National Board of Health and Welfare conducts case studies in the healthcare sector, which have shown poor information management and inadequate information security routines as the main risks for healthcare-related injuries (National board of health and welfare, 2007). The results from our research confirm the lack of a holistic view of patients. We contribute with deeper knowledge in this area by pointing out that the patient process is the main aspect to identify and analyze in order to achieve patient safety and privacy in healthcare. Future work must focus on how to identify and analyze patient processes in order to develop a solution for secure patient information management in a distributed healthcare domain.

References


Paper 7: Patients Safety and Patient Privacy in Information Security from the Patient’s view: A Case Study


Abstract. In the context of information systems and information technology, information security is a concept that is becoming widely used. The European Network of Excellence INTEROP classifies information security as a non-functional aspect of interoperability and as such it is an integral part of the design process for interoperable systems. In the last decade, academics and practitioners have shown their interest in information security, for example by developing security models for evaluating products and setting up security specifications in order to safeguard the confidentiality, integrity, availability and accountability of data. Earlier research has shown that measures to achieve information security in the administrative or organisational level are missing or inadequate. Therefore, there is a need to improve information security models by including vital elements of information security. In this paper, we introduce a holistic view of information security based on a Swedish model combined with a literature survey. Furthermore we suggest extending this model using concepts based on semiotic theory and adopting the view of an information system as constituted of the technical, formal and informal (TFI) parts. The aim is to increase the understanding of the information security domain in order to develop a well-founded theoretical framework, which can be used both in the analysis and the design phase of interoperable systems. Finally, we describe and apply the Information Security (InfoSec) model to the results of three different case studies in the healthcare domain. Limits of the model will be highlighted and an extension will be proposed.

Introduction

In the information society, security of information plays a central role in several domains with different scopes and objectives: Privacy of personal data in healthcare; Integrity of transaction and business continuity in the business domain; Safeguard of citizens in the infrastructure domain; and Defence of democracy in the e-government domain, are some examples of such objectives.

In the last decades, due to the spread of Information and Communication Technologies (ICT), governmental organisations and communities of academics and practitioners have developed security models for evaluating products, and setting up security specifications in order to prevent incidents and reducing the risk of harm.

Many different terms have been used to describe security in the IT/IS area. Information security has become a commonly used concept, and is a broader term than data security and IT security [1]. Information is dependent on data as a
carrier and on IT as a tool to manage the information; hence, information
security has an organizational focus [2].

The Swedish National Encyclopedia [3] states that information security is
focused on information that the data represent, and on related protection
defines information system security as: “the protection of information systems
against unauthorized access to or modification of information, whether in
storage, processing or transit, and against the denial of service to authorized
users or the provision of service to unauthorized users, including those measures
necessary to detect, document, and counter such threats”. Four characteristics of
information security are: availability, confidentiality, integrity and accountability,
simplified as “the right information to the right people in the right time” [5].
The Swedish Standardization of Information Technology (SIS) advocates that
information security concerns the protection of information assets, aiming to
maintain confidentiality, integrity, availability and accountability of information
[6].

Availability concerns the expected use of resources within the desired time frame.
Confidentiality relates to data not being accessible or revealed to unauthorized
people. Integrity concerns protection against undesired changes. Accountability
refers to the ability of distinctly deriving performed operations from an
individual. Both technical and administrative security measures are required to
achieve these four characteristics. Administrative security concerns the management
of information security; strategies, policies, risk assessments, education etc.
Planning and implementation of security requires a structured way of working.
This part of the overall security is at an organizational level and concerns the
business as a whole.

Technical security concerns measures to be taken in order to achieve the overall
requirements, and is subdivided into physical security and IT security. Physical
security is about physical protection of information, e.g. fire protection and alarm
systems. IT-security refers to security for information in technical information
systems and can be subdivided into computer- and communication security.
Computer Security relates to the protection of hardware and its contents, e.g.
encryption and backup techniques. Communication Security involves the protection
of networks and other media that communicate information between
computers, e.g. firewalls.

In order to provide a more understandable view of how information security
characteristics and security measures relate to one another, an information
security model (Fig. 1) has been created based on the common characteristics of
information security and SIS classification of information security measures [6].
The aim of the model is to describe what information security represents both in
terms of characteristics and measures, combining the definitions and
descriptions mentioned above.
The main concept “information security” is presented in the middle. The four characteristics together represent information security, and are placed at the top of the figure. All requirements from the organizations concerning these characteristics must be fulfilled for information security to be achieved. The lower part of the model presents the different security measures, divided in a hierarchical order and these are gathered directly from the SIS conceptual classification [6]. Since the term “information security” includes several parts of security measures, the model has been useful both in the research and the educational area, in order to get an understanding of information security and its content. Furthermore, the model has been used as a tool in the research area to express where the problems and needs exist in the information security area [7].

In Figure 1, administrative security is not subdivided, but a case study in the distributed healthcare domain has shown that there is a need to improve the model with a more fine-grained understanding of administrative issues [7]. One way to improve the InfoSec model is to look at other security standards, methods and models in order to discover solutions to extend the InfoSec model. The aim of the paper is to present the suggested extended InfoSec model by using concepts derived from a semiotic model (TFI) in order to increase the understanding of the information security domain and to develop a well-founded theoretical framework which can be used both in the analysis and the design phase of interoperable systems. The results from three different case studies have been drawn upon in order to show the limitations of the current model and to validate the extended model.

Our contribution aims to provide a theoretically founded and empirically tested information security model for the analysis of Information Systems and its context. In this model both the IT infrastructure and the more contextual related aspects related to organizational culture and human behavior are taken into account in order to enlarge the scope of the analysis and to select countermeasures with a holistic view of information security.

The following section presents related work, describes the TFI-model and argues for its appropriateness. In Section 3 the results from three case studies
are described, highlighting the limitations of the information security model. In Section 4 we present a suggestion for an extended InfoSec model and the same results from the case studies are compared with the model in order to validate its extension. Finally, Section 5 concludes the paper.

**Related Work**

The harmonisation of the North American (TCSEC commonly known as Orange Book) and European (ITSEC) criteria for IT security evaluations led, at the end of the 1990s, to the definition of a common set of criteria (Common Criteria) for use in evaluating products and systems and for stating security requirements in a standardised way. The International Standard Organisation accepted these criteria in the ISO15408-1999. These standards define the IT product or system under evaluation as a Target of Evaluation (TOE). TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

Additional standards and models were developed by other national and international organizations taking into account the abovementioned works and more context specific issues. The European Computer Manufacturers Association, ECMA, wanted to achieve a widely accepted basic security functionality class for commercial applications, defining the "Commercially Oriented Functionality Class" (COFC) and afterwards the Extended Commercially Oriented Functionality Class (E - COFC), which extends the application of ECMA’s class of commercial security functions to an environment of interconnected IT systems.

These standards consider “administrative security measures” outside the scope of security evaluation criteria “because they involve specialized techniques or because they are somewhat peripheral to IT security” (CC, Introduction and general model). Despite recognizing that a significant part of the security of a TOE can often be achieved through administrative measures such as organizational, personnel, physical, and procedural controls, they chose to focus on IT security measures and started from the assumption of a secure use of IT systems and products.

A different approach to the security of information can be found in the Code of Practice BS7799, recently accepted by the ISO in the ISO/IEC 27000 family. In this case the processing of information assumes a central role and the focus is on the management of information security instead of the design of secure IT systems and products. This approach considers security of information as a quality sub-factor and provides a set of controls to be put in place in order to deploy an information security management system based on a “plan-do-check-act” cycle similar to the ISO 9000 for quality management. Another quality management based approach to information security comes from Firesmith [8] who defines taxonomy of security-related requirements based on the safety requirements of a system.
This brief overview of security standards shows that the focus of security models, standards and best practices, has moved from considering security as an intrinsic feature of IT systems and products towards a wider vision including the processing of information and the related management issues such as roles and responsibilities. Starting from well-known principles and standards, some authors [9] use layered models to classify security controls and to describe security models. For instance, at the top level there is the organization policy with respect to security, followed by specific corporate programs to promote security and, finally, technical controls. A step forward with respect to these approaches can be to focus on more context-related aspects such as organizational culture and human behavior instead of technology and processes. To this end, starting from the above mentioned InfoSec model, we propose an extension based on concepts derived from a semiotic model. Adopting this view makes it possible to better understand all those context specific aspects that can be difficult to analyze using generalized risk management techniques.

The TFI Model

Adopting the view of an information system as constituted of the technical, formal and informal (TFI) parts which are in a state of continuous interaction [10], the need for an holistic approach to the study of IS security becomes apparent. Using the words of Stamper et al [11] it is possible to illustrate this interrelation of abstracted layers explaining that, “Informal norms are fundamental, because formal norms can only operate by virtue of the informal norms needed to interpret them, while technical norms can play no role…unless embedded within a system of formal norm.” In other words, the informal ways of managing information in organisations are critical and they can not always be replaced by rules or embedded in technical systems. With this view the informal elements (i.e. perception of risks, awareness, beliefs, culture, etc.), which are very context related, should drive the design and the selection of formal (policies, business processes, standards, procedures, etc.) and technical solutions (i.e. software and hardware platforms, network infrastructures, devices, etc.). In the context of information systems crossing the boundaries of a single organization (i.e. virtual organizations and other interoperable systems), the relationship among these three levels is even more complex and requires addressing additional issues such as trust and privacy by the means of new formal and informal mechanisms (i.e. Circle of Trust, federated Identity Management Systems, etc.).

The above mentioned conceptual framework, based on semiotic theory, will be one of the assumptions behind all the subsequent discussion on IS security management. Furthermore we agree with Dhillon’s [12] assumption of viewing problems as an emergent property of reflexive interaction between a system and its context, instead of considering them as a consequence of a system’s function. These premises give an idea of the complexity implicit in preventing, detecting, investigating and responding to incidents, using deterministic methods, when different organizational contexts are involved. This complexity is a serious
challenge for the design phase of Information Security Management Systems (ISMS) when organizations with different security models in terms of people, rules and technology need to cooperate. Indeed, information security can be considered a critical non-functional requirement when inter-organizational interoperability is pursued.

IS security is a wide field and contributions come from several disciplines such as mathematics, engineering, as well as social and management sciences. In this section we briefly introduce some of the contributions to the IS security literature in order to clarify the differences among the three levels [13]: (1) technical: automating and standardizing parts of formal systems such as computers helping in operational tasks; (2) formal: organizational level security mechanisms like governance, policies or processes, such as establishing controls in the structure of organization and (3) informal: individual level security mechanisms, like shaping the norms, beliefs, values, and attitudes of employees, such as establishing normative controls.

Technical level security. From a technical perspective, the preservation of confidentiality, integrity availability and accountability requires the adoption of IT security solutions such as encryption of data and communication, physical eavesdropping, access control systems, secure code programming, authorization and authentication mechanisms, database security mechanisms, intrusion detection systems, firewalls, etc. At this level it is possible to introduce models and methods for the selection of the appropriate technological solution depending on the needs for a particular application.

Formal level security. The formal level of IS security is related to the set of policies, rules, controls, standards, etc. aimed to define an interface between the technological subsystem (Technical level) and the behavioral subsystem (Informal level). According with Lee’s definition of an IS [14], this is the level where much of the effort of the IS management is concentrated. An interesting review of the security literature identifies a trend in information system research moving away from a narrow technical viewpoint towards a socio-organizational perspective [15]. In fact the first methods for addressing security at this level are checklist, risk analysis and evaluation. At the beginning such methods have been grounded in particular well-defined reality (i.e. military), focusing on a functionalist view of reality. However Dhillon and Backhouse [15] show that the definition of rules, standards and controls becomes more complicated than the design of technical systems.

Informal level security. In the domain of the informal level of IS security, the unit of analysis is individual and the research is concerned with behavioral issues like values, attitude, beliefs, and norms that are dominant, and which influence an individual employee with regard do security practices in an organization. The solutions suggested in this domain are more descriptive than prescriptive in nature and the findings at this level need to be effectively implemented through other levels (i.e. formal and technical). An interesting review of research papers
in the behavioral domain, looking at used theories, suggested solutions, current challenges, and future research, has been presented by Harris and Mishra [13].

This approach helps in the management of insider threats. Numerous studies [16-20] have indicated that there is a problem in managing information security especially with respect to controlling the behavior of internal employees. Research has also shown that often internal employees subvert existing controls in order to gain undue advantage essentially because either an opportunity exists to do so or they are disgruntled [21]. The problem gets compounded even further when an organization is geographically dispersed and it becomes difficult to institute the necessary formal controls [22].

Also, the prevention of social engineering attacks deals with the informal level of information security. According with Jones [23], while the typical hacker “takes more advantage of holes in security,” the social engineer manipulates personnel to gain information that would not normally be available, such as passwords, user IDs, or even corporate directories. In effect, social engineering is typically employed by hackers as a means to acquire information that would be extremely difficult to obtain through strictly technical means. Unlike hacking, social engineering taps into the psychology of what people expect from others and their natural tendency to be helpful. Therefore technical barriers and rigid rules are not sufficient to counter these threats if people are not aware of the security risks.

**Extended InfoSec Model based on TFI**

One way to extend the InfoSec model in its administrative part is to use the elements of the TFI-model; formal and informal. Administrative security concerns information security management, which can be both formal and informal. According to Chapter 2, the formal element includes policies, rules controls, standards etc aimed to define an interface between the technological subsystems while the informal element includes the aspects related to the human behaviour. This seems to be in conjunction with the security area too. Björck [24] has also declared this division of information security when he classifies some written papers from the security areas. He divides them into technical, formal and informal parts. He also concludes that information security papers mostly concern technical aspects while there is a further need of research in the formal level, but above all, that the informal level has been neglected. One important element at this level is to make the users security aware. Concerning the formal part it seems to be natural to subdivide it into external and internal levels. Each organisation is subject to external regulations concerning security issues, for instance, laws, regulations and agreements with other companies. Furthermore, there is internal formalism for information security management, such as IT-strategies, security polices, educational programs etc. According to Lee [14] this is the level where much of the effort of the information security management is concentrated. Hence, we have extended the InfoSec model as depicted in Figure 2.
Evaluating the new InfoSec Model

In this section we present the case studies and apply a summary of the results to the new extended model in order to illustrate its usefulness. While it is beyond the scope of this paper to describe the specific case studies in great detail, this can be found in referenced papers. However, a brief description is presented in this section.

The Applied Case Studies

The first case study [25] was conducted in the home healthcare of two municipalities. The focus on this case study was patient privacy, and information from the Swedish Data Inspection Board (DIB) was used as a basis for the interviews with the responsible persons and the healthcare staff working in home healthcare. Observations were also carried out in order to obtain an idea of how personal data is managed by following the healthcare staff in their work.

The second case study [26] includes observations and interviews with healthcare staff at a hospital in the western region of Sweden. The aim of the study was to determine how users of EHR are affected by the requirements of information security, as well as how the users themselves affect information security and in what way they follow the recommendations and advice of the Swedish DIB.

The third case study was performed as part of the VITA Nova Hemma research project [27]. In this research project different healthcare providers participated in order to investigate how a process manager can be used to support a leg ulcer process. This process connects different healthcare actors: primary care, secondary care and municipalities [28, 29]. Part of the case study included a system analysis of different security aspects for the involved healthcare systems. Interviews were held with administrators for the respective healthcare systems.
A second part included further studies of the healthcare organizations’ systems and networks. The suppliers of the patient record systems and the people responsible for the communication networks in the included healthcare organizations were interviewed. The basis for the questions in the security analysis was the ISO-standard ISO/IEC 17799 Information Security Management [30].

The results are briefly summarized: **IT-security** - inadequate logon functions in both systems and networks. **Computer Security** - inadequate access profiles levels. **Communication security** - facsimiles as a communication transmitter, interruptions in the networks, inadequate authentications techniques and security measures concerning mobility. **Administrative security** – lacks of IT-strategies and information security policies, inadequate education in information security, no compliance and follow up, inadequate security awareness and attitudes, inadequate security routines, and no security requirements.

The results from the case studies are presented in Figure 3a and show a number of problems and needs in the different levels of security. The symbols refer to the results for specific case studies, for instance, 1a refers to case study 1 and the results noted a in that particular case. It is out of the scope of this paper to analyze the particular result. Instead, we focus on the structure of the problems and needs. The results show that there is a cluster of problems and needs in the administrative security area. In comparison with the technical security this part will be hard to express in more detail, and there is no balance concerning the graphical illustration between the technical and administrative levels. One reason could be that technical measures have a higher priority and have been in focus for a longer period of time. Therefore it is necessary to further detail the administrative part of the information security model as well, and thus get an improved view of where problems and needs are located within administrative security.

![Fig. 3a: Needs in healthcare.](image)

![Fig. 3b: Corresponding results in the extended InfoSec model](image)

One approach is to apply the results shown in Figure 3a to the extended InfoSec model. The result at the administrative security level has been classified...
according to the new levels of administrative security: formal and informal. The formal issues have been further classified as external and internal. The result of this classification is shown in Figure 3b and should be compared with results from Figure 3a.

The result shows that our case studies exhibit both formal and informal problems and needs. However, in the formal part, there are no reported problems at the formal external level. This does not imply that there are no problems in this area, however. Other investigations reveal problems at this level, concerning, for instance, legislation contradiction [31]. It is reasonable to assume that the problem was not mentioned in our case studies since other more internal problems impact the respondents’ daily work more directly. Another formal external problem could be e-contracting. In the healthcare area, no such contracting is applied to date, and therefore no such problems have been identified. In the future, when different healthcare performers will exchange patient information, some kind of contracting may very well be implemented, and may hence also become a security problem at this level.

An interesting finding is that if the InfoSec model had included external administrative security from the beginning, the interviewer could have asked more direct questions for the formal external purposes. Instead, the administrative part alone was in focus, causing the questions to be rather abstract. This also shows that the extended model could be of great use in order to emphasize the whole of the information security area, and the administrative security level in particular.

In the informal part we not only find problems like inadequate security awareness and attitudes, but also missing measures for compliance and follow up activities. Technical solutions are quite easy to implement. Formal administrative solutions can be considered a rigid task to perform but are in fact attainable. The main challenge for information security in the future is to implement useful methods to achieve security awareness in organizations. According to Valentine: “Employee security awareness programs need to begin growing out of their infancy and be treated with as much attention to detail as any other information security engagement” [32].

Discussion and Conclusion
We have shown how the InfoSec model can be extended by using elements from the TFI model. The administrative part of the InfoSec model has been subdivided into formal and informal security. The formal part has been further subdivided into external and internal parts. Our main contributions include showing how the extended InfoSec model can be of great use in order to emphasize a more holistic view of the information security area, and the administrative security level in particular. The model also visualises, more specifically, within what areas information security measures need to be taken into account.
The case studies presented in this paper indicated no external problems and needs in the formal part of information security. We do not claim that all external regulations and legislation issues have been taken to account or that there are no problems concerning the external part. This investigation of external issues has just not been in focus. In the internal formal part, there is a need for information strategies and information security policies strongly related to context or the type of domains such as healthcare, military and business sectors. The internal rules, instructions and education should emerge after defining the policies. In the informal part there is also a need for measures to support the organisation in implementing information security awareness. This is not a simple task, but very important in order to reach sufficient information security within the whole organisation.

One weakness of this paper is that only one single investigation has been used to evaluate the extended InfoSec model. Future work must evaluate the model in other studies as well, both theoretically and practically, in order to establish its usefulness.

Furthermore, we need to investigate how to construct context-related strategies and policies. A risk management methodology which takes behavior and cultural aspects into account is needed to improve security awareness. The extended InfoSec model has a holistic approach and can therefore be a helpful tool to bring informal issues into account. For example, why such a risk management methodology should be based on our model, especially in the asset identification phase (physical asset but also value of information for the stakeholders) and also in the control selection phase.

The need for formalisation in the design phase of information systems development is moving towards the use of semantic technologies and ontologies. Future research should therefore evaluate the extended model in other domains. In the INTEROP project and the task group of non-functional aspects in particular, some related work which is on-going may enable a broader evaluation. The extended model should be seen as a semantic model in order to be a useful support in different areas including the information security issues.

References


The Need for a Coordinator for Cross-Border Healthcare Planning

Rose-Mharia Åhfeldt and Eva Söderström

Abstract. In healthcare today, different caregivers are involved with different types of diseases and disabilities. Consequently, patients are transferred between organizations. These caregivers do not currently collaborate to a satisfactory degree, which results in patients suffering from the lack of coordination. This includes shortcomings in patients safety, i.e. the ability of the caregivers to provide patients with the necessary care. It is thus important to analyze the work process for healthcare planning that spans across several healthcare borders. This paper presents a project aimed at performing such an analysis. It uses the results to identify required improvements. These may be used as a way of establishing a better basis for decisions guiding the development of new or existing IT systems that in one way or another deal with healthcare planning. Results show, for example, the importance of assigning a specific person – a coordinator – with the overall responsibility for coordinating all the activities conducted for the patient in order to improve their safety.

Introduction

Healthcare today faces many challenges. One of these is to ensure that healthcare organizations can collaborate in order to satisfy patient needs for a complete and continuous healthcare process that spans the borders of several caregivers [1, 2, 3, 4]. This non-functional aspect is currently being addressed within Swedish healthcare. The need for interoperability not only stems from the patients, but also from healthcare staff that interact with patients on a daily basis [5, 6]. Collaboration between different caregivers must therefore be improved. Many patients suffer from multiple diseases, meaning they have several diagnoses and also require care from different types of caregivers.

Information security in healthcare has two primary goals:
• To achieve a high level of patient safety, i.e. to provide patients with the opportunity to obtain the best care with the right information at the right time; and

21 A version of this paper was published in the Conference Proceedings of the 11th International Symposium of Health Information Management Research (iSHIMR), Halifax, Canada, July 2006.
• To achieve a high level of patient privacy, i.e. to protect sensitive patient information from being distributed to unauthorized persons

It is difficult to achieve both goals at the same time. Often, one aim is compromised on behalf of the other. Therefore, a balance between the aims is necessary when discussing work concerning information security in healthcare [5]. More and more patients receive care in their homes, which places higher requirements on coordination of care efforts between the caregivers for patient safety to be maintained [2; 5].

Work processes for planning healthcare that spans across several organizational borders must be analysed before it is possible to identify how to establish and organize coordination within distributed healthcare [4]. Based on the description of the current situation, improvements can be identified which may create a better decision basis for the development of the IT systems dealing with healthcare planning. This type of analysis and identification of improvements is the focus of this paper.

The paper structure is as follows: the problem description is further motivated in Section 2 along with additional background information. In Section 3, some details about the project approach are presented, before introducing the results in Sections 4 and 5. Some concluding remarks are made in Section 6.

Problem Description
The lifespan of Swedish citizens is increasing more and more. In 2003, Sweden was the only country in the world where more than 5 % of the population was older than 80 years [7]. As people become older, the likelihood of suffering from chronic diseases increases. Furthermore, some people suffer from several illnesses at the same time, which in Sweden is called “multi-sick”. This concept is defined as patients with three or more diagnoses [7]. A related concept is “multi-failing” patients, which according to the same source refers to persons with a fragile life situation, and thus need recurring reviews of the care efforts. The number of multi-failing people is much higher than the number of multi-sick ones [7].

During the last three-four years of their lives, 70 % of the population have some kind of bodily dysfunction. The official population prognosis predicts a continued increase in lifespan. The likelihood of needing much care in the final years thus increases as well [7].

The Need for Common Healthcare Planning
The situation presented above shows some of the challenges that healthcare must address in the future. Multi-sick individuals need care from not one, but several, caregivers. Often, the diagnoses imply that care is needed for a longer period of time. This affects all caregivers, and they must increasingly collaborate and coordinate their activities. The need for common healthcare planning is
clear, as well as a need of structured coordination from a patient perspective. The “law of payment responsibility” has pushed management of healthcare planning to regions and county councils. The law has perhaps primarily pointed to further needs of a common healthcare plan, not only for patients included in the payment responsibility, but for all patients that need healthcare from several caregivers. As the human lifespan increases, together with longer periods of the “fourth age” (i.e. the period when diseases and dysfunctions limit what people can and have the strength to do), this need will increase as well.

It is well known that collaboration and interoperability between actors and their IT systems is essential. In the global sense, problems may arise in communication between people, between people and IT (or ICT), and between the IT systems themselves [8]. These issues exist on a national, regional and local scale. Interoperability can be achieved only if the interaction between two parties can take place at three levels: data, resource, and business process, with the semantics defined in a business context [9]. Interoperability and collaboration is hence not only an IT issue, but an organizational one as well. Collaboration that places the patient in focus is necessary in order to achieve good patient safety. In life threatening situations, for example, knowledge about a patient’s history can be essential to finding the right treatment in time. Furthermore, patients suffering from leg ulcers can receive health service activities from the municipality, along with care from home healthcare actors (primary care) after the ulcer dressing. With the help of IT, it is possible to appoint a process manager that follows patients when they move between different caregivers [3; 10]. Consequently, a person can monitor activities, view which ones are being undertaken, as well as how the activities are scheduled and organized. However, technical support is not the only aspect needed. Organisational changes must also take place [4].

The Issue of Responsibility

Today, there is much discussion about collaboration in healthcare. In order to increase the quality of care, healthcare actors must coordinate their efforts and activities. What is missing is someone with an over-arching responsibility for the collaboration. All caregivers have an indirect responsibility, and coordination often works satisfactorily. However, this depends more on the caregivers' goodwill than on the organizations themselves. There are too many examples of failure in shared responsibility, and the situation is therefore not acceptable.

Participation of Patients and Relatives in Healthcare Work

In healthcare, the patient should be in focus. However, in practice, patients are rarely given an overview of the set goals, decided efforts, and ongoing activities that concern them. A multi-sick patient with many caregivers is often “clinched” between the work processes of the different caregivers. There is also a lack of a common goal formulation for the entire care process. Patients and their relatives need firstly, to participate in the common healthcare planning, and secondly, to
actively take part in its implementation. They are the ones most capable of determining whether or not goals have been reached.

**Project Description and Approach**

The purpose of the project was to analyse the work process for cross-border healthcare planning, and to identify requirements for improvement based on the analysis of the current situation. The result will provide a basis for deciding how to develop existing IT systems that deal with healthcare planning in one way or another. Examples of such systems are WebCare and S@ms [11, 12]. There is a need to coordinate and develop this IT support. The participants were healthcare staff from one county council in Sweden, including one municipality, the primary care, and private caregivers. All in all, 23 people were involved.

Five working meetings were held with participants. All the meetings were documented and the material was validated by distributing the transcripts to participants for commenting. The process analysis was performed using the Visuera Method [13], which supports the implementation and operation of a process-oriented approach. This contributes to: optimisation of resources that can be monitored and measured, calculation and measurement of delivery times, highlighting and elimination of unnecessary delays, getting the right information to end-users at the right time, and simplified “follow up” activities. The Visuera Method shares features with existing workflow tools. The difference is that a workflow system does not integrate applications. In the Visuera Method, both end-users and applications are integrated with the same solution, hence enabling a higher degree of automation. Having the eProcess in real time makes the business process more efficient [13].

**Results**

This section presents the project results in terms of a proposed solution for cross-border healthcare planning.

**A Generic Process Model**

The proposed process model (Figure 1) does not assume any organizational prerequisites, but is applicable to all types of case descriptions. The main processes: contact/initiation, healthcare planning, and healthcare activities can be seen as iterative, depending on the care situation. Iterations may take place within or between different actors. Iteration within one caregiver could, for example, be an application of a renewed effort within home healthcare or iteration between caregivers could be renewed healthcare planning.

**Coordination Responsibility**

There is a clear lack of coordination responsibility within healthcare today. Coordination responsibility implies responsibility for activities performed by other caregivers, and there is no legal foundation for such situations in Sweden.
today. Several questions arise: What does “responsibility” mean? How comprehensive would the responsibility be? What are the incentives? The project proposes the creation of a “coordinator” role. The “coordinator” should only be responsible for coordinating collaboration at a general level, such as distributing notifications of changes, making relevant contacts, summoning for renewed healthcare planning, and so on. It should and must not mean that the responsibility of other caregivers is reduced. According to Swedish law, all healthcare actors have their areas of responsibility, and there is an implicit responsibility to collaborate. However, the “coordinator” role needs to be explicit and clarified.

It is not predetermined how the coordinator should be assigned to the role, but our results propose that the coordinator is assigned during healthcare planning. It may be one or several persons, and the assignment should be made by the responsible caregiver or by the caregiver with whom the patient engages the most. The coordinator has an active responsibility, which means that he/she/they may be assigned activities that are not explicit or known today. Appropriate resources must be allocated to the responsibility.

![Figure 1: The generic process model of cross-border healthcare planning](image-url)
Healthcare Information

Part of the solution regarding how patients and their relatives can become involved in healthcare is a proposition for a service we call “healthcare information”. The main purpose is to provide patients and relatives with access to goals, plans, follow-ups and daily activities in their care, and their being able to influence the implementation of these activities. This model was proposed in a previous project – S@ms [11]. However, it needs to be further enhanced, primarily from a role-based perspective (the coordinator), but also from further enhancement of the structure for goals, evaluation instruments and goal fulfilment. Based on the general process description, a number of defined interfaces emerge. The information distributed via these interfaces comes from the caregivers’ own IT-based organizational support. The information will exist in several places, but double documentation should not exist. This places requirements on realization of interactions with other systems. No assumptions are made in the performed analysis regarding how to construct the technical solution for the IT support to be developed.

Conclusions

The proposed solution generates a number of conclusions and proposals for future developments:

The coordinator compromise: If collaboration between different caregiver organisations is to function satisfactory, there is a need for what this project terms ”a coordinator” with an active responsibility to ensure that collaboration takes place. The project does not propose exactly how this should be implemented, primarily since some aspects concerning the role are unclear. There is thus a need for future work in order to ensure a satisfactory and accepted result. However, there is still a need to point out the need for this role.

The need for analysing specific healthcare processes: the project results include a simplified model of a complex reality. Further investigations are needed concerning the information flow in this model. Process descriptions were made from a caregiver perspective. A complementary analysis would be undertaken from the patient/caretaker perspective. For example, are there value benefits? Are there further interfaces to other caregivers/functions not included in the model? Such an analysis would clarify shortcomings in quality and potential improvements thereof, as a necessary decision base for implementation.

Collaboration forms within development, implementation, and operation: Financial issues for common healthcare planning have been discussed in the project. Previous experiences point to the difficulty of getting different municipalities committed to common projects. We stress the need to identifying what actors are to be part of initiated common projects or when common solutions are to be implemented. All actors should participate from the start.
Operation, maintenance and financing are factors that must be acknowledged and emphasized when several healthcare organizations share IT systems.

**Legislation:** The proposed solution regarding the coordinator role does have legal implications. There is a need to analyze which of these aspects concern responsibility, mandate and authority in the different healthcare organizations. Who is allowed to do what in a legal sense? What laws and regulations are common and which ones can be different between the caregivers? Legal experts in healthcare must meet in order to answer these questions. Long-term plans for implementing common IT support must also be part of such investigations. Furthermore, it is essential to consider other investigations in continued planning, such as the currently ongoing Swedish patient data investigation.

Summarised suggestions for further organisational development: The following summarises actions and questions that need to be further investigated and elaborated on.

- Clarifying the coordinator role
- Legislation investigation into responsibilities and mandate, with the consideration to and resolution of authority and information management issues
- Test piloting the proposed model in real life situations, and
- Aspects for future projects: identifying which healthcare organizations that should participate, and including them from the start; consideration of financial issues; and discussion regarding operation and maintenance once the organizational model has been enhanced and tested

The lack of coordination in healthcare planning is an important issue to solve in order to achieve non-functional aspects such as trust and patient safety. Our and previous results (e.g. [4] and [6]) point to the need for national coordination and support in terms of both a technical infrastructure and organizational coordination strategy. Responsible healthcare leaders and politicians must take an active part here. Our work has taken the discussion one step further, by proposing how coordination could be managed, and what it should consist of. Furthermore, laws and regulations must also be reviewed, and already implemented success stories and good examples must be developed. Coordination responsibilities should be clarified and implemented. Interoperability between different healthcare organizations will not be satisfactory until the non-functional aspects are taken seriously.

**Acknowledgement**
A special acknowledgement goes to Visuera Integration AB and Stockholm County Council for their participation.
References

Appendix

Interview questions with nurses (N) and managers (M) from case studies 1 and 5

The following questions are formulated based on recommendations given by the Swedish Data Inspection Board and their common advice concerning the processing of personal data.

Introductory questions
• For how long have you held your position in the organization and what does it include? (N, M)
• What level of experience do you have of using computers? (N, M)

Managing a patient’s identity
• How is the control of a new patient’s identity managed? (N)
• Has it ever occurred that patients have been mixed up, and if so, what were the consequences? (N)
• Which are the basic principles for patient identification in your organisation? (M)

Strategies to ensure information requirements by the Directive 95/46/EC
• Directive 95/46/EC aims to prevent the violation of personal integrity in the processing of personal data. According to the directive, there are strict requirements that the information given to patients must be improved. Furthermore, the controller of the personal data must without delay make strategies such as the strict demand of information can be fulfilled as the directive apply. Does your organization, in your opinion, have such strategies that meet the requirements of information demanded according to the directive? (N, M)

Distribution of regulation information
• How are the constitutions or other organizational rules distributed so you can realize them in the organization? (N, M)

Managing protection of unauthorised access
• Staff members can make unauthorized access externally but also internally. The unauthorized access can be both intentional and unintentional. How is unauthorized access prevented in the record system you are using? In what way would the protection be improved? (N, M)
• If patient information is distributed to other users, the receiver should be ensured by encryption. Is the information in the system encrypted? If yes, what kind of encryption algorithm do you use? (M)
Levels of access profiles
• In order to prevent unauthorized use or access, a control system of authorization should be established. Such a system should have the opportunities to identify the users and possibilities to confirm them, for example by using personal passwords. The system should have the ability to check the use so that only those who need the information in their work should have the access to protected personal data. There should also exist routines for access control. What are your opinion about the current access and checking of authority in your existing systems? (N, M)
• Have you got any information about how often the authorities are updated, and what person in charge manages the updating? (N)

Follow-up routines
• What knowledge do you have about the organization’s security policies? (N)
• Does the organization follow-up and evaluate the policies? If yes, how often? (N)
• Is there any routine evaluation or following-up of the information security within the organization? If yes, how often? (M)

Educational program of information security
• What kind of educational program for educating healthcare staff in general information security issues is provided by your organization? Was there any specific strategy for security education when the computerized system was introduced? (N)
• Is there any existing educational program to educate healthcare staff in information security in general? When introducing new systems, how are security issues managed in the education? (M)

Log management
• To check the access to the system, there should be, depending on the sensitivity of the personal data, a log file stored on a separate storage device. This log file should be followed-up and be protected against non-permitted changes. What is your knowledge about the log file in the system and what it contains? Have you got any information about what data is stored in the log file? (N, M)

Distribution of patient information
• In what way do you send patient information to other healthcare providers: electronically or manually? (N, M)
• How do you manage security protection concerning distribution of patient information to other healthcare providers? (N, M)

National Program for IT (Case study 5)
• What are your considerations about the National Program of IT? (N, M)
• How can information security be improved in this program, from your opinion? (N, M)
• What are the main security risks with the project? (N, M)
Patient safety and patient privacy (Case study 5)

- The main purpose of information security in healthcare is to achieve two important aims. The first is to achieve a high level of patient safety, i.e. to provide patients with the opportunities for the best care with the right information at the right time. The other aim is to achieve a high level of patient privacy; i.e. to protect sensitive patient information being distributed to unauthorized persons.

  a. Which of these two aims is most emphasized in present healthcare? (N, M)

  b. From our opinion, what are the desired focus concerning these two aims? (N, M)

  c. In the future, which of these two aims is emphasized then from your opinion? (N, M)
Interview questions with system administrators (S) and nurses (N) from case study 2

**Introductory questions**
- For how long have you held your position in the organisation and what does it imply? (S, N)
- What experiences do you have of using computers?

**Strategies to ensure information requirements by the Directive 95/46/EC**
- Directive 95/46/EC aims to prevent the violation of personal integrity in the processing of personal data. According to the directive, there are strict requirements that the information given to patients must be improved. Furthermore, the controller of the personal data must without delay make strategies such as the strict demand of information can be fulfilled as the directive apply? (S, N)

**Education and information**
- Have you received any education in information security from your employer? (N)
- Have the users received any education in information security? (S)
- What kind of routines exists for developing and following-up information security? (S)
- Does any educational program exist in the organization in order to educate healthcare actors information security? (S)
- What kind of information have you received concerning the information security policy in the organization? (N)
- How is this information disseminated to the users concerning the information security policy?
- How is the policy followed-up and further developed in the organization? (S)
- Did any specific strategy for education in security exist when the systems were computerized and introduced? (S)
- How do you get knowledge about constitutions and other rules and how they can be used in your daily work? From your opinion, are they complete and sufficient? (N)
- How are constitutions and other rules disseminated in the organization in order to be enable users to use them in their daily work? From your opinion, are they complete and sufficient? (S)
- In what way are you impacted by the information security requirements? (N)
- In what way are the users impacted by the information security requirements? (S)

**Authentication**
- Which are the basic principles for patient identification in your organisation? (S, N))
- How was your identity checked when you were employed? (N)
Appendix

• What are the basic principles for user identification in the systems? (S)

Authentication and access control
• Have you ever used another user’s name and password to log on to the system? (N)
• Have you ever allowed someone else to use your username and password to log on? (N)
• Are there any routines for checking that users use their own user login and not someone else’s? (S)
• What is your opinion concerning authentication methods? Does it hinder you in your daily work? (N)
• What is your opinion about access control techniques in the existing systems? (S)
• Are authorization decisions documented? (S)

Authorization and password
• Does the system inform you when you need to change the password or is it your own decision and activity? (S, N)
• What are your experiences about the process of password change? How often do you change your password? (N)
• How many passwords do you have to remember in your work? (N)
• What are your experiences about remembering the password(s)? (N)
• Have you ever discussed your password with a colleague or written it down somewhere else? (N)
• Do you believe that your password is sufficiently safe or is it easily figured out? (N)
• Have you ever used a password including the name a relative or something similar? (N)

Confidentiality
• Are there any routines in the organization that impact who has access to the patient records? Are these routines and rules clearly described how are they followed-up in the organization? (S, N)
• How is unauthorized access to computerized records prevented and how can the protection be improved? (S, N)
• How do you transfer patient information to other healthcare units? If you use any technical equipment such as e-mail or facsimile, is the information then encrypted? (S, N)

Non-repudiation
• In what way do you check that the receivers are authorized to access the transmitted information? (S, N)
• For how long can a note in the patient record be unsigned? (N, S)

Accountability
• Is sensitive information logged in the system? (S, N)
• How are the logs checked and managed? (S, N)
• Do you have any knowledge about what kind of information that is logged? (N)
• How do you apprehend that the systems are logged? Do you consider logging a necessary action or not? (N)

Privacy
• Is it difficult to remember all information concerning one patient when you work with different patients and then write information into the patient records? (N)
• Do you use different access levels such as read, write and delete and can the user change it? (N)
• In what way can you change already recorded information? (S)
• How is information stored? (S)
• Is the information available or stored in separate storage units? (S)
• Can unauthorized people have access to printed information? How often are copies printed out from the record and stored in archive? (S)
• How often are you provided back-ups of the computerized records? (S)

Other questions
• What is your experience concerning managing sensitive information? (N)
• In what way do interruption in the patient record system impact your work? (N)
• How is information security impacted when the patient record system is interrupted? (N)
• Are the systems available enough to enable you to do your work sufficiently? (N)
• Do you consider your work requirement to be reasonable? Why? (N)
• How do you consider the working conditions in your department concerning strains, the level of requirements (low/high)? (N)
Interview questions with system- and network administrators (cases 3 and 5) and system developers (case 3)

The following questions are formulated from ISO IEC 17799 Management of Information Security, paragraphs 8 Communications and operations management, and 9 Access control.

Introductory questions
• For how long have you have held your position in the organization and what does it imply?

Business requirements for access controls
• What kinds of business and security requirements have been gathered from the organization concerning access controls? In what way are they documented?
• Are there any possibilities in the system of information classification?
• What kind of access controls do you use? For instance, roll-based?
• In what way do you support the legal aspects of the protection of data and services?

Access control policy
• How is your policy constructed? Are there rules you need to follow strictly and others that are more up to the user to follow?
• What kind of access policy do you use? “Everything is forbidden which not explicit is allowed” or the opposite “Everything is allowed which not explicit is forbidden”.
• Are there any specific functions in the systems that must be signed by the administrator or another person before it is executed?

Access control rules
• How are user registrations managed? Is every user unique or does group identities exist?
• Is it possible to have printed information from the system about who the registered users are and their access privileges?
• How do you manage user accounts? Is there any automatic function in the system indicating that user accounts not have been in use for a specific period of time?
• How are the users verified?
• If passwords are used, how are they managed? Can the users choose their own passwords? What is the recommended length of the passwords? How are the passwords stored? Encrypted?
• Are there any other tools for authentication? Smart cards, biometrical methods etc.
• Is it possible to log on to the system automatically, for instance, saving the password in a macro or a function key?
Monitoring system access use
• Do you use IDS or do you have any other automatically functions for incident events?
• Do you have any routines for recording deviations of user identity, date and time for log in and log out, terminal identity and terminal placing, recording of successful and unsuccessful system authentication, and registering of successful and unsuccessful of access of data and other resources?
• How is the logging process managed? Is it possible to inactivate the logging functions?
• How do you recommend storing the log files and how can they be protected from modification and cancellation?

Encryption and signing
• Is the information in the system encrypted? If not, how do you protect confidential information?
• If you use encryption, what kind of encryption method do you use?
• How is signing managed?
• Have you considered any strong authentication technique, for instance smart cards?

Brief description of the network
• Briefly describe the structure of the network.
• Are there any external connections to the network, for instance other companies, authorities etc? If so, how are these connections protected?
• Can users access the network from a distance, for instance from their homes? If so, how are these connections protected?
• Do you use wireless networks? If so, how are these protected?

Policies, guidelines, compliances and follow-up routines
• What kind of policies do you have describing how the security work would be managed?
• Do you follow any standard or other guidelines?
• Are there specific policies concerning sufficient use of the network from a user perspective, for instance, rules about dissemination of files, downloading of material from the Internet, managing files on other media, management of passwords etc?
• How is the compliance checked according to the policy and regulations?
• What kind of education do you give the users concerning information security?

Technical security measures and routines
• How is the physical protection managed concerning critical equipments?
• Do you have IDS or other incident management resources?
• How do you manage virus protection technically?
• How are mobile equipments, for instance mobile laptops, managed?
• How do you structure the technical protection against Internet, for instance firewalls, DMZ, IDS, routers, filters etc?
• How are users authenticated when they log on to the network?
• How are user accounts managed in systems and in the network?
• What kind of activities do you log?
• How are the logs stored and managed?
• Do system administrators have unique passwords or do they use a group password?

Distribution of patient information
• How is distribution of patient information to other healthcare providers managed technically?
• How is security protection managed concerning distribution of patient information to other healthcare providers?

Patient safety and patient privacy (only case study 5)
• The main purpose of information security in healthcare is to achieve two important aims. The first is to achieve a high level of patient safety, i.e. to provide patients with the opportunities for the best care with the right information at the right time. The other aim is to achieve a high level of patient privacy; i.e. to protect sensitive patient information being distributed to unauthorized persons.
  a. Which of these two aims is most emphasized in present healthcare?
  b. From our opinion, what are the desired focus concerning these two aims?
  c. In the future, which of these two aims is emphasized then from your opinion?
Appendix

Interview questions from case studies 4 and 6 with management people

The following questions are mainly based upon the information security model.

1. What information security problems do you consider are the most unmistakable in healthcare from a national perspective?
   a. generally
   b. administratively
   c. physically
   d. IT-related – computer security/communication security

2. In your opinion, are there any positive aspects of information security in present healthcare (as contrast to problems)?

3. What information security problems do you consider are the most unmistakable concerning cross border healthcare from the patient process perspective?

4. If one looks forward and see possibilities for technical solutions in order to integrate information between different healthcare organizations. What security problems do in this case consider being the most substantially??

5. From the same scenario as I question 4, what positive aspects of information security are there in the future?

6. What kind of security measures do you consider necessary in order to solve the problems as mentioned in questions 4?

7. In your opinion, would the possibility of availability of needed patient information generate new security problems in the future?

8. What security demands and requirements will then be needed from your opinion?

9. The main purpose of information security in healthcare is to achieve two important aims. The first is to achieve a high level of patient safety, i.e. to provide patients with the opportunities for the best care with the right information at the right time. The other aim is to achieve a high level of patient privacy; i.e. to protect sensitive patient information being distributed to unauthorized persons.
   a. Which of these two aims is most emphasized in present healthcare?
   b. From our opinion, what are the desired focus concerning these two aims?
   c. In the future, which of these two aims is emphasized then from your opinion?
Interview questions from case study 7

The following questions are mainly based upon the information security model and its relation to patient safety and patient privacy.

1. What does the term “patient security” mean to you?
2. What kind of present patient security risks do you see?
3. What does the term “patient privacy” mean to you?
4. What kind of present privacy risks do you consider as a patient spokesperson?
5. According to the law, all health information is classified as sensitive information.
   a. From your opinion, how sensitive is this information and its management?
   b. What consideration do you think other patient groups have concerning sensitive patient information?
   c. In what way would patient information be further classified?
6. What kind of security measures (administrative as well as technical) do you consider necessary in order to solve the problems and risks that you have mentioned concerning patient safety and patient privacy?
7. The main purpose of information security in healthcare is to achieve two important aims. The first is to achieve a high level of patient safety, i.e. to provide patients with the opportunities for the best care with the right information at the right time. The other aim is to achieve a high level of patient privacy; i.e. to protect sensitive patient information being distributed to unauthorized persons.
   a. Which of these two aims is most emphasized in present healthcare?
   b. From our opinion, what are the desired focus concerning these two aims?
   c. In the future, which of these two aims is emphasized then from your opinion?
DEPARTMENT OF COMPUTER AND SYSTEMS SCIENCES
Stockholm University/KTH
www.dsv.su.se/eng/publikationer/index.html
Ph.D. theses:

No 91-004 Olsson, Jan
An Architecture for Diagnostic Reasoning Based on Causal Models
No 93-008 Orci, Terttu
Temporal Reasoning and Data Bases
No 93-009 Eriksson, Lars-Henrik
Finitary Partial Definitions and General Logic
No 93-010 Johannesson, Paul
Schema Integration Schema Translation, and Interoperability in Federated Information Systems
No 93-018 Wangler, Benkt
Contributions to Functional Requirements Modelling
No 93-019 Boman, Magnus
A Logical Specification for Federated Information Systems
No 93-024 Rayner, Manny
Abductive Equivalential Translation and its Application to Natural-Language Database Interfacing
No 93-025 Idestam-Almquist, Peter
Generalization of Clauses
No 93-026 Aronsson, Martin
GCLA: The Design, Use, and Implementation of a Program Development
No 93-029 Boström, Henrik
Explanation-Based Transformation of Logic programs
No 94-001 Samuelsson, Christer
Fast Natural Language Parsing Using Explanation-Based Learning
No 94-003 Ekenberg, Love
Decision Support in Numerically Imprecise Domains
No 94-004 Kowalski, Stewart
IT Insecurity: A Multi-disciplinary Inquiry
No 94-007 Asker, Lars
Partial Explanations as a Basis for Learning
No 94-009 Kjellin, Harald
A Method for Acquiring and Refining Knowledge in Weak Theory Domains
No 94-011 Britts, Stefan
Object Database Design
No 94-014 Kilander, Fredrik
Incremental Conceptual Clustering in an On-Line Application
No 95-019 Song, Wei
Schema Integration: - Principles, Methods and Applications
No 95-050 Johansson, Anna-Lena
Logic Program Synthesis Using Schema Instantiation in an Interactive Environment
No 95-054 Stensmo, Magnus
Adaptive Automated Diagnosis
No 96-004 Wärn, Annika
Recognising Human Plans: Issues for Plan Recognition in Human - Computer Interaction
No 96-006 Orsvärn, Klas
Knowledge Modelling with Libraries of Task Decomposition Methods
No 96-008 Dalianis, Hercules
Concise Natural Language Generation from Formal Specifications
No 96-009 Holm, Peter
On the Design and Usage of Information Technology and the Structuring of Communication and Work
No 96-018 Höök, Kristina
A Glass Box Approach to Adaptive Hypermedia
No 96-021 Yngström, Louise
A Systemic-Holistic Approach to Academic Programmes in IT Security
No 97-005 Wohed, Rolf
A Language for Enterprise and Information System Modelling
No 97-008 Gambäck, Björn
Processing Swedish Sentences: A Unification-Based Grammar and Some Applications
No 97-010 Kapidzic Cicovic, Nada
Extended Certificate Management System: Design and Protocols
No 97-011 Danielson, Mats
Computational Decision Analysis
No 97-012 Wijkman, Pierre
Contributions to Evolutionary Computation
No 97-017 Zhang, Ying
Multi-Temporal Database Management with a Visual Query Interface
No 98-001 Essler, Ulf
Analyzing Groupware Adoption: A Framework and Three Case Studies in Lotus Notes Deployment
No 98-008 Koistinen, Jari
Contributions in Distributed Object Systems Engineering
No 99-009 Hakkarainen, Sari
Dynamic Aspects and Semantic Enrichment in Schema Comparison
No 99-015 Magnusson, Christer
Hedging Shareholder Value in an IT dependent Business society - the Framework BRITS
No 00-004 Verhagen, Henricus
Norm Autonomous Agents
No 00-006 Wohed, Petia
Schema Quality, Schema Enrichment, and Reuse in Information Systems Analysis
No 01-001 Hökenhammar, Peter
Integrerad Beställningsprocess vid Datasytstemutveckling
No 01-008 von Schéele, Fabian
Controlling Time and Communication in Service Economy
No 01-015 Kajko-Mattsson, Mira
Corrective Maintenance Maturity Model: Problem Management
No 01-019 Stirna, Janis
The Influence of Intentional and Situational Factors on Enterprise Modelling Tool Acquisition in Organisations
No 01-020 Persson, Anne
Enterprise Modelling in Practice: Situational Factors and their Influence on Adopting a Participative Approach
No 02-003 Sneiders, Eriks
Automated Question Answering: Template-Based Approach
No 02-005 Eineborg, Martin
Inductive Logic Programming for Part-of-Speech Tagging
No 02-006 Bider, Ilia
State-Oriented Business Process Modelling: Principles, Theory and Practice
No 02-007 Malmberg, Åke
Notations Supporting Knowledge Acquisition from Multiple Sources
No 02-012 Männikkö-Barbutiu, Sirku
SENIOR CYBORGS- About Appropriation of Personal Computers Among Some Swedish Elderly People
No 02-028  **Brash, Danny**  
Reuse in Information Systems Development: A Qualitative Inquiry

No 03-001  **Svensson, Martin**  
Designing, Defining and Evaluating Social Navigation

No 03-002  **Espinoza, Fredrik**  
Individual Service Provisioning

No 03-004  **Eriksson-Granskog, Agneta**  
General Metarules for Interactive Modular Construction of Natural Deduction Proofs

No 03-005  **De Zoysa, T. Nandika Kasun**  
A Model of Security Architecture for Multi-Party Transactions

No 03-008  **Tholander, Jakob**  
Constructing to Learn, Learning to Construct - Studies on Computational Tools for Learning

No 03-009  **Karlgren, Klas**  
Mastering the Use of Gobbledygook - Studies on the Development of Expertise Through Exposure to Experienced Practitioners' Deliberation on Authentic Problems

No 03-014  **Kjellman, Arne**  
Constructive Systems Science - The Only Remaining Alternative?

No 03-015  **Rydberg Fåhraeus, Eva**  
A Triple Helix of Learning Processes - How to cultivate learning, communication and collaboration among distance-education learners

No 03-016  **Zemke, Stefan**  
Data Mining for Prediction - Financial Series Case

No 04-002  **Hulth, Anette**  
Combining Machine Learning and Natural Language Processing for Automatic Keyword Extraction

No 04-011  **Jayaweera, Prasad M.**  
A Unified Framework for e-Commerce Systems Development: *Business Process Patterns Perspective*

No 04-013  **Söderström, Eva**  
B2B Standards Implementation: Issues and Solutions

No 04-014  **Backlund, Per**  
Development Process Knowledge Transfer through Method Adaptation, Implementation, and Use

No 05-003  **Davies, Guy**  
Mapping and Integration of Schema Representations of Component Specifications

No 05-004  **Jansson, Eva**  
Working Together when Being Apart – An Analysis of Distributed Collaborative Work through ICT from an Organizational and Psychosocial Perspective

No 05-007  **Cöster, Rickard**  
Algorithms and Representations for Personalised Information Access

No 05-009  **Ciobanu Morogan, Matei**  
Security System for Ad-hoc Wireless Networks based on Generic Secure Objects

No 05-010  **Björck, Fredrik**  
Discovering Information Security Management

No 05-012  **Brouwers, Lisa**  
Microsimulation Models for Disaster Policy Making

No 05-014  **Näckros, Kjell**  
Visualising Security through Computer Games

Investigating Game-Based Instruction in ICT Security: an Experimental approach

No 05-015  **Bylund, Markus**  
A Design Rationale for Pervasive Computing

No 05-016  **Strand, Mattias**  
External Data Incorporation into Data Warehouses

No 05-020  **Casmir, Respickius**  
A Dynamic and Adaptive Information Security Awareness (DAISA) approach
Svensson, Harald
Developing Support for Agile and Plan-Driven Methods

Rudström, Åsa
Co-Construction of Hybrid Spaces

Lindgren, Tony
Methods of Solving Conflicts among Induced Rules

Wrigstad, Tobias
Owner-Based Alias Management

Skoglund, Mats
Curbing Dependencies in Software Evolution

Zdravkovic, Jelena
Process Integration for the Extended Enterprise

Olsson Neve, Theresia
Capturing and Analysing Emotions to Support Organisational Learning: The Affect Based Learning Matrix

Chaula, Job Asheri
A Socio-Technical Analysis of Information Systems Security Assurance

Fernaeus, Ylva
Let’s Make a Digital Patchwork

Bakari, Jabiri Kuwe
A Holistic Approach for Managing ICT Security in Non-Commercial Organisations

Sundholm, Hillevi
Spaces within Spaces: The Construction of a Collaborative Reality

Hansson, Karin
A Framework for Evaluation of Flood Management Strategies

Aidemark, Jan
Strategic Planning of Knowledge Management Systems

Kabilan, Vandana
Ontology for Information Systems (O4IS) Design Methodology: Conceptualizing, Designing and Representing Domain Ontologies

Mattsson, Johan
Pointing, Placing, Touching

Kessler, Anna-Maria
A Systemic Approach Framework for Operational Risk

Van Nguyen Hong
Mobile Agent Approach to Congestion Control in Heterogeneous Networks