LUND UNIVERSITY
School of Economics and Management

..

Managing Information Security in Healthcare:

A Case Study in Region Skåne

Master thesis, 15 hp, Department of Informatics

Submitted: June 2008
Authors: Emil Wallin
Ying Xu

Supervisor: Anders Svensson
Examiners: Erik Wallin
Linda Öberg

Managing Information Security in Healthcare:

A Case Study in Region Skåne

© Emil Wallin
© Ying Xu

Master Thesis submitted June, 2008
Size: 73 pages
Supervisor: Anders Svensson

Abstract

Information security is vital to organizations. This is particularly evident in healthcare where patient information is regarded as very sensitive. The patient is the most important actor in healthcare, and therefore patient information must be kept secure from breaches. At the same time, the right information must be available at the right time when needed in order to provide patients with the best possible care. The availability and accessibility of information is becoming more and more important as we are moving towards a society where patients can receive care from several providers in cross-border healthcare, implying that information need to be sent across borders in a distributed healthcare domain.

This research took a broad approach into the distributed healthcare domain of Sweden, with practical focus in Region Skåne. A thorough literature review was conducted and semi-structured interviews with key personnel in the psychiatry division of the Region were also conducted. Due to limited time and resources, other regions in Sweden and interviews with patients were omitted from this research.

The results derived from this research show that there is a great need for focus on patient security and providing patients with the best possible care, than to focus on patient privacy, where information about patients are kept safe. Moreover, the results show that IT utilization in healthcare is far from optimized, with several different systems for patient journal records being used in the same region and most of these systems are not created accordingly to user needs or even to Swedish laws.

This research contributes by: exploring the information security model characteristics, comparing *eHealth* and *eBanking* arguing that *eHealth* can learn from *eBanking*, identifying some problems and needs in healthcare as well as by presenting an introduction to healthcare in Region Skåne.

Keywords: Information Security, ICT, Risk Management, Patient Security, Patient Privacy, eHealth, Swedish Healthcare System.

Table of Contents

List of Tables

List of Figures

1. Research Scheme

This chapter outlines the content of our research report, as well as introducing the field of information security, and healthcare. We introduce our research as well as presenting our research questions.

1.1 Introduction

Information is vital to organizations and it is imperative that it is secured through the process of information security risk management (Websense, 2005). Information security risk assessments ensure that the correct assets are being identified and that the risks are quantified accurately to ensure appropriate mitigation or acceptance. Because of the importance of information in organizations, risk management standards and information security guidelines have emerged to supply organizations with a basic risk management process for accurate identification, analysis and management of information risks. The field of Information and Communication Technologies (ICTs) is developing rapidly and these can help in many ways to address challenges in healthcare (UNESCO, 2002; The Royal Society, 2006).

There is a substantial need for research in the area of information security in healthcare in order to explore problems and needs at a general level (SEMA, 2005). Therefore, this research project will conduct exploratory case studies within the psychiatry division and at IT departments (in Region Skåne) to determine their information security risk assessment processes and reasons for adopting them as well as their concerns for the future. At the same time, this is a study on what the risks are when sharing information (e.g. patient journals and e-mails) within a hospital in distributed healthcare between its members, patients and practitioners.

Patient information is a critical factor in healthcare, perhaps even the most critical information to secure in healthcare (The Royal Society, 2006). Dwivedi (2003) argue that national electronic patient record will be the norm in the future. Their claim is validated by the fact that various governments have launched similar schemes, with the objective of providing patients records in electronic format. Our literature review will include a more thorough description of the healthcare situation and information security.

Healthcare in Sweden (more specifically, Region Skåne) under the EU healthcare system have many unsolved security issues, concerning accessibility and readability of patient journals, e-mails from patients, and education and knowledge of healthcare personnel. These issues concern personal information about patients and need to be assessed and solved to ensure patient safety and patient privacy (Åhlfeldt, 2006).

The healthcare system has changed radically with the introduction of information systems (IS) and intranets, which is far from purely beneficial; a number of risk and security issues have been raised by the introduction of IT and IS. Earlier research suggests solutions and predicts the future of information security in healthcare. For instance, Dwivedi (2003) argues that healthcare stakeholders will be allowed remote access to patient's medical history as a norm in the near future. The Royal Society (2006) claims that the healthcare system will evolve continuously in the next 15 years and that ICTs are likely to be both a driver for change and an enabler of the changes needed. But the most important issue is to include the patient in the process of information security and privacy in healthcare.

1.2 Purpose

Hospitals are public organizations that provide long-term stays for patients, and are staffed by professional physicians, surgeons and nurses. A plethora of information is transferred, interpreted, created and stored everyday within these organizations. The role of ICT information security and risk management is especially important in these organizations that keep a vast amount of confidential information, to ensure for the delivery of better, more secure and more efficient healthcare services (Ministry of Health and Social Affairs, 2006). In this research project, we will explore how practitioners of medical attendance in hospitals follow guidelines of security and how security issues and risk management is handled by IT personnel..

This study becomes important as it provides us a view of how Swedish healthcare organizations construct and develop their information security risk assessment methodologies. In addition, this study will demonstrate areas of caution for healthcare to ensure the best possible levels of information security. Finally, this research is important as it shows how patient information should be handled in order to obtain both patient privacy and patient security and the research will show what healthcare can learn from other business areas.

1.3 Research Questions

This research includes two research questions. The first one is:

- *What general guidelines, principles and ICTs serve as the foundation of information security and risk management in businesses as well as in healthcare and what can healthcare learn from these other business areas?*

While assessing these three research categories (guidelines, principles and ICTs) we are interested in knowing what the implications from healthcare personnel are both concerning the situation today in healthcare and for the future of healthcare (regarding information security). The second research question is directed towards problems and needs in healthcare, with focus on patient security and patient privacy:

- *What are the perceived problems and needs concerning information security in healthcare in Region Skåne and what needs to be done for the future?*

1.4 Delimitations

Since the project time is limited to ten weeks, we will only be able to conduct our research within the psychiatry division and with IT staff for the research quality. English is the writing language for this thesis, and all the work referred to Swedish literature and transcription, and Swedish-speaking interviewees will be done by our Swedish-speaking author.

We will focus our interviews on doctors, IT personnel and other key members of hospitals. Other key members include management and even nurses. Patients are excluded from this work. The problems with patients are that they will most likely be less inclined to participate in this study than healthcare personnel, and it will be very difficult to schedule interviews with patients. Patients are an integral part of this work and will be included in the literature review, but due to limited time and the above-mentioned reasons, there is no possibility for us to interview patients.

Our empirical research is focused on distributed healthcare (where the healthcare sector includes various healthcare organizations and units and is also referred to as cross-border healthcare in this report) in

Southern Sweden, thus not taking into account any hospitals, standards or guidelines existing in other regions of Sweden, or any other countries. Our literature review will, however, consider other countries (not including Africa, Asia or South America) and regions within Sweden as well as general principles for the European Union. We believe that issues in Region Skåne can be applied on the entire Swedish healthcare, and thus this report does not see Region Skåne as a unique problem area.

1.5 Thesis Structure

In this thesis, information security and risk management in general build up the theoretical framework. As we focus our research on information security in healthcare domain, an extra chapter is created as a bridge between the theoretical part and our case study for a more natural structure. Various continental healthcare policies (e.g. EU eHealth Action Plan) and national healthcare acts (e.g. Swedish National eHealth Strategy) are mentioned in chapter 3 to define the importance of information in today's healthcare system. Problems and needs in the area are also discussed. Patient safety and patient privacy are the two typical information security issues in healthcare from the patients' view. A short description about the patient process is mentioned although patients do not belong to the research interviewee group due to the delimitations. In the discussion, we lift our topic from healthcare domain back to the general information security, to have an overall information security understanding in business. Not only for the features of information security in healthcare, but we are interested in comparing these features with those in other business areas as well, for instance, Internet banking. A final outcome of all chapters' contents synthesizing and some suggestion for future further research end the thesis in the conclusion chapter. This report therefore consists of seven chapters, which are as follows:

- **Chapter 1: Introduction**; introduces the topic, purpose, research questions, delimitations and structure.
- **Chapter 2: Literature Review on Information Security**; draws together the key concepts of information security: ICTs, information security models & characteristics, methods for ensuring information security. This chapter also introduces a risk management part: risk, risk management approaches, significance and purpose of risk management Standards process, risk analysis.
- **Chapter 3: Information and Patient Security in Healthcare**; the third chapter lays out the related findings by identifying the purpose, as well as the problems and needs of the area. System and network security in health care brings out the significance of patient information security in healthcare records. The current Swedish health system, in which IT is implemented, is a further focus in this chapter, with problem background, actors and divisions, Electronic Medical Records, Swedish laws & regulations and so forth. Patient safety and patient privacy are discussed from the patients' perspective. Furthermore, we include European Union's eHealth action plan and the Swedish national strategy in eHealth, thus providing a framework on how healthcare are preparing for the future from both a 'global' (European) and a national perspective.
- **Chapter 4: Method**; related in this outlines how the thesis' chosen research method looks like (the case study/ the interviews) and establishes the motivations behind certain selections. It includes a description on how we got in contact with our interview subjects, how we conducted our literature review, how we conducted our actual interviews as well as how we analyze our gathered data.
- **Chapter 5: Interview results**; presents the findings of the case studies, which are the conducted interviews.
- **Chapter 6: Discussion**; findings for this research project are discussed in further depth, study on other business areas featured by information privacy, drawing the comparison between information security in healthcare domain and general business organization domain.
- **Chapter 7: Conclusion**; synthesizes all chapters' contents and presents the final outcome of the thesis. Directions for further research and contributions to IS research and industry are also established.

2. Literature Review

This chapter introduces the field of information security, and the notion of risk management and risk assessment. Moreover, it presents the importance of keeping information secure and the importance of evaluating risks and creating Standards and Guidelines in organizations to minimize risks. Briefly presented in this chapter are Information and Communication Technologies and the implications it can have on businesses. General principles, such as the importance of availability of important information are presented.

2.1 Information Security

Keeping vital information secure is imperative to all organizations. This is done by practicing information security, and the work must start with a management supporting the co-workers and also by educating end users and organization members in information security (SEMA, 2005). Information security is about protecting information from accidents, breaches or other events that could make it harder to understand the information. Information security is practiced in organizations that tend to rely on information, and a certain lack of information could harm the organization. This mean that information security is important to all businesses as information is very important for businesses. It is important to note that although privacy advocates and the general public often use the phrases "information privacy" and "information security" interchangeably; they are, in fact, very different. Information privacy is about an individual's right to have his or her personal information kept safe and confidential. This right is defined in federal and state law and regulation. Information security, on the other hand, is the means and the mechanisms to protect the privacy (Roberts, 2008). This literature review will focus on information security, thus how to keep the information secure.

The notion of information security has been standardized and defined by ISO, more specifically by the standard *ISO/IEC 17799*. This standard provides guidelines that information security management can find useful. The *ISO/IEC* standard *17799* (International Standard for IT security known as *Information Technology – Code of Practice for Information Security Management)* defines information security within three terms; *Secrecy, Accuracy* and *Accessibility*. Secrecy deals with the notion that information should only be available to those with right authority to read and use the information. Steps are needed to ensure that no unauthorized use occurs. The accuracy of information regards protecting the information so that it is accurate, complete and correct. Lastly, the accessibility of information concerns ensuring that users have access to the information they need when they need it without delays.

The DM Review board (2006) has identified three main security concerns concerning information security: the first one is *The Malware Menace*. Viruses, Trojan horses, worms, spyware and other forms of malicious software pose a major threat to the security of electronic health information. In many cases anti-virus and anti-spyware products can help, but they only treat the symptoms of infection instead of the cause, which often is an improperly configured computer. The second concern is *Automatic Log-off.* Workers in healthcare settings all too often leave their computer workstations without logging off. This poses a major security risk to the organization and the patients, especially when the workstation is in an area accessible to unauthorized people. The third concern is the existence of *Removable Media*. The creation of USB devices such as thumb drives and even *iPods* has created a world in which data can be downloaded to a tiny device and stolen with the click of a mouse. Patient files, folders and personal information residing on the computers at, hospitals and other healthcare organizations are at risk. Threats can also be directed towards physical assets (houses and venues) or information can be used incorrectly. All threats can be divided into internal or external threats. Internal threats can be caused by insufficient administrative or IT routines, while external threats are theft, virus attacks and similar.

When these security concerns have been assessed and thoroughly examined, the question of what improvements are necessary regarding these terms arises. Improvements may be needed, such as reinstallation of fire alarms, new access techniques, installing new burglar alarms, electric circuits that can handle power outages and so on. By hardening computers with the appropriate security configurations, organizations can eliminate the vast majority of system vulnerabilities that malware exploits. Computer sessions should terminate after a certain amount of inactivity. Removable media must be made secure.

The control objectives in *ISO/IEC 17799* are intended to be implemented to meet the requirements identified by a risk assessment, and is intended as a practical guideline for developing security standards in organizations and effective security management practices (ISO Standards, 2005). An organization cannot be certified as an *ISO/IEC 17799* compliant organization, since the standard only provides guidelines and not actual tailored solutions for organizations, there are no specifications that an auditor or implementer can refer to. There are many more *ISO/IEC standards*, with *27001* (management systems for information security – requirements), *27002* (guidelines for controlling information security) and *27006* (Requirements for bodies providing audit and certification of information security management systems) being among the most important in the information security field in Sweden. In Sweden, the *ISO/IEC* work is driven by the company SIS, who strives towards a common language (mainly through standards) and follows the premise that "It is not money that makes the world spin, it is standards" (SIS, 2007).

Moreover, there exist differences in attitudes towards security within organizations; for instance, network administrators believe that some security measures are not required in the network. Network administrators maintain that the actual systems take care of those measures, but system administrators believe that these security measures are dealt with in the networks. It can be seen from the viewpoint that security seems to mean different things to different persons in organizations, perhaps due to their place in the organizational hierarchy (Whitman & Mattord, 2005).

2.1.1 Information and Communication Technologies

Information and communication technology (ICT) has become a foundation of modern society. Many countries now regard the understanding of ICTs and the mastering of basic skills and concepts within ICTs as part of the core of education in their country, alongside reading and writing (UNESCO, 2002).

ICT is an umbrella term encompassing any communication device or application and the various services and applications associated with them. Communication devices and applications include radio, television, cell phones, and computer hardware and so on. People use their cell phones and computers every day; ICT enhance global communication, television shows news from around the world within an instant, and the overall global connectivity is increasing every day. The European Commission claim that the importance of ICT lies more in its ability to create greater access to information and communication in underserved populations than in the technology itself. ICT as a strategic tool will ensure safer and more accessible health services (Ministry of Health and Social Affairs, 2006).

ICTs will help address concerns for healthcare systems as ICTs have much potential. They can expose inconsistencies and inefficiencies in organizations, promote self-care, facilitate joined-up healthcare provision, make service-providers more accountable and even help coping with workforce shortages if correctly used. These potentials could allow ICTs to redesign the organizational structure of healthcare (Ministry of Health and Social Affairs, 2006). Technological developments will drive patient-focused healthcare to be anywhere anytime and 'on-demand'. Electronic records are destined to become important for the overall information environment in healthcare. ICTs will help professionals with information even if participants are at remote locations. Broadband technologies will allow for on-demand access to any information. This will be even more efficient if cell phones are fully integrated with wireless local area networking technology (WLAN).

Introducing ICT use in Swedish distributed healthcare requires the creation of certain conditions, according to the Ministry of Health and Social Affairs (2006). This introduction is hampered by several general problems, divided into three main areas; information needs to uniformly defined, ICT infrastructure needs to be improved and changes in legislation need to occur. These three problem areas must be addressed by doing the following; 1) bring legislation and regulations in line with increased ICT use, 2) create a national information structure for health care services and 3) to further develop the national healthcare infrastructure, which should be done with the view of creating a secure electronic communication system that can link medical devices with care units (Ministry of Health and Social Affairs, 2006).

2.1.2 Information Security Characteristics and Models

Information security has become a commonly used concept, and is a broader term than data security and IT security (Björck, 2001). In the society of Information Age, security of information plays a central role in several domains with different scopes and objectives such as: *Privacy of personal data* in healthcare; *Integrity of transaction* and *business continuity* in the business domain; and *Defending democracy* in the e-government domain. In earlier research, it has been shown that measures to achieve information security in the administrative or organizational level are missing or inadequate. Therefore, the need to improve information security models by including vital elements of information security is turning to be more serious.

In the last decades, due to the spread of ICTs, governmental organizations 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. According to the context of IS/IT, information security is a concept that is becoming widely used. 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. The U.S. National Information Systems Security Glossary (2006, p 33) 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".

Characteristics of Information Security

In order to improve the understanding of the concept of information security, patient safety and patient privacy, the characteristics of information security must be seen as a success. The relation 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.

Information security concerns security issues in all kinds of information processing and includes the following four characteristics: *Availability, Confidentiality, Integrity* and *Accountability* (SIS, 2003). According to SIS (2003) information security is defined as the protection of information assets, aiming to maintain confidentiality, integrity, availability and accountability of information. *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. *Availability* and *Integrity* represent *Patient safety*; *Confidentiality* and *Accountability* are for *Patient privacy*. We will discuss the problems and needs in *Patient safety* and *Patient privacy* in the later chapter although patients are excluded in our interviews.

The Model

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. 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* concerns 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 security measures relate to one another, an information security model has been created (Figure 1). The aim of the model is to describe what information security represents. The model combines the definitions and descriptions mentioned above. All concepts are derived from SIS (2003).

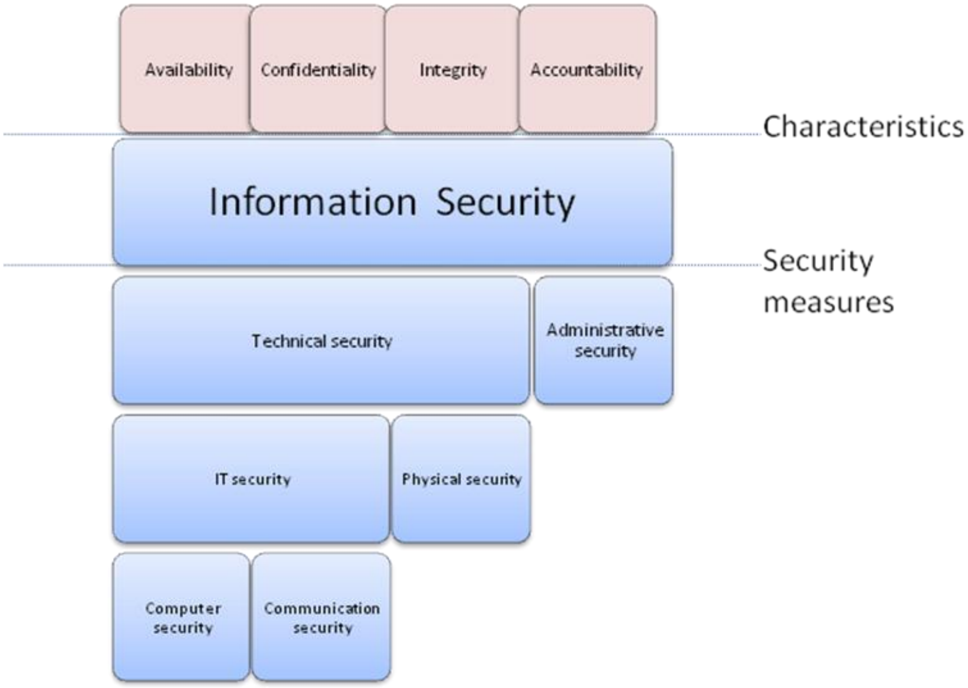

Figure 1: Information Security Model
(Author's own interpretation: SIS, 2003; SEMA, 2005)

The main concept *information security* is presented in the middle. The four characteristics together represent information security, and are positioned at the top of the model. All requirements from 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 (SIS, 2003). Required security measures include both *Technical* and *Administrative security*.

2.2 Risk Management

Today's information security professional's use risk analysis techniques to identify the level of security to be implemented. Security has to provide sufficient protection, and be economically feasible to implement. Before designing information security for a system, it is important to know what the risks are, or in other words how risks in organizations are perceived. Therefore, risk perception becomes the key to designing and implementing security mechanisms in IS.

2.2.1 Risk

Douglas (1990, 1992) explains, "Risk refers to external dangers such as natural disasters and threatening behavior by enemies". Through the course of history, civilization introduced many new risks (Hadden, 1986). Trade societies and economic activity introduced what we now call business risk, safety risk, and investment risk depending on context; hence, risk may mean different things.

Vlek and Stallen (1981) give a more detailed definition of risk, claiming that risk can be measured. According to them, risk is the probability of a loss or the size of the possible loss. Therefore risk is a function, the product of probability and the size of loss. A common characteristic of the definitions provided by Vlek and Stallen is that they are context free; they refer only to abstract terms such as probability and loss designed for cross-situational generalization. It is an important question whether or not such a context-free approach has any psychological validity (Brehmer, 1987).

In sum, the term 'risk' refers to the threat of loss of an organizational asset, incorporating the asset's value, its vulnerabilities and the range of threats to that asset measured in terms of probability and impact (ASIS International, 2002; Visintine, 2003; Frosdick, 1997). Information security risk management is the process by which an organization's information assets are valued, vulnerabilities and threats are identified and the implementation and monitoring of the measures put in place to protect these assets (Whitman & Mattord, 2005). It is critical for organizations as it is the most effective and cost-efficient means by which organizations can implement adequate levels of security to protect their information assets and as it is risk that drives the organization's level of security that is put in place (Roper, 1999).

2.2.2 Risk Assessment

Analysis and assessment of risks has become the most important tool for designing security mechanisms since the feasibility of security mechanisms started to be questioned (Courtney, 1977; Fitzgerald, 1978). All security professionals use risk analysis to justify the cost of designing and implementing security on IS. Courtney (1977) and Fitzgerald (1978) first came up with risk analysis methods. However, there always exists the lack of ability to establish feedback regarding the effectiveness of the security mechanism; because IS security is a low priority of management until risks actually materializes (O'Mara, 1985).

The quantitative approaches to risk assessment have been criticized as it conveys little practical value in relation to one-off decisions. In one-off situations as potential loss (or gain) increases in absolute terms, people tend to avoid the risk and choose the status quo alternative (Higgins, 1990). Lichtenstein (1996) describes risk assessment in the development of information systems as a two-stage process. First, he talks about defining the scope of risk assessment, identifying the information resources and determining and prioritizing risks to these resources. Secondly, he discusses making decisions to control the risks; such as a decision to transfer a risk by implementing safeguards. Lichtenstein's research has revealed that, although each organization or institution chooses a different method for risk assessment prior to development of an information system, most use economic or statistical approaches. Most organizations use, with the exception of cost, qualitative rather than quantitative measures (Lichtenstein, 1996).

2.3 Risk Management Standards

In an effort to improve risk management practice, risk management Standards and information security risk management Guidelines have been produced. They aim to deliver a high-quality effective risk management process for organizations,(Waring & Glendon, 1998). The purpose behind the Standards and Guidelines is to act as a point of reference for risk management and risk assessment and make it suitable for most organizations. Normally, in a country, Standards and Guidelines share a common risk assessment methodology, incorporating context establishment, risk identification, risk analysis and risk evaluation.

2.3.1 Risk Management Standards Process for Risk Assessment

As outlined above, the general risk management Standards and information security risk management Guidelines share a common methodology for information security risk assessment, following a similar process. We define risk management and risk assessment based on the literature (Vlek and Stallen, 1981; Roper, 1999; Courtney, 1977; Fitzgerald, 1978) as the following:

- *Risk Management* refers to the overall process for establishing context, threat, asset, vulnerability identification, consequence and likelihood analysis, risk prioritization, risk control sourcing and implementation and monitoring, communication, maintenance and review functions.

- *Risk Assessment* concerns the process of establishing context, threat, asset, vulnerability identification, consequence & likelihood analysis, and risk prioritization.

The information security risk assessment process is a staged approach within information security risk management that aims to identify and prioritize information assets; the specific threats that the organization faces, the chance of these threats occurring and the impacts they will have on the business. Only when the output of the information security risk assessment process is correct, the information security risk management process is then able to implement effective control mechanisms against high-likelihood, high-consequence risks of the high-priority information assets in order to balance the costs of the controls with the level of security provided (Roper, 1999). The whole process contains four phases – establishment, risk identification, risk analysis, and risk evaluation (Figure 2).

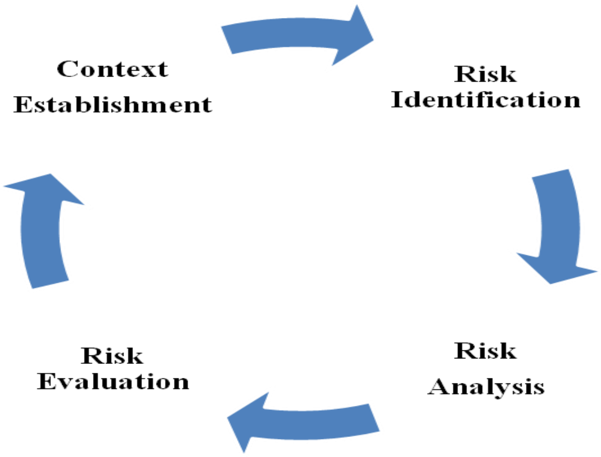

Figure 2: Risk management Standards process lifecycle
(Author's own interpretation: Halliday et al, 1996; Bandyopadhyay et al, 1999; ASIS International, 2002)

Context Establishment

The Standard process begins with context establishment, to outline the strategic context, organizational context and risk management context to ensure proper alignment with organizational strategy, objectives and goals. Here, the organization develops an understanding of itself to appreciate its own complexities and nuances that may influence their information security environment and requirements. This phase examines the organization to determine if there are any industry-specific risks and other issues that may be present that may impact the risk management process, or steer it down a particular path. Analyzing the organization ensures that the business environment is known to align organizational goals with the goals of the information security risk assessment and establish what risks may be present in each area of the organization to better scope and place boundaries on the risk management process to come (Halliday et al, 1996; Bandyopadhyay et al, 1999). It is also during the context establishment phase that risk evaluation criterion are outlined.

Risk Identification

Risk identification follows to identify information security risks by examining what can happen, how and why it can happen and what tools can be used to identify an organization's day-to-day operations through various information-gathering techniques such as brainstorming and interviews, (Frosdick, 1997).

Ideally, this phase should also integrate threat and vulnerability analysis of each asset to build as accurate a profile as possible on what may attack that asset, and through what security 'hole' (Visintine, 2003; ASIS International, 2002). A vulnerability is defined as being an inherent weakness in an information asset that can be exploited (e.g. an open port connected to the internet or the use of un-patched software) (Roper, 1999), whereas a threat is anything that can exploit that asset (e.g. viruses, Trojan Horses), hacking and human error (Visintine, 2003). The outcome of this phase is a list of threats to the information assets of the organization, given the vulnerabilities in the assets and controls already in place.

Risk Analysis

Risk analysis is the process by which the threats are measured in terms of consequence and likelihood (Roper, 1999). Organizations attempt to assign values to each threat, determining the probability of that threat occurring and if it were to occur, the impact that threat would have on that information asset, to create a risk. Control selection and implementation, monitoring and review of controls and risks and the communication activities with stakeholders are critical phases of the overarching risk management process in addition to the risk assessment process (Thorn, 2001; ASIS International, 2002; Visintine, 2003). This can be done through qualitative, quantitative or combined methods, using the knowledge and estimation powers of both the risk managers, key stakeholders and other sources of information (Visintine, 2003).

Qualitative approaches to this process use metric representations in order to establish a level of risk – 'high', 'medium' and 'low' are shown in Table 1 (Roper, 1999; Thorn, 2001). By using this matrix, a 'likely' probability and 'high' impact measurement result in an overall 'high' risk rating. Therefore, this particular information asset would most likely require protective measures installed to control that risk. However, if a particular threat was 'unlikely' to occur, even with a 'high' impact criticality rating, the threat is typically deemed as not being worth controlling (Roper, 1999).

Likelihood	Critical	High	Medium	Low
Almost certain	High	High	Medium	Low
Likely	High	High	Medium	Low
Moderate	High	High	Medium	Low
Unlikely	Low	Low	Low	Low

Table 1: Consequence and Likelihood Matrix
(Author's own creation: Roper, 1999; Thorn, 2001)

Quantitative approaches use statistical and mathematical formulas to determine the importance of each threat, including the Expected Value Analysis and Annualized Loss Expectancy methods that assign monetary values to each threat (Bandyopadhyay et al, 1999).

Risk Evaluation

Risk evaluation is the final phase, where the organization compares the result of the risk analysis with the risk evaluation criteria. Thus, organizational criticality ratings are assigned to outline the priority with which risks to treat immediately according to that set criteria, which risks can be treated at a later date, and which risks can be ignored. Once the evaluation is done, a new lifecycle of risk management Standard process will occur.

2.3.2 Issues in the Application of Risk Management Standards

Concerning risk management Standards and information security Guidelines, a problem with perception versus reality is evident; where having a general framework built from a general Standard/Policy is perceived as being useful for communication, easy to use and provides good outcomes for the organization. However, these perceptions might bring forth problems of inadequate guidance, granularity, complexity and misalignment of outcomes. Additionally, while organizations are becoming much more risk-aware, many large organizations still have not developed formal risk assessment methodologies despite the emergence of these Standards and Guidelines (KPMG, 2002). The Standards can be viewed as the 'criteria' for an information security risk assessment, they aim at improving communication and awareness among business units as reported, as well as a tool by information security staff to establish the need for information security risk assessments and the importance of information risks. Subjectivity concerns the problem of what to do when estimates are required, and how to interpret the Standards themselves to fit the organization's context and structure (Lichtenstein, 1996). The complexity of formal methodologies, including the Standards, stem from the enormity of the risk assessment process and the large organizations that most often use them (Halliday et al, 1996).

There are inherent issues in the use of baselines – Standards and Guidelines contain many hidden complexities and nuances that, whilst appearing user-friendly and simple on the surface, can actually confuse or overpower risk managers (Halliday et al, 1996). This is problematic – if organizations do not understand these complexities, a high level risk assessment process will be the result and specific assets and risks will not be identified, providing poor organizational information security. Standards and Guidelines also suffer from the problem of subjectivity (Lichtenstein, 1996) – not only constrained to phases of risk analysis, but also to the interpretation of the Standards and Guidelines themselves, and their translations to the organizational context.

In addition, the general risk management Standard process provides an organization with the base phases that can be effectively tailored to establish a core information security risk assessment process. However, the reality of this issue is quite different: not all organizations are always following that Standard process as intended in the context establishment and asset identification phases due to the level of knowledge the Standards require and the lack of guidance that the Standards provide of the application of its process. This means that it is left to the organization to decide the required detail for an effective analysis of their contexts, systems, assets and risks with little guidance. By not properly identifying the context of the organization in an information security risk assessment, improper alignment of the assessment's outcomes with organizational goals may result, such that the output of the information security risk assessment may actually conflict with the organization's strategic direction or its business objectives according to the information security risk management Guidelines (ASIS International, 2002).

In sum, the Standards must provide greater guidance for its users on these areas to ensure that its process is being accurately followed so that critical activities are done clearly and precisely to benefit the organization's information security risk assessment, and ultimately the organization itself. To establish that training and education programs, awareness and additional knowledge input from experts are required to assist organizations in translating the Standard processes to their organizational context is a must to solve this issue. Furthermore, as for the general risk management Standards, they should be more explicit on which areas of its methodology require a high level of granularity, and which areas may pass with a low level (ASIS International, 2002).

Due to the evidence that these issues exist and the lack of research and reporting on this area, an exploratory study is required to determin*e which problems actually manifest in industry, to understand what organizations believe about these Standards, how they are used and how successful they are at providing adequate information security coverage.* In this project, the focus is on the general risk Standards and Guidelines used in healthcare systems in the Southern Sweden Region Skåne.

3. Electronic Healthcare – eHealth

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 in the healthcare sector is important to be taken into account in order to achieve both patient safety and patient privacy (Utbult, 2004). Accessibility to the right patient information at the right time is a necessity in order to provide the best possible care for a patient. In this chapter, we will discuss the significance of information security in the healthcare domain, with focus on Swedish healthcare system and its development, problems & needs, and current solutions.

3.1 Information Security in Healthcare

Global and national healthcare is in a state of great alterations - economical and demographical conditions change rapidly and new forms of healthcare and medical technology are added continuously. Information in its different forms is a necessity for healthcare work, and security is an obvious requirement for almost every aspect of managing information. Patient information security demands should be the same regardless if the patient information is being managed by a computerized or non-computerized system. Even though healthcare is in this state of changes, computer technology's emergence in healthcare has been somewhat slow. This is because of the complexity of healthcare concerning different working forms and organizations, and in some ways because of the conservatism characterizing healthcare (Hälso- och sjukvårdsinstitutet 1998). Nevertheless, despite the problems and the afore-mentioned conservatism, it is vital to understand that opportunities offered by IT solutions are very important for healthcare; IT may improve and facilitate, for instance, documentation, information gathering and decision-making in healthcare. Another reason for the slow introduction of computer technology is the cost of IT investments. However, although IT investments are costly, IT- support will generate cost savings by providing more efficient work routines and information management, and it will increase the quality of healthcare (The Royal Society, 2006).

Achieving high quality is a keystone in healthcare and efforts must therefore be optimized and knowledge and information made available without organizational hindrance. This implies that that the right information must be available at the right level of care at the right time (Lagerlund 1999; SITHS, 1999). A description of SITHS ("Säker IT i Hälso- och Sjukvården" – "Secure IT in Healthcare) can be found at Carelink (2008), and is a basic service provided by Carelink aimed at ensuring patient security and helping healthcare personnel identify themselves when needed.

When documenting information in healthcare, it must be done to ensure quality; taking into account that healthcare is information-intensive. Some of the main reasons for malfunctioning IT systems are deficiencies in the staff's area of responsibility, organization, and knowledge. Analyses illustrate that the staff of an organization is in itself the biggest risk factor for incorrect management of IT systems and that the internal personnel commit the most security violations (Dahlin & Arnesjö 1996).

The amount of electronic personal health information that is created, stored and exchanged is growing in all segments of healthcare. The question is no longer whether health information will eventually be created, stored and communicated completely by electronic means. It will. Banks have been Internet-based for years, hospitals have started to add all patient journals as electronic journals, e-mails and servers contain tons of personal information and the question now is rather: How will we ensure the security of health information? The information should be protected first, and this calls for a common security framework. The Health Information Trust Alliance (HITrust), a health information security organization, is approaching this subject and is bringing together industry leaders who will shape the direction and establish such a common security framework (Roberts, 2008).

3.1.1 Purpose of Information Security in Healthcare

The main purpose of information security in healthcare is mainly to achieve two important aims: high-leveled patient safety and patient privacy. A high level of patient safety aims to provide patients with the best care with the right information at the right time. A high level of patient privacy is to protect sensitive patient information being distributed to unauthorized persons. Achieving both these aims simultaneously is difficult - often either one or the other aim is compromised (Utbult, 2004). Patient safety is more associated to availability and integrity, while patient privacy is related more to confidentiality and accountability. Investigations carried out by the Swedish Data Inspection Board (Datainspektionen, 1998; 2005) show deficiencies in how patient information is managed in healthcare (concerning patient privacy), arguing that there is a great need for further studies in this area. These relation boundaries are not static, but depend on each other. Therefore, a balance between the two connected aims is necessary when discussing work concerning information security in healthcare (Utbult, 2004). In fact, more and more patients receive care in their homes nowadays, which places higher requirements on coordination of care efforts between the caregivers for patient safety to be maintained (Utbult, 2004). Furthermore, work processes for planning healthcare that spans across several organizational borders must be analyzed before it is possible to identify how to establish and organize coordination within distributed healthcare (Perjons, 2005).

3.1.2 Information Security Problems and Needs in Healthcare

The importance of information security in healthcare is not something that came overnight; it has always been an important issue for the domain, in order to ensure that recorded patient information is correct as well as made available when needed. It is also important in ensuring that patient information is protected from unauthorized access to protect the patient privacy. The computerization of patient records has been a necessary step in order to achieve these important concepts. But, since the focus during this implementation has been on technology, the problems and risks of the management of patient information have not been addressed sufficiently. 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.

The healthcare domain has, with differing poignancy, always faced great challenges since it operates in a changing and demanding society and has a plethora of quality demands to live up to. When the information society evolved and the age of computerization began, these challenges were more prominent. Nevertheless, the computerization of patient records in healthcare has taken a long time to implement, as mentioned earlier. One reason for this is that patient information is sensitive and thus must be managed accordingly. Another reason is that demands on healthcare have increased due to patients being able to move around more and needing help regardless of where they are located and when they become ill. IT can be used to support information management in addressing these new requirements. However, the slow implementation of IT has meant that many healthcare units still keep patient record systems that do not communicate with other systems. 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.

3.1.3 System and Network Security in the Healthcare Domain

Today, healthcare organizations manage sensitive information in their computerized healthcare records. This change in healthcare has processed from manually managed to computerized patient records in the last decades. There are many advantages with computerized patient record systems. Van Bemmel and Musen (1997) mention advantages such as simultaneous access from multiple locations, legibility, variety of views on data, decision support etc. The aim of the security activity is usually to carry out a system and network analysis in the existing systems where the involved medical record systems and networks are analyzed from different security aspects. However, security issues have a high priority when patient information is to be exchanged between different care performers in the healthcare sector. For example, when the need for communication between different healthcare performers increases in order to improve the quality of patient care, the security requirements also increase both in digital medical records and network systems. Hence, it is important to preserve the rigorous security requirements of sensitive information, such as patient information, even in computer-based systems (Van Bemmel and Musen, 1997).

When information is exchanged between various care actors, the information becomes more dispersive. This creates new security demands, both technical and administrative, to be managed (Blobel, 1997). It is necessary to point out that the deficiencies found at the technical level must be considered a high security risk in healthcare and managing user accounts in a secure way must be of crucial importance for the reliability of healthcare when dealing with patient information: 1) variances in the level of information security of the different medical record systems and networks of the investigated healthcare organization are especially located in the medical record systems even if they also exist in the network system; 2) sensitive patient information is managed in the healthcare area and therefore it is important to implement a high level of security solution; based on different organizational and legal security frameworks (Blobel, 1997; Datainspektionen, 1998).

In the global sense, problems may arise in communication between people, between people and IT/ICT, and between the IT systems themselves (Kosanke, 2005). These communication issues exist on a national, regional and a 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 (Chen, 2003). Thus, interoperability and collaboration is not to be considered only an IT issue, but an organizational one as well. IT can help to appoint a process manager that follows patients when they move between different caregivers (Sågänger, 1998; Johannesson, 2005).

3.2 IT & Information Security in Swedish Healthcare System

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. Consequently, information security in the healthcare sector is important to be taken into account in order to achieve both patient safety and patient privacy (Utbult, 2004). Accessibility to the right patient information at the right time is a necessity in order to provide the best possible care for a patient. It is a complex undertaking since healthcare is increasingly characterized by diversity, distributed care givers, and extended use of IT.

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 (Denmark, Norway, Sweden, Finland and Iceland) 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 (Norden, 2005). When IT solutions are applied in healthcare, especially in a distributed way, information security is a critical issue (Ministry of Health and Social Affairs, 2006). 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 (Norden, 2005). 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 which he or she normally uses; while at the same time requiring, 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. To get a clear holistic view of a patient's health, relevant information about the patient must be available when needed (Carelink, 2001).

3.2.1 The Swedish Healthcare System

Healthcare in Sweden today faces several great challenges. One of these challenges is to ensure the collaboration of healthcare organizations to satisfy patient needs for a complete and continuous healthcare process that traverse the borders of more than one caregiver (Carelink, 2001; Johannesson, 2005). This challenge is currently being addressed within Swedish healthcare. The emerging need for interoperability not only stems from the patients, but also from healthcare staff that interact with patients on a daily basis (Blobel, 2001; Utbult, 2004). 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.

In 2003, Sweden was the only country in the world where more than five percent of the population was older than 80 years (Gurner, 2003). Because of people becoming older, the likelihood of suffering from chronic diseases increases. Many people also suffer from several different illnesses at the same time, which in Sweden is referred to as being "multi-sick". This concept is defined as patients having three or more diagnoses (Gurner, 2003). A related concept to "multi-sick" patients is the concept "multi-failing" patients; which according to the same source refers to persons with a fragile life situation, and thus need habitual reviews of the care efforts. The number of multi-failing people is much higher than the number of multi-sick ones and during the last three-four years of their lives, 70 % of the population suffers from some kind of physical dysfunction. The likelihood of needing much care in the final years thus increases as well (Gurner, 2003). Multi-sick individuals need care from not one, but several, caregivers, and diagnoses may imply that care is needed for a longer period of time. This affects all caregivers, and they must increasingly collaborate and coordinate their activities.

Sweden has a decentralized health care system, with 20 county councils and 290 municipal councils as principals and care providers. Their responsibility as principals includes the provision of adequate care services and the requirement to develop quality-assure and finance all care activities. Both county and municipal councils employ the services of private care providers to a greater or lesser extent. Patients can have contact with several hospitals, in different towns and county councils, while receiving care at home, or at private healthcare units. Under the terms of the *Health and Medical Services* Act, county councils are required to provide health and medical care of a high standard to all residents in the county. Health and medical care planning must be based on the inhabitants' care needs and include health and medical care services offered by private and other care providers. The act also requires municipal councils to offer health and medical care of a high standard to specific groups, including the elderly and the disabled. Since the 1992 *Ädel* reform, which made the municipalities responsible for long-term services and care for the elderly, many elder people are able to remain in their homes with support from the health and medical care and social services. The overall responsibility for Swedish healthcare rests with *the government* and *the Ministry of Health and Social Affairs*. Figure 3 shows an overview of distributed healthcare in Sweden, with the patient in the centre of the figure. Patients can have contact with several hospitals in different towns and county councils, while receiving care at home, or at private healthcare units (Figure 3). The figure includes Primary care, Secondary care, private care, and care carried out in people's homes.

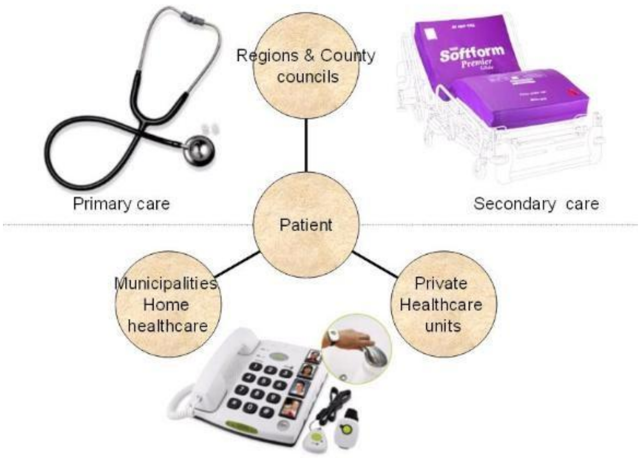

Figure 3: Distributed healthcare in Sweden
(Author's own creation)

Swedish healthcare is currently undergoing widespread changes. Healthcare is moving out from hospitals and is carried out in other forms and locations. Patients with complex care needs can, for instance, obtain extensive care activities in their own homes. They can have contact with several different healthcare providers, both within municipalities and county councils (distributed healthcare, shown in Figure 3). 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 (Datainspektionen, 2005). The National Board of Welfare (2004) 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 (National Board of Health and Welfare, 2004). 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 that county councils, in practice, have little or no control of who has access to information about patients (Datainspektionen, 2005). 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. Furthermore, the board claims that the healthcare providers must offer systematic measures in order to achieve sufficient routines for patient information exchange (National Board of Welfare, 2004).

In Region Skåne, much information on principles of securing information can be found in the Information Security Handbook (Informationssäkerhetshandboken, 2008), which is a regularly updated hand book only available online through the Regions' homepage. This hand book includes how to organize information security, how to control access and so forth.

3.2.2 Electronic Medical Records

The patient is the most important actor in healthcare and within healthcare, one of the more central units of information is the patient record. Patient records have traditionally been paper-based, and contain notes from doctors, nurses and other care providers. These notes can then be supplemented with other sources of data, including laboratory and other test results, such as X-rays, ultrasound and lung functions. The overall purpose of the patient record is to facilitate and support the provision of excellent and secure patient care (Dahlin & Arnesjö, 1996). This means, of course, that the recorded data must be available at the right time and place, while also being reliable. Dahlin and Arnesjö (1996) further describe patient record documentation as a "documentation wheel" with many spokes. This documentation wheel includes everything from registration of administrative patient-related information to pure medical data (anamnesis, status and diagnosis, for example). Everything that is documented into a patient record is supposed to be important information. This information must then be made available and be managed by a computerized record system. By doing this, electronic medical records are created. These will be referred to as EMR (EMR and EHR – Electronic Health Records, are considered to be the same thing in this report) from here on. The advantages of EMR, according to Dahlin and Arnesjö (1996) are, for instance: searchability, extensive availability, diverse presentation probabilities, a possibility for quality development and so on. In order to achieve and fulfill these advantages, a certain attitude is needed. Dahlin and Arnesjö (1996) argue that openness towards obtaining new technology is required and that information and information transition are standardized. Moreover, Dahlin and Arnesjö (1996) believe that EMR in future will become more user-friendly, useful and standardized.

Today, the use of EMR varies between different hospitals in Sweden. Research has shown that 95% of Primary Care has implemented EMR, but on the other hand, in 2006 only 55% of all medical prescriptions were sent electronically (Jerlvall and Pehrsson, 2006). Some hospitals have just started to introduce EMR while others are almost computerized with regard to patient record management. In 1998, the Swedish Data Inspection Board published a report about the processing of personal data in hospitals (Datainspektionen, 1998). In this report they provide recommendations concerning basic security measures on how to control personal data in healthcare, which include, among other, that the nursing staff must always be vigilant that the processing of sensitive personal data onto another national registration number does not occur and the patient's identity must always be ensured through some form of control checking. Based on 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 the organization.

Lagerlund (1999) argue that the users of systems constitute the biggest risk concerning information security in organizations. According to France (2001) most staff is not aware how to manage EMR and common information security problems when they arise, as they are affected when::

- *The login function does not work satisfactorily*, i.e. the login routine is not compatible to the users' way of working.
- *Users are not aware of or have inadequate knowledge of information security issues.*
- *They use the login and logoff routines of the system*, in order to support traceability.
- *Interruption to EMR occurs.*

Users can 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.. Users should have the right to training and information about routines in the organization concerning how to manage and check log files and also on what data is stored. Users are positive to having their work logged partly because they want patients' to trust them in the work they perform and partly for their own protection. This implies that users understand the reasons for logging information in healthcare (France, 2001).

Interruptions occurring in EMR availability convey more work for the users since they are forced to duplicate registrations of patient information. However, compared to paper based records, the users are more positive to EMR and the availability of patient information has improved. Furthermore, the management level also should pay attention whether simple and secure login and logoff techniques have been purchased and implemented in the organization or not. Datainspektionen (1998) states in their report that systems must not contribute to the unsuitable use of an authority control system by having slow and too complicated login and logoff procedures. In order for the users to understand the consequences of their own actions, it is necessary that appropriate security training and attention is implemented, thereby thus avoiding needless risks (Björner 2000). In order to preserve and reinforce patient confidence, healthcare should strive for security aware users.

3.2.3 Swedish laws and regulations affecting Swedish healthcare

Healthcare is controlled by a considerable number of acts, orders and statutes, which monitor healthcare and function in many ways as guides for healthcare work. Therefore, a brief description of the most important Swedish acts that cause an impact on the use of IT in healthcare is provided by the table below (Table 2).

Act	*Function*	*Description*
The Patient Record Act (SFS 1985:562)	Information recorded on paper form /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.
The Secrecy Act (SFS 1980:100)	Obligation to observe professional secrecy in public business and prohibit the distribution of public documents.	The primary purpose 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.
The Personal Data Act (SFS 1998:204)	Provisions to protect the personal integrity of people (patients in healthcare).	The Act, which is adapted to EU rules, applies to personal data that is transmitted, disseminated or made available by other means.
The Act on Healthcare Records (SFS 1998:544)	Care according to healthcare, dental care, psychiatric compulsion care, legal psychiatric care, and care in infection protection.	Data, 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.

Table 2: Healthcare Acts in Sweden
(Author's own creation)

A new Patient Record Act

In May 2008 a new patient record act was remitted by the Swedish government (Regeringen, 2008) and it was approved by the Swedish parliament on May 22nd. The main purpose of this new law, which will inure on the 1st of July 2008 thus replacing the old patient record act and the act on healthcare records, is to allow easier access to electronic journals for healthcare providers. The law will also provide smoother access to patient records for the patients themselves.

3.2.5 Current Information Security Solutions in Sweden

In Sweden, different projects have been conducted in order to find 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 (Ministry of Health and Social Affairs, 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 forth.

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 commendable and the work is proceeding in the right direction.

Sweden utilizes a personal number system, which assign every Swedish citizen his or her unique identification number. It is consequently much easier to be certain that the right patient is being treated. However, there can be problems with unique identifiers as well. 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 (e.g. car registry, social insurance register, tax registry). This is also the reason why many other countries do not use this type of identifier.

3.3 The patients' view of Information Security

The patient is the most important actor in healthcare. This implies that healthcare needs to operate so that it fulfills the requirements of good care, which is to provide patients with both patient safety and patient privacy. Furthermore, patients in the 21st century 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 therefore required and the need of information security in healthcare is evident. In our research, patients are excluded from interviews due to delimitations, but we still like to discuss their importance for information security in the healthcare domain.

According to the Swedish Health and Medical Service Act (SFS, 1982:763), the aim of healthcare is to supply citizens with good health. Health care has to be provided respecting the equality of human beings and the dignity of humans as individuals. Healthcare has to be operated so that it fulfills the requirements of good care (SFS, 1982:763). This implies that healthcare has to be of good quality, safe and secure for the patients, and easily accessible. Furthermore it must be 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 following consultation with the treated patients (SOU 2006:82). All this implies that healthcare works for the patient, and is thus the purpose of its aims. Hence, the healthcare sector has to provide patients with both *patient safety* and *patient privacy*. In order to fulfill these aims, good medical knowledge and good management of patient information is required.

Implementation of IT in healthcare has been relatively slow, but is at least walking the right path. Work for the future aims to involve IT as a support for good and efficient information management within healthcare. This is necessary, not least since patients may be required to visit more than one healthcare provider. A certain illness may necessitate visits to several different healthcare providers, which means that the patient information has to follow the patient's progress through the treatment (*the patient process*). Earlier research has shown significant deficiencies concerning information security when patient information has to be exchanged between different healthcare organizations (Åhlfeldt, 2006).

One main aim of healthcare, as mentioned above, is to achieve both patient security and patient privacy. According to Utbult (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. Patient security is harmed by lack of information. This 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. In addition, the aim of patient privacy is to protect sensitive patient information from being distributed to unauthorized persons.

With regard to the area of information security and its four characteristics (*Availability*, *Integrity*, *Confidentiality* and *Accountability*), patient safety is therefore related to availability and integrity. Patient information must be available and correct; the right information at the right time at the right place. 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.

3.4 Preparing for the future: a global and a national perspective

Healthcare systems of all developed countries face the challenge for improving quality, efficiency and safety of patients' care. For meeting this challenge, health is moving from being organization-centered to process-based care (Blobel, 2007). Healthcare will become increasingly focused on patients and the needs of the patients, as opposed to the needs of the service providers. Treatment can be provided closer to the patient's home. Healthcare will be integrated with other services, such as social care, with seamless multi-disciplinary services the main aim. Further on, the number of service providers will increase (The Royal Society, 2006).

The design of ICTs should be done by understanding the needs of healthcare professionals, patients and carers. Professionals and other users must be consulted and involved in implementation, and ICTs are likely to fail if their design is not based on how people work together. The iterative process is of special importance when handling large, complex systems such as healthcare systems; emerging ICTs should be designed with the will to experiment – try something, if it does not work, abandon the unsuccessful parts and try again. In short ICTs need to be flexible and easy to use but this must be weighed against privacy concerns. Confidentiality issues should not take time from the delivery of care. A second privacy concern is the balance between sharing personal data for societal benefits and the privacy of this data. To what degree are patients willing to share their personal data? This conflict must be solved before the full benefits of healthcare ICTs can be realized (The Royal Society, 2006). Those future plans goes in line with other researchers, for example Sausner (2007) who argue that it is of great importance that 'battle plans' are created before breaches in security occur.

3.4.1 The European Union's eHealth Action Plan

EU Information Society (*EUIS*) has announced that 'Healthcare systems are becoming increasingly dependent on Information and Communication Technologies (ICTs) to deliver top-quality care to European citizens' (European Commission, 2006). The EU's eHealth action plan sets out a clear road map for this sector. *EUIS* made an action plan with a string of targets which should be adopted by 2010, including remote access of patient journals. The European Commission is also promoting a greater awareness through an open and multi-stakeholder dialogue on a new IT security Strategy for Europe (eHealthNews, 2006). EU has allowed for EU citizens the right to seek treatment in another EU country.

Technology is advancing at a fast pace and changing the complexion of our daily lives. Healthcare systems become increasingly dependent on ICTs, because ICTs help doctors, pharmacists and hospitals deliver better quality and more efficient healthcare services to patients. This kind of healthcare service is called *eHealth* which facilitates access regardless of geographical location (e.g. doctors can access patients' medical records more easily, get immediate access to test results from the laboratory, and deliver prescriptions directly to pharmacists). Thanks to innovative telemedicine and personal health systems, heart-attack patients can carry monitors that alert their doctor once their condition changes. Furthermore, *eHealth* breaks down barriers, enabling health service providers from different Member Regions (within one country) and Member States (within one continent) to work more closely together. *eHealth systems* make it simpler to organize and carry out treatment abroad for particular patients. Rapid and reliable ICTs have become a vital component of efficient and effective 'health management systems'; *eHealth tools* (e.g. databases for patient records, mobile monitors which transmit data automatically, and handling systems for patient call centers) have been enabled to build as a strong base. If these systems are able to communicate with each other, the potential benefits they can bring to patients will increase significantly.

In a Union where citizens increasingly travel across borders, individuals should be able to find the highest standards of healthcare wherever they go. In 2004, *eHealth* policy was set out as a part of the *eHealth* action plan which covered everything from electronic prescriptions and health cards to new information systems that reduce waiting times and errors. The plan aims to bring national authorities closer together in order to move towards a *European eHealth Area*, in which the geographical location of an individual citizen has minimal impact on the quality of healthcare they receive (European Commission, 2006). The plan calls on Member States to develop tailored national and regional *eHealth* strategies to respond to their own specific needs. Through sharing ideas and experiences across Europe, all our citizens can benefit more rapidly from efficient and reliable *eHealth* systems. The plan sets out the steps needed for widespread adoption of *eHealth technologies* across the EU by 2010.

3.4.2 National Strategy for eHealth, Sweden

As mentioned above, a national strategy for *eHealth* has been conducted in Sweden. Six different organizations work together for the National Strategy; *Ministry of Health and Social Affairs, Swedish Association of Local Authorities and Regions, National Board of Health and Welfare, Medical Products Agency, National Corporation of Swedish Pharmacies and Carelink* (Ministry of Health and Social Affairs, 2006). The following section of information is derived from their work called *National Strategy for eHealth, Sweden* (2006). They argue that a common *eHealth* strategy offers numerous potential benefits in terms of improvements and greater efficiency for patients, health care professionals and decision-makers.

The National Strategy acknowledges the benefits that ICTs offer, and claims that a range of issues relating to ICTs must be addressed and solved at national level. These concerns should be dealt with on the basis of a common approach and the work is divided into six main areas of action: 1) Bringing laws and regulations into line with extended use of ICT, 2) Creating a common information structure, 3) Creating a common technical infrastructure, 4) Facilitating interoperable, supportive ICT systems, 5) Facilitating access to information across organizational boundaries and 6) Making information and services easily accessible to citizens.

The vision for the future is that citizens, patients and relatives will enjoy quick access to information with little trouble, regarding health issues and health status. Interoperable *eHealth* solutions that guarantee patient safety will be accessible for health and elderly care professionals. Citizens of the future will seek more individual, tailored solutions to health problem, and will more and more use the Internet to learn about health concerns. Citizens of the future will also use the Internet on an ever-increasing scale and therefore a national health portal should be created. Appointments will be done through such web portals or telephones and access to care will no longer be hampered by geographical or administrative boundaries. Prescriptions can be sent via this portal. Health care professionals will be able to access EMRs without being hampered by administration, health data registers will allow for anonymous use of EMR and for authorities to follow up on the quality of treatment. ICT systems will be easily accessed through single sign-on services. But, this future scenario will only be realized if ICT use is placed in a new operational perspective focused on the common need for secure, efficient and accessible care. The national strategy recognizes ICT as a versatile tool which offers many new possibilities and it will become increasingly more important in the future. Furthermore, they say that ICT use is insufficiently coordinated and has never been used to its full potential, which means that conditions must be created for ICT use in healthcare.

In different parts of Sweden, different projects have been undertaken. In Southern Sweden, a project called the Clinical Portal has started, which tries to integrate different healthcare systems using service-based platform architecture to create IT-support. The Clinical Portal includes services such as Care Survey, Important Medical Information and a Common Medicine List. Smart Cards must be used for authentication according to the Clinical Portal and all information passing through the Portal must be logged, enabling supervisors to see what kind of information has been sent to whom and when it is being sent (SOU, 2006:82). This does not, however, deal with the problems with unauthorized access from theft of Smart Cards or likewise.

What is common for these different projects is the need for a holistic view of information systems; not only including a cooperative infrastructure for information security, but also techniques concerning strong authentication as well as generic services (authorization, access controls, confidentiality and so on). Above all, it is necessary to point out the advantages in the long-term perspective (Carelink, 2003).

3.5 Security Policies in Other Business Areas: eHealth vs. eBanking

Information security in healthcare is still in its developing phases. Not long ago, all patient journals existed only in paper versions. These changes indicate that healthcare can (and should) learn from other businesses areas that have extensive experience in personal electronic information security. As Websense (2005) says: 'It has always been good business practice for companies the world over – whether in financial, educational, health care, business or retail organizations – to protect their customers' privacy and control access to sensitive information'. There is hence a need to emphasize security as a part of the whole business and not as an isolated phenomenon.

Most companies keep sensitive personal information in their files – names, Social Security numbers, credit card, or other account data – that identifies customers or employees (FTC, 2008). This information often is necessary to fill orders, meet payroll, or perform other necessary business functions. However, if sensitive data falls into the wrong hands, it can lead to fraud, identity theft, or similar harms. Electronic banking (*eBanking*) is a typical representative of such type of business. Both *eBanking* and *eHealth* involve important personal information transferring in their business environment. The definition of *eBanking* is the use of electronic delivery channels for banking products and services, and is a division of electronic finance (Schaechter, 2002).

eBanking is a typical example of a business area that handles large amounts of personal information electronically. Security is the primary factor that determines *eBanking* technology (Sudha, 2007). Moreover, banking businesses have learned that security solutions must not be built upon a single approach (for example only using biometrics as defense), but recognizes that security must be multi-factor and comprehensive (Markowitz, 2007). Of course, banks have problems of their own, for example, Websense (2005) states that 1 in 3 American companies have detected spyware on their network, 45% of businesses have reported unauthorized access by insiders and instant messaging services (IM) expose companies to security risks. According to Wah (1999), the success of banks operating via the Internet will lie in their ability to attract and keep customers. Banks have developed mechanisms over more than 30 years to deliver ubiquitous access to data with adequate security at reasonable costs (The Royal Society, 2006).The level of security and privacy associated with *eBanking* affects the acceptance and adoption of new innovation. The emergence and introduction of *eBanking* did not create inherently new risks, however: rather, it increased and modified some of the traditional risks associated with banking (Basel Committee, 2003). Banks are doing good job safeguarding digital information today, especially compared to other financial services (Bielski 2007), even though many problems still exist within *eBanking*.

With IT implementation into business, *eBanking* has gained much more experience than *eHealth* in the last decades. Not only because of the business history, but it is easier to manage client personal account information database as well. It involves less personal information in *eBanking* than in *eHealth* – personal information has been reduced to a Social Security Number (*SSN*) and a full name; transaction records appear to be simple with date/time, payment object, amount of the payment, and the remaining amount of money in the account. One person can hold more than one bank account in the same bank and it is common that he or she has bank accounts in other banks as well.

Additionally, due to the nature of *eBanking*, it provides more flexible access platforms to both personal clients and business clients. Clients are able to access via any computers from anywhere anytime with the Internet connection to launch *eBanking* services. This advantage is more obvious when the user makes international transactions (e.g. Visa, MasterCard) and cross-border payments. So far in *eHealth*, information is only accessible from certain places.

Conclusively, *eBanking* is, despite a high number of reported frauds and thefts, an area for *eHealth* to consider adapting techniques from. Both *eBanking* and *eHealth* handle personal information that must be protected, but banks have been able to protect personal information for a long while, and are always under pressure to provide customers with prominent and easy-to-understand advice on the importance of security precautions and personal information policies (Schaechter, 2002).

4. Method

In this chapter we present how our research was conducted. First we present our strategy for research, and we then present how the case study was conducted as well as a brief discussion on some ethical dimensions.

4.1 Methodology

Our research took a broad approach. We included 1) Information Security in general, 2) Risk management in general, 3) Information Security in healthcare and Information Security in Sweden & Skåne, 4) Investigation through a case study consisting of five interviews in healthcare in Region Skåne. This is a broad approach, but we wished to keep this since we believe that both healthcare and the area of information security suffer from narrow-minded thinking and lack of complete solutions to problems, and we believe that some of the areas in our approach are not covered enough.

Case studies allow individuals to gather data from a number of different sources within an organization, in order to triangulate all information and verify that the data received is correct (Yin, 2003). These data collection techniques include interviews, observation of people in their natural environment and document analysis. Our focus is on interviews. For the purposes of this research, the division of psychiatry and IT departments are selected as the targets for our interviews in this research. Five interviews with workers from three different job types were conducted, but several potential key members were excluded. These exclusions include patients, nurses, secretaries and so forth. The reasons for this are mainly that we suffer from lack of time as well as a risk of being even broader in our approach. The reason for choosing psychiatry as the division to investigate, is that we assume that psychiatric divisions handle more sensitive information than most other divisions (compare it to dental care, for instance).

We wished to record the interview in two ways; writing notes by hand and recording through a tape recorder. However, we were not able to assess any technical equipment such as recorders, and thus only regular notes were conducted. We planned the interview investigation having the whole process in mind, envisaging final report from the start. The plan for the interview investigation was in some ways created with Kvale's (1996) seven basic stages in mind (*Thematizing*, *Designing*, *Interviewing*, *Transcribing*, *Analyzing*, *Verifying* and *Reporting)*. We began by thematizing the investigation, where we acquired extensive knowledge on the topic, enabling us to know if the interview gives us new information, where we clarify the purpose of the study along with a definition of how we gather information and how we analyze it. We then designed the investigation, by considering the number of subjects (four to five, with at least three different roles in a hospital or healthcare management, including doctors, nurses and IT staff). We considered time and resources – we would need at least one hour for an interview to be meaningful. We also considered the ethical dimensions of the interview. When the actual interview took place, we needed to be aware that it is an interpersonal situation between two actors sharing a mutual interest on the research scheme. We prepared for the interview by creating an interview guide how to provide the interviewee with a context for the interview (briefing before and after the interview) as well as figuring out how to keep questions simple and dynamic, enabling a positive interaction with feedback and follow-up on questions.

When interviews were done, they needed to be transcribed. This is done by translating something from an oral language to written language. We wrote what our interview subjects said and kept every word to prepare the analysis phase. When transcribing the raw data from the interviews, we did it individually and then compared our transcriptions and finalized it into a third, common, transcription. In our next section, we describe how we got in contact with our research participants, as well as how we conducted our interviews.

4.2 The interviews

Face-to-face, one-on-one interviews with key personnel within an organization are the primary method for data-gathering in case studies and are essential sources of information (Kvale, 1996; Yin, 2003). These interviews ought to be recorded at the participant organizations with permission and transcribed to ensure a thorough analysis of all answers and that all relevant concepts could be brought to attention. Open-ended questions were asked from a structured series of questions, and allowed for follow-up discussions and probing queries to glean as much relevant and important information as possible.

Discourse is built on oral language, and for reports it is necessary to transcribe and transform the received information into written language (a written construction of an oral conversation). To simplify transcription, interviews need to be thoroughly recorded. This can be done with four different approaches; taking written notes, taking mental notes, record through a tape recorder and record through a video recorder. Tape recorders are very popular, but video recorders have the possibility of catching body language (and any other visual aspects) (Kvale, 1996). Unfortunately, for our work, only paper notes were conducted so we had to be more observant during our interviews.

4.2.1 Contacting Interviewees

When we began contacting potential interviewees the first initial contact was made with top management. We contacted top management in the psychiatry division to assess how to easily contact the healthcare personnel we were interested in interviewing. From these persons we received a few names and their e-mail addresses, why we promptly e-mailed them and introduced them to our research and asking them if they had time for an interview. For our first four e-mails, we only received two answers, and none of them had any opportunity to do an interview with us. But they provided us with more names, and eventually a director in the psychiatry division and one person responsible for information security responded positively to our wishes. Those two interviews were scheduled for and while planning these interviews, we got response from yet another IT employee. The third interview was scheduled right after the other one on, which was on May 9th. We conducted these interviews knowing we still wanted two more interviews (with doctors and/or nurses) why we arranged so that the Swedish-speaking half of our research team (two persons) could attend a doctor's meeting at BUP Lund (Child and youth psychiatry in Lund). This clinic was preferred as we were told that the doctor's working there were in general young. At this meeting, two more interview occasions were scheduled; both at Tuesday the 13th of May and the interviewees were doctors. Three of our interviews (the one with the one responsible for information security and the two interviews with doctors) were conducted in Swedish, following wishes from the interviewees, thus only allowing for one of us to attend, conduct and transcribe these interviews.

All the interviews were carried out at different hospital departments in Lund, belonging to UsiL ("Universitetssjukhuset i Lund" – "the University Hospital of Lund") and connected to either IT or the psychiatry division. Our initial plans to interview five persons with different jobs, was followed. We could, however, not use technical equipment such as tape recorders for our interviews since we could not obtain any. We don't believe this was a problem for our research, since we aimed at being very observant and accurate in our documentation of the interviews.

4.2.2 Conducting and Transcribing Interviews

As mentioned above, three of our interviews were conducted in Swedish and translated into English during transcription, while the other two were conducted in English. This could create problems, but the translations were done cautiously and were checked by neutral readers to make sure nothing went missing in the transcription. We took notes with pen and paper during the interviews, and these notes were later transcribed into the Interview Transcriptions (Appendix 4). Based on our transcribed interviews, we created our Interview Results (Chapter 5), which together with our literature review, form the basis for our discussion and conclusion chapters. All the interviews lasted around 60 minutes, which was the minimum time we wanted the interviews to last. We kept the interviews at such a pace so that we could take notes without hesitation, and ask again if something was unclear during the dialogue. In the interview results and transcriptions we mention Melior, which is the main software used for registering and maintenance of patient journals in the Region.

We began interviews by talking about the research in general, and we had our Interview proposal (Appendix 1) at hand. When the participants were well informed, we started the interviews with a background check – we wished to know what the interviewees' position in healthcare was as well as more specifically what they work with. Furthermore we wanted to find out how the process of employment was carried out when the interviewees were employed as well as how patients are identified in the organization. We then moved on to different questions for different job types. During the interviews with doctors we focused on computer experience, education in information security, information on laws and constitutions, transferring information between healthcare units, log-keeping and the actual computerized patient journal systems. When interviewing IT personnel we assumed that we did not need to ask about computer experience, instead asking about management of user registrations, authorization tools, and then log-keeping as well as focus on Melior. Finally, when interviewing the director of psychiatry (the Director) we asked about policies in the organization positive aspects and negative aspects regarding the work with information and patient security today and what requirements will be needed in the near future. All interviews were concluded with asking the interviewees where the main focal point should be in the near future, concerning patient security and safety, information security and so forth. After all questions were asked, we asked if the participants wished to remain anonymous in our report, but all participants turned down that offer, claiming that they had not said anything that could harm anyone. We tried to keep our questions on such a non-sensitive level so that we would provide truthful answers from them. In our interviews, we also showed the folders in Appendix 6, concerning secrecy, healthcare information and how personal records are managed in Region Skåne. This was done to clarify if they recognized the folders, in order to find out how much information is provided to personnel, concerning information security.

Regarding ethics, participation in our research was, of course, voluntary and we made sure of confirming informed consent from the participants, which was based upon the interviewees understanding and voluntary participation. We believe by acting good, honest and true, we gained integrity and trust in our research. Informed consent (Israel & Hay, 2006; Singer and Vinson, 2002) was gathered either orally or through e-mail contact. We also offered our participants the opportunity to be anonymous – the notion of confidentiality. This confidentiality is limited to the extent that we as researchers will still know the identity of the participants and if our supervisor wants to take part of our full material, the confidentiality could be breached. None of our participants wished to remain anonymous, however. This was rather surprising since we had the presumption that workers in healthcare would be more inclined than many other businesses to remain anonymous, put that was not the case. Our aim has been to act professionally all through the research. We believe that by telling everything exactly how we did it, we will remain more ethical. Also, by acting professionally, we hope that we have not harmed any future students' chances of doing similar research in the Region. With acting professionally we mean that we act professional during interviews, we receive informed consent, offer confidentiality, and present the purpose of our research as well as being well prepared.

The transcriptions were then done by writing from our written notes into computerized text format. The transcriptions were divided into the questions asked during interviews and the answers derived from them. All five transcriptions begin by presenting each interviewee and telling when we conducted the interviews.

5. Interview Results

The results from the interviews are divided into a few categories, which we believe summarize what we received from the interviews. The categories were created with our literature review in mind. These results are the important parts from our interview transcriptions (Appendix 4). The categories are *Patient and Personnel Privacy*, *Standards and Guidelines in Region Skåne*, *Electronic Medical Records*, *Accessibility and Availability of information, Cross-Border Healthcare*, and finally *Preparing for the Future*. The five interviewees will be referred to by using only a single word, in the result, discussion and conclusion chapters. The abbreviations are as follows (abbreviations are presented in the order that the interviewees are presented in the interview transcription appendix):

IT1 for the first interviewee (information security administrator), the *Director* for the second (management), *IT2* for the third (IT staff), *Doc1* (the first doctor) and finally *Doc2* (the second doctor). These abbreviations are obviously based on the title of our interviewees.

We conducted five interviews, with one person from top management in psychiatry, two persons from IT departments and two doctors working within psychiatry. They belong to several age groups, with the doctors being the youngest and the Director being the oldest. The doctors, being younger than our other participants, have not worked for more than a few years in the Region. The other three participants have worked for at least ten years. The reason for choosing younger doctors was mainly that they tend to work at several care units, thus receiving more insight from these units (and not only from a single care unit).

5.1 Patient and Personnel Privacy

The first focus in our interviews was to assess how new employees are identified and user accounts registered and managed, as well as how patients are identified within the organization. All our research participants remember signing an agreement (or employment contract) containing a limited amount of information on laws and such. Doc2 also mentions how she was interviewed by the director of the clinic:

> “I was first interviewed by the director of the clinic, where we discussed working conditions and employment contracts.”

Many new employees also receive Smart Cards, which are used for login and digital signing purposes. In order to receive Smart Cards, certificates must be signed and then a process begins, as IT2 says:

> “This information …is sent to SITHS, who supply employees with certificates. These certificates are proof that the employee works within healthcare and that his or her work will be conducted at a certain place in a certain way.”

When this certificate is received, Smart Card may be handed out to employees. These smart cards contain two keys; one for login to computers and for one digital signatures (signing e-mails or entries into journal records). Furthermore, these Smart Cards can be used to obtain certain ‘electronic tickets’ which are used to gain access to e-mail, Melior, the Intranet from your home or gain access to rooms or corridors. Not every employee has these Smart Cards; instead, several units have other access cards which might only function as access cards for buildings. One of our interviewees expressed positive feelings about receiving such a card:

> “A Smart Card for login, thus not forcing personnel to remember five different passwords that must be changed all the time, would be preferable.“

When it comes to identifying patients, these questions was asked only to the doctors and their replies were alike with Doc1 saying:

> "When patients arrive for the first time, they have to show ID to the nurse or maybe the secretary."

And Doc2 says that:

> "When patient first arrives, nurses check their ID as well as their parents, and after that they are considered to be the persons they say they are."

Contacts with patients are done by either meeting them or talking to them over phone. If patients send e-mails, they are not to be replied to unless a certain agreement has been carried out with that particular patient about keeping e-mail contact. When patients are identified and a preliminary assessment on needed treatment has been carried out, healthcare personnel are obliged by Swedish laws to put this information into a patient journal. If a journal does not exist, a new one is created.

We tried to gather information on how much information was handed to new employees, and therefore we brought a few folders to the interviews (Appendix 6) asking if they recognized them. Only two of the interviewees recognized any of those three folders, and it was the same one concerning secrecy and duty to keep secret. Director mentions that (the yellow brochure concerns secrecy):

> "The yellow brochure is a much discussed one, concerning what should and should not be included as well as on what is secrecy now that the Region is "one secrecy area"."

That Region Skåne is considered one secrecy area, is a notion that is mentioned by several of our interviewees. This work, along with the ambition of "one patient – one journal" is two concepts that show the ambitions of common journal systems, common principles and common working routines in order to provide better, more efficient care. Concerning the Region as one secrecy area, this implies that all information, even sensitive information (such as information on sexually transmitted diseases) which was earlier regarded as individual secrecy areas, are now involved into one journal ("one patient – one journal") with possible access for most healthcare personnel in the Region.

5.2 Standards and Guidelines in Region Skåne

We wished to assess what kind of standards, guidelines, rules, laws and constitutions are followed within the region, how they are presented to employees and how they are updated and managed. Mainly, these standards and guidelines were difficult to generalize, due to the fact that Region Skåne is a multi-layered region and the fact that the Region serves under national laws and constitutions. Therefore, few standards and guidelines were found within each unit or clinic. The Director explains the different layers:

> "The university hospitals in Lund could be said to consist of four different levels; 1) the Region (Region Skåne), 2) UsiL (the University hospital of Lund), 3), Psychiatry division (in this case; other divisions in other cases) and 4) the clinics. This implies that on level 1 – the Region – policies are created which every unit must follow, and in UsiL yet other policies are created. Furthermore, in psychiatry, some certain policies must be followed, but they are still not created by the actual division. Information security guidelines and principles are mainly constituted in level 1."

This means that the Region creates overruling guidelines, and some guidelines are created which are valid only within UsiL. Within the psychiatry division ('level 3'), some certain policies exist. It is difficult for clinics to create their own policies, as they are guided by both regional and national laws and constitutions. The entire region is 'monitored' by laws and constitutions which state how healthcare should act in most cases. The Director mentions that it is not easy to create your own policies or guidelines, when attempting outside the Region (or, more specifically, inside certain clinics or divisions).

When it comes to how employees are informed on standards, laws and such, we found that not much information is provided continually. As Doc1 mentions:

> "No particular information is received except for the information that is embedded into education and work."

Since information is not received in abundance in their work, employees might be inclined to search for information themselves. As Doc2 says.

> "I believe that we have to find most information for ourselves, for instance by reading doctor's magazines such as Läkartidningen or by connecting to the Intranet skane.se."

Although that much information is not received by personnel, this fact does not seem to pose a large problem for the workers. In part because not many major changes have occurred the last few years, which would force management and such to inform employees on these changes. However, employees have some problems with exactly how laws and constitutions are conducted and written which can be read about in "Preparing for the future" later in this chapter.

5.3 Electronic Medical Records

It is obvious that Region Skåne has not reached a point where only one patient journal system is in use. In Skåne, one electronic patient journal system is used more than any other; Melior. However, the Region does not solely use Melior, as the Director says:

> "The aim in the project Region Skåne to create a unified medical database enhances the possibility to provide patients with more effective and 'right' treatment. When the project started in the late '90s, different departments used different systems; up to eight or ten different systems were detected in Lund. This was, of course, a major problem. Patient information could not be transferred between systems because systems were not compatible with each other."

The Region strives towards "one patient – one journal" and this would in some way imply that only one journal system should be in use. With the Region considered as one secrecy area, a unified journal system would be a way to enhance this. But working towards a single, common system might not be entirely a positive target, as IT1 states:

> "If we only had one system, the owner of the system would have too much power. If we only use Melior for example, then Siemens would have all the 'power' concerning patient journal systems in the Region."

Within the division of psychiatry in Region Skåne all care units are working with Melior. Other divisions, such as primary care, use different journal systems. Some departments do not even need such journal systems, such as dental care as they only handle a small amount of information. When changes are wished for in the Melior systems, for example a function that users wish that it was added, a complicated process emerges. If a certain issue (question) is raised concerning the functionality of the system, the following process emerges, as the Director says:

> "Yes, they can be changed, but a difficult process emerges when updates or changes to the software are wished for. This is mainly because the software Melior is owned by Siemens in Germany. First a question might be asked to a department within Region Skåne, then these questions move on to the entire Region, then to discussions for Sweden in Stockholm, and furthermore it could be sent to Germany. Upon reaching Germany, questions from other countries are also added, and in the end Siemens might consider the original questions. So changes are difficult, thus forcing Region Skåne to adapt to the system, instead of adapting the system to the Region."

Regarding the more technical parts of the system Melior concerning access, we asked those questions mainly to IT1 as IT2 was not involved in any work regarding that. IT1 says, concerning access controls:

> "Only the information that treating personnel need for the health care should be available to, or rather, handled by the personnel…. Access can be controlled, however, for example … a doctor might wish to see a certain patient journal and therefore calls, stating his business. The doctor may then be allowed, for a predefined amount of time, to have access to needed information."

Doctors are therefore allowed certain access and are allowed to perform almost any function in Melior (read, write, delete, change, print etc.), and nurses and secretaries also have access to patient journals. The actual patients may have access to information in their own journals and are also allowed to complain if they find any information in the journals which should not be there. IT2 says:

> "Patients can also gain access to parts of their journals… When patients wish for information to be changed in their journals, they should contact Patientnämnden and explain to them their issues with the recorded information."

The will of the patient must remain in the forefront. If any information is found to be meaningless, threatening or otherwise harmful to patients, it should be removed or changed. It is important to focus on exactly what relevant information is. Patients must also have access to their own records, as Doc1 says:

> "Patients are allowed access to the information they ask for."

Regarding user education in the Melior system, we found that not much education was practiced in the Region. Some participants wished for more education, while some said that there exists an over-reliance on the notion of education. IT1 claims that "There is an overreliance on education and we should instead focus on why people act the way they do".

Regarding education in the systems, Doc2 had received some education in using Melior functions, but not recently, saying that:

> "I received some education in my former employment in Hässleholm, but have not received any since arriving in Lund. "

And Doc1 mentions that:

> "We had one occasion of Melior training during our medical education, but none since I started working in the Region. This implies that knowledge is missing with many healthcare workers, for example secretaries"

Education in computer training has not been any specific inclusions in the work of doctors, but has rather been embedded into the medical training. Computers are used a lot in the medical training and are an integral part of becoming a doctor. But when it comes to different job types, for example secretaries, they might benefit from more education in computers or certain systems. But as IT1 mentions, there exist an over-reliance on education and we should instead:

> "… focus on creating such simple systems that no real education is ever needed for user to do their work efficiently".

We did not receive any specific details on any other electronic patient journal systems, mainly because Melior is the dominant system in psychiatry. Other software includes Pasis / Prima and KundRad, which are used for remittances and other patient-related purposes. There even exist homemade solutions, as IT1 states it:

> "Some healthcare units have created their own, tailored, systems for handling patient information. This might work wonderfully for that particular unit, but is not compatible with other systems or might be too dependent on the creator of the system: what happens if he or she quits? This programs could be created in Microsoft Excel or likewise".

Obviously, these solutions are not preferred, even if they work well, since they are too creator-dependent and they are not compatible with other systems (according to IT1).

5.4 Accessibility and Availability of information – the printing of documents

It was evident during our interviews that despite all journals being transferred to electronic systems, a plethora of documents, records and e-mails are still printed back into paper-based form. People are not satisfied with having information available only in electronic form. Apart from patient journals, the Information Security Hand book (mentioned in chapter 3) is something that is also printed; the hand book is only updated online and if you print it, you might forget important updates unless you print new versions regularly (IT1 works with revising and updating this hand book). Several of our participants perceived printing as a problem, and provided us with both reasons for it and solutions to it. Doc1 provides us with two reasons for why personnel print patient records:

> "Since you have no opportunity of simple browsing in Melior, many might feel the need to print records instead of reading them on the screen… Printed records are supposed to enter the shredder after we finish working with them… Another problem is that you cannot have several documents open at the same time within Melior… which also might make people consider printing records to simplify their work. "

Another reason to print would be to print parts of journals in order to discuss a patient with other treating personnel, instead of being forced to sit in front of a computer screen and discuss it. After the discussion, the paper must be destroyed. When it comes to how to prevent records from being printed, thus creating a major risk that papers are left in offices or on tables and therefore become visible to unauthorized persons, two of our interviewees mentioned that printing access should be removed and the actual printer could be removed from the office for a week or so, thus forcing personnel to work solely with computer-based records. IT1 states:

> "Maybe we should try to remove the printer from work for one week, and see how much it is actually missed. I have suggested this at work, but so far not received enough positive response to actually do it. "

IT2 goes one step further, claiming that "patient journals should not be allowed to be printed at all". It is also obvious that all our interviews prefer electronic-based journals with most of them expressing positive comments about it. The Director says this on increased accessibility with electronic records:

> "Doctors are able to find out what they want to know about a patient quickly and easily. Patients might also have easier access to their own records".

Doc1 says that "…electronic patient journals are way more preferable than paper based journals. ", while Doc2 mentions:

> "I think that using computer-based systems is much better… since information does not disappear… with paper-based journals, a piece of paper could easily go missing. "

But, our interviewees express fears that this availability for personnel potentially makes the information more available to unauthorized persons. All that is needed is a password, they say. A big difference between electronic and paper based journals, as the Director says, is:

> "…paper based journals… only existed at one place in the world… electronic journals, they can exist anywhere… which creates the problem that many people can have access to information that they are not allowed to access".

Controlling access is done either via Smart Cards, which contain information on the user's identity and role, or afterwards via log controls. Everything that any employee in Region Skåne does, concerning computers, is logged and kept in a record. These logs can be assessed either if patients are worried or if scheduled controls are done, as IT1 says:

> "It is necessary for nervous patients to assure that no unauthorized personnel read their journals. I receive phone calls from concerned patients asking to check the logs".

And as the Director says:

> "…logs are checked on a random basis, where we select a random sample of patient journals to see if any suspicious access has occurred".

Not all personnel believe logging to be a totally positive experience, however. Doc2 expresses positive opinions:

> "… my work is being logged. I think this is good, especially from the point of view of patient security".

While Doc1 thinks that "it is sad that we need to be logged, although it might be needed". Since all work is being logged, and user accounts are connected to identities, and Smart Cards are also identity-connected, it is rather simple to look up who actually did what. Despite the fears raised by personnel, none of the doctors had actually experienced any unauthorized access. As long as people are honest, the rules that exist today pose no problems. Doc1 mentions that:

> "There is a large responsibility on individuals not to provide others with log-in information or printed records".

This implies that, despite the fact that many actually print journal records, few have actually experienced this as a problem in their work. Personnel might be careless with leaving information visible, but have not experienced unauthorized people reading it.

5.5 Cross-border Healthcare

The ambition to provide good cross-border (or distributed) healthcare is evident in the Region. The project Region Skåne is in itself a proof of this. The project aims at having unified medical database and is, as mentioned earlier, considered one secrecy area. The Director talks about the Region and early problems during its implementation:

> "The aim in the project Region Skåne is to create a unified medical database enhances the possibility to provide patients with more effective and 'right' treatment. When the project started in the late '90s, different departments used different systems; up to eight or ten different systems were detected in Lund. This was, of course, a major problem. Patient information could not be transferred between systems because systems were not compatible with each other"

Our impression is that these early problems are far from addressed. However, information is sent between units faster and more often today. Our interviewees mention that patient information is only sent via phone calls or through the patient journal system (Melior). When information is sent through Melior, a Bevakningssystem (monitoring system) is used. As Doc1 and Doc2 explains:

> "…we can send information on a certain patient to another doctor or nurse at another care unit, containing information on measures that need to be carried out regarding that particular patient. This provides a good overview… "Bevakningssystem" can function as an aide-mémoire with several patients included."

> "The problem with using this is that sometimes you can have too much information in that system, although the system itself works well… "Bevakningssystem" is pretty well protected, since you can specify to whom the information will be sent."

There is a need for greater focus on enabling cross-border healthcare. Information should be made available cross countries, and not only regions. Information within the Region Skåne is accessible today in many ways (a unified journal system is realized within the psychiatry division, for instance) but cross-region access in Sweden is not realized yet. The Director says that the ambition is to realize this within five years. But focus must also be on making information available outside Sweden. As the Director says:

> "We also need further focus on cross-border healthcare, allowing patients residing in Sweden but being on vacation on, for instance, Hawaii to receive proper treatment based on parts of their journals being accessible for the Hawaiian hospital."

This implies that maybe not all information should be available to foreign hospitals, but at least enough information to provide good care to patients.

5.6 Preparing for the Future

Finally, we turn our focus to what the interviewees believe to be the most important things to focus on for the future, concerning healthcare in Skåne and Sweden. We found that our participants had somewhat differing opinions on what is the most important aspect to focus on. The most unified opinions were on accessibility and information relevance. The doctors wished for even more accessibility on information in order to carry out proper treatment. Some of our interviewees also expressed concerns on relevant information – there is a need to focus on what is relevant information in journal records, and what is not. Relevant information is important, allowing treating personnel to more easily find needed information. Doc1 says that it "is not lucid what relevant information in patient journals is" claiming that some people write too much information, and furthermore, people do not use the same language when writing. The Director argues that:

> "We must focus on what is relevant information and what is not… Socialstyrelsen might benefit from being less unclear when telling how patient journals should be written, instead of providing negative feedback on already created journals"

Socialstyrelsen, the Social Welfare Agency, provide rules and guidelines on how to conduct patient records.

Furthermore, regarding accessibility, we perceived a desire for more access to information and more correct information in journals, and also more information from other care units and divisions. Smart Cards are one way to achieve this safely. Doc2 argues that:

> "…we could benefit a lot from having information from primary care in our journals… I want more accessibility, and this will in the end be more secure for patients, as we can provide good care to them by using the correct information on medical treatment"

The next concept for the future is the conflict between keeping information secure and providing enough access to key members of healthcare. Our participants were rather clear on this matter, with IT1 saying:

> "The first thing would be to shift focus from "securing the information" to make information "easily available for those in need of it". Sometimes there is too much attention drawn to protecting measure and ease-of-use while accessibility is put into the shadows"

And Doc2 claims that:

> "In some ways, I believe that correct information should overrule protection. As a doctor, it will be easier to provide good healthcare if the right information is available for me"

Moreover, Doc1 also agrees on this concept, saying that:

> "I wish for even more access to patient information… This implies less focus on securing the information and more focus on providing the right people with right access to the right information when needed. A discussion on the conflict regarding what information and patient security really is should be focused on. Is it to protect information at all costs or making sure that patients are not harmed by the use of information? It might be more secure for a patient if all information about him or her is available to treating personnel."

It is evident that our participants wish for more focus on accessibility rather than more focus on information security. They argue that, in the long run, it will be safer for patients if information is made available. Of course, proper measures must be carried to ensure that unauthorized access does not occur. We should focus less on education and more on why people act the way they do. Why do people print electronic records? Something that is mentioned, concerning education and printing, is that this could be solved after newer generations take over totally in healthcare. As IT1 says:

> "It's not as much about education as it is about what you're used to: young people bring their laptops everywhere"

And Doc1 also mentions the generation gap:

> "…the generation gap plays a big part in differences and attitudes in computer and software knowledge usage".

One way to achieve more accessibility, and simplify the creation and writing of journals that is desired by our participants, is updates to existing technique. There is a lack of proper functions in Melior and systems should be so simple that no real education is ever needed. By updating some functions in Melior, for instance, as Doc1 wishes for, the number of printed records could decrease:

> "…only one document is allowed to be open simultaneously… This should be changed in Melior"

IT2 goes one step further, as mentioned earlier:

> "Maybe disallow printing on certain information would be a good idea".

The most common, and important, notion that all participants seem to agree on is that it is important to provide good care to patients. In addition, web-based standards for patient journals in the near future are also discussed by the Director and IT1 (claiming that we are half-way there), with IT1 comparing this development to the banking industry:

> "Banks have, on the other hand, been able to handle personal information for years online… Hopefully, healthcare information is of less information for thieves, crackers and likewise… What should be considered a risk here is the possibility of sabotage and manipulation of sensitive data".

Overall, our participants perceived the future focus somewhat differently; doctors were more focused on more accessibility and relevant information, while IT personnel focused more on disallowing printing and simplifying access. The Director had opinions that resembled both IT personnel and the doctors as he wished for easier access, more access and focus on relevant information.

6. Discussion

This chapter provides extended and synthesized explanations based on the findings of our literature review (Chapter 2 & 3) and case studies based on our method (Chapter 4 & 5). The perceptions of information security in healthcare will be presented, and *eBanking* will be discussed to figure out the similarity and comparison with *eHealth* in terms of personal information security policy. Moreover, the directions for future research and important aspects to focus on for the future will be addressed as well.

6.1 Information Security Risk Management issues found in the case study

The first presented problem when attempting to assess Information Security Risk Management issues in healthcare, and therefore also standards, guidelines, principles and such, is that healthcare in Skåne and Sweden is multi-layered. The nation of Sweden is obviously the top layer, and within Region Skåne, at least four layers can be found; the Region, hospitals in Lund (UsiL), divisions (such as psychiatry division) and finally the clinics. This implies that some standards exist on a national level, mainly based on laws and constitutions (or the actual laws and constitutions) such as Patientjournallagen. Furthermore, the Region, as it is considered one secrecy area, needs to maintain its own principles for healthcare work. Then within each division, different information to handle and different treatment to provide creates the need for different policies, while some clinics might even create their own principles. But, mainly, healthcare is defined and monitored by Swedish laws and governmental institutions (such as the Ministry of Health and Social Affairs and The National Board of Welfare). Information on these standards, guidelines, laws and so forth, are obviously not presented in abundance to healthcare personnel; much information might be looked up individually by, for instance, doctors or nurses in magazines or the Intranet (skane.se). A reason for the lack of information provided to personnel is that not many major changes have occurred in the last years within the Region, which would create the need for much information to be provided. Despite the lack of information, this does not seem to pose major problems in healthcare. But this might become a major problem in the future.

Standards on patient identification are not that complex. The only real patient identification that occurs is when patients first arrive at a healthcare unit, where patients ID is checked (along with the parents', if they are there as well), and patients are then considered to be the person they claim to be. No contacts with patients are done through e-mails, and if patients send e-mails without certain agreement, treating personnel are obliged not to answer these e-mails. But no further principles for ensuring that patients are who they say they are exist in the psychiatry division, which provides no safety net should identity theft occur.

6.2 Information Security Problems & Needs in Healthcare

Today, for employees in healthcare, information is available quicker and easier by means of modern IT; but IT use also involves new demands on information security awareness (The Royal Society, 2006). It is obvious, from different sources and earlier work in this area (Lagerlund, 1999; Åhlfeldt, 2006) that user behavior is one of the most important reasons for the present shortcomings of information security. Nowadays, it is quite common that different caregivers are involved with different types of diseases and disabilities, treating multi-sick patients. Consequently, patients are transferred between organizations, thus forming cross-border (or distributed) healthcare. These caregivers do not currently collaborate to a satisfactory degree, which results in patients suffering from the lack of coordination and proper treatment.

It is thus important to analyze the work process for healthcare planning that spans across several healthcare borders.

A number of problems and needs were identified in our case study. The first one is a lack of education and lack of knowledge in certain areas in the Region; there is not much education on information security, nor is there any extensive education on electronic patient journal systems. This creates the problems that many healthcare practitioners lack the proper knowledge to work properly with patient information and information security. Secretaries are a job category that might benefit from more education in work. On the other hand, another perceived problem is that there is too much reliance on education. As IT1 said in our interview

> "There is an overreliance on education and we should instead focus on why people act the way they do… (*and*) on creating such simple systems that no real education is ever needed"

The way people act includes printing a plethora of electronic documents into paper format, which does not go hand in hand with the notions of "one secrecy area" and "one patient - one journal". Personnel print too much patient records and e-mails which are left visible to others. Our results show a wish to prevent personnel from printing altogether, or for a limited time, thus forcing healthcare personnel to work with the information by using computers solely.

Furthermore, the ambition to have a unified system in Skåne is far from realized. The aim in the Region is

> "…to create a unified medical database… to provide patients with more effective and 'right' treatment.", as the Director mentioned.

Within the psychiatry division, this ambition is realized (through Melior), but other units and divisions, such as primary care, use a totally different system. Some departments might even use more than one system, and most different systems are not compatible with each other. The existing systems are not working according to laws in Sweden, as they allow more access than some personnel is actually allowed. Access control can be managed through Smart Cards while access can be controlled at a later stage through log controls, but this does not prevent identity-theft or the use of stolen logins. As Doc1 mentioned:

> "All that is needed to access a journal is a valid login, which is bad for security"

Some parts in security might never be totally solved (such as preventing someone from stealing your wallet, thus stealing your Smart Card), which puts a major responsibility on individuals to protect their information and identity, which brings us back to the notion that the users might be the most important area for improvement in healthcare.

6.3 Preparing for the Future

Regarding what we should focus on for the future of healthcare, several key issues arose during our case study. These includes focus on what is relevant information in patient journals, more accessibility to needed information for treating personnel, better software and more unified Software for healthcare. the first one, relevant information, concerns exactly what information should be included into patient journals and that the work of Socialstyrelsen (who decides how patient journals should be written) would benefit from more clarification on journal creation. The main arguments for keeping relevant information are that information will be easier to find, and only information that enhances treatment will be included. These reasons are straightforward and valid. Moreover, it is of great importance to make relevant information available to those in need of it (providing the right access to the right person when needed). Today, there is too much focus on information security and we should, as IT1 say:

> "…shift focus from "securing the information" to make information "easily available for those in need of it". Sometimes there is too much attention drawn to protecting measure"

To enable better availability, however, security measures need still be carried out, and IT utilization must be improved, compared to today. One part of this is to create simple, efficient systems (Not only journal systems) so that no real education is needed in order to use the system.

In addition, web-based standards for patient journals in the near future are also discussed by the Director and IT1 with IT1 comparing this development to the banking industry:

> "Banks have, on the other hand, been able to handle personal information for years online… Hopefully, healthcare information is of less information for thieves, crackers and likewise".

Citizens have used electronic banking systems for years, and bank information is extremely attractive to thieves. It is perceived that healthcare information should not be as attractive as banking information. Banks (and therefore *eBanking*) will be discussed in the next section.

Overall, our participants perceived the future focus somewhat differently; doctors were more focused on more accessibility and relevant information, while IT personnel focused more on disallowing printing and simplifying access. The Director from management had opinions that resembled both IT personnel and doctors. It is highly likely that the future will consist of web-based solutions, either through Intranet connections, common databases or so forth. This will create even more accessibility and security issues in healthcare.

The most common, and important, notion that all participants seem to agree on is that it is highly important to provide good care to patients.

6.4 Comparative approach

Apparently, several findings in the literature review and the case study resemble each other, while some findings show the differences between theory and practice. We outlined some concepts in our literature review and aimed at aligning these concepts in the interview results as well. We begin by presenting some similarities and then move to differences and what we believe to be the reasons to these differences. We have also included some references for the discussed topics. The section is finalized by a brief discussion on what the field can learn from other business areas and a look on problems and needs from both technical and administrative security level (see Chapter 2, Information Security Model and SIS, 2003).

Similarities

The first major common topic between theory and practice is the notion that the right information must be made available to the right person when and where needed (see Lagerlund, 1999; Utbult, 2004 and Doc1 & Doc2 in the Interview Results). This goes hand in hand with the notion that the main aim of Swedish healthcare is to provide good healthcare to citizens (SFS, 1982:763 and Doc1 & Doc2 in the Interview Results). To provide good care, not only the proper equipment and competent personnel is needed, but also the right information concerning medication, treatment and such. SITHS (1999) summarized information requirements as "the right information to the right person in the right time and at the right place), which is meant less as definition, and more as a vision. This vision is, however, something that our research participants evidently wish to be more realized in the future.

Another common topic is the vision of cross-border healthcare, allowing information on residents in Sweden (for instance) to be accessed from anywhere (see Dwivedi, 2003); first in Sweden, and then realizing this on a global. This is shown in the literature by, for instance, the *eHealth* action plan and the national strategy for *eHealth*, Sweden. To realize this, the vision of "one patient – one journal" must be fully developed, and more common systems for keeping computerized records must be realized in healthcare. But, when realizing this, we should be aware that owners of electronic systems should not be given too much power by being the only provider of certain systems.

The laws presented in Chapter 3, are fully embedded into Swedish healthcare, guiding and monitoring it. However, our case study shows that these laws are not always clear on certain topics, for example on exactly how patient journals should be conducted (the Director in Interview Results, for example). The education and knowledge of personnel is not always satisfactory, which is showed by both our case study and for example France (2001) in our literature review.

Differences

Contrary to much written literature, our research participants wished for less focus on information security and more focus on providing the right access to the right information. Focus on securing the information has been pointed out by, among others, The Royal Society (2006) and Websense (2005). According to our participants, we should shift focus to making information available for those in need of, which of course implies some focus on preventing unauthorized access. Unauthorized access was something that none of our research participants had experienced as a major problem (mainly because unauthorized almost never occurred in the Region, according to the case study), which mean that there is a valid reason for participants to claim we should keep less focus on security.

Furthermore, there exist a number of standards, guidelines and principles in healthcare. But these are not always fully presented (informed) to healthcare practitioners, but the information is available to those who seek it (see Doc2, for example). The importance of creating and presenting these Standards has been pointed out by, for instance, Halliday et al (1996). In Region Skåne, a number of principles and Standards have been created, as shown in some way by the folders in Appendix 6 and the presence of Swedish laws in healthcare. Most Standards and Guidelines in Swedish healthcare stem from Swedish laws, with only minor adjustments being made in clinics, divisions or regions (see the discussion on multi-layered healthcare in Chapter 6.2). However, users are not informed that much about these Standards, which depends on factors such as the Standards being embedded into education and work as well as few Standards being created or modified in the last few years.

SIS (2003) outlined four characteristics of information security, *availability*, *confidentiality*, *integrity* and accountability. The most important characteristic, according to the case study, is the availability of information. All characteristics are presented, however, with accountability and confidentiality being realized through logs for example, while integrity is maintained through access control. Our case study shows a preferred direction towards patient safety (*availability* and *integrity*) and less focus on patient privacy (*confidentiality* and *accountability*).

As conclusion, the implementation of EMR/EHR, *eHealth* and other digitalizing efforts can benefit from experiences, knowledge and situations in other business areas, with *eBanking* being the first one to consider. As mentioned in our literature review, *eBanking* is an area that has handled personal information electronically for years. *eBanking* does, of course, suffer from frauds and identity thefts, but as mentioned in our case study, patient information is (hopefully) of less importance to thieves than bank account information. This implies that good security solutions for *eBanking* could work even better in *eHealth*. However, basic security issues must be concerned, regardless of business. Basic security training is something to consider and the introduction of monitoring activity in real-time. Websense (2005) also argue that monitoring activities help identify security issues which need to be addressed. Another common issue is that it is more difficult create a security plan after a breach has occurred. It is of paramount importance that a 'battle plan' is created before breaches (Sausner, 2007). Sausner also says reiterates that, although more than a dozen good manuals exist out there, some things in information security can only be learned from experience.

Security Needs

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. It is 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. Users are affected by, and affect the requirements of information security. This is due to 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. Table 3 presents needed security measures for the future, as a summary of the information security needs according to our respondents (Table 3).

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

Table 3: Security needs (Authors' own creation)

Healthcare processes have to be analyzed 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.

7. Conclusions

This chapter includes our research conclusions, what we believe to be our contributions to the field as well as some directions for future research in the research area.

7.1 Conclusions

Our research questions were:

- *What general guidelines, principles and ICTs serve as the foundation of information security and risk management in businesses as well as in healthcare and what can healthcare learn from these other business areas?*
- *What are the perceived problems and needs concerning information security in healthcare in Region Skåne and what needs to be done for the future?*

Our literature review answers the first question as it includes information security, ICT, Standards & Guidelines as well as a description of what healthcare can learn from other business areas (in this case *eBanking*). Our second question is answered in the following sections.

There is great need to focus more on patient security. Today much effort is directed towards patient privacy, thus keeping information secure, but this report has shown the need for more focus on making the right information available to the right person when need. The letter I in IT must not be forgotten; information must be made more accessible and available to treating personnel and also to utilize systems to a satisfactory extent. This does not, however, imply that patient privacy should be neglected in any way.

In Sweden, as well as on a global scale, we are moving towards cross-border healthcare, where patients can receive good care in countries and regions other than their native ones. But today, this vision is not even realized in Swedish regions, such as Region Skåne. Much has been done to unify the Region, but still many different electronic patient journal systems exist, along with unclear laws and constitutions. Swedish laws that concern Swedish healthcare (both for guiding and monitoring purposes) would benefit from revisions and more clear descriptions, which puts a burden on governmental institutions and agencies, in order to improve healthcare. Of course much work needs to be done by system users themselves.

Healthcare should look at other business areas that have succeeded in managing personal information online, mainly *eBanking*. Swedish healthcare have already implemented IT and ICTs in many aspects, but this report show that there is still a long way to go. If the main aim of Swedish healthcare, to provide good care to citizens, is to be realized in the future with increasing use and need of ICTs, healthcare personnel will need to be more educated in systems than they are today as a lack of knowledge exist. Systems would benefit from being simple enough so that no real education is ever needed. Some problems in ICT use could disappear when younger generations fully take over in healthcare, but healthcare should not count on this as a solution, rather as one explanation.

This study has established the problems and needs on information security both in general healthcare domain and in Swedish healthcare system (more specifically the Region of Skåne). The present focus is on patient privacy since legislation focuses on protecting this issue, but the focus will probably change depending on the healthcare requirements on improved availability and accessibility of information. Our case study shows a greater need to focus on patient security and therefore to balance the characteristics of information security because the balance between patient safety and patient privacy is personal, culture and situation-dependent. The respondents identified one common problem that a comprehensive view of the whole area concerning patient information exchange between different healthcare actors is missing, as well as a desire for relevant information in journals and a focus on better systems.

From a patient perspective, privacy is important but should not be imposed at the expense of patient safety. Patient participation should be encouraged, because the patient is the only one who can ultimately determine if both patient safety and patient privacy have been achieved. From an information security perspective, we believe that the healthcare sector still has a long way to go before patients are truly involved in their own patient processes, and the security of patients is considered to be on an acceptable level.

7.2 Contributions

This research took a broad approach covering several areas and topics: it offers an increased understanding of information security risk management by expanding the information security model and its characteristics; it presents a description of information security problems and needs in distributed healthcare; it includes an overview of information security in healthcare in Region Skåne; and it provides a comparison between *eHealth* and *eBanking*.

- The information security model increase the understanding of information security by providing a more complete view of the information security area, technically and administratively and showing the four characteristics of information security and their relation to patient safety and patient privacy.

- The information security problems and needs in healthcare contribute in detail by pointing out problems and needs of the healthcare business. Moreover, it shows the importance of secure patient information management within as well as between healthcare organizations.

- The view of information security in healthcare in Region Skåne will give other researchers and healthcare managers a head start into the Region by showing current problems and solutions as well as pointing out things to consider for the future; with a need to address lack of both technical and administrative security.

- The comparison of *eHealth* vs. *eBanking* contributes in detail by giving a short shot in *eBanking* business, with its problems and needs area by showing similarities and differences between two businesses domains.

7.3 Directions for Future Research

Future studies should address the limitations and extend the findings in this research, into future projects. The patient's role should be more discussed and researched, as patient involvement in this research was not possible. 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; SEMA, 2005), but there is a need to proceed from talking to acting; both for governmental institutions and for healthcare practitioners and directors. Other than the Internet banking domain, these findings can be compared and contrasted by gaining findings from other highly secure organizations, or organizations in different industries that traditionally require greater security awareness (e.g. aviation industry, military industry, police industry). This research can be leveraged by future studies to produce an alternate information security risk assessment methodology for information security that ensures that simplifications made from the process still contain certain key elements, or if a Standard process is used, which specific elements must be considered.

References

1. ASIS International. (2002). 'The General Security Risk Assessment Guidelines', *ASIS International*, Alexandria, Virginia, USA.
2. Bandyopadhyay, K., Mykytyn, P.P. and Mykytyn, K. (1999). 'A framework for integrated risk management in information technology', *Management Decision*, vol.37, no.5, pp.437-444.
3. Björck, F. and Yngström, L. (2001). IFIP World Computer Congress / SEC 2000 Revisited. In WISE 2, Proceedings of the IFIP TC11 WG 11.8 Second World Conference on Information Security Education, held in Perth July 12-14. Edited by Armstrong, H. and L. Yngström, 209-223. Perth, Australia: International Federation for Information Processing.
4. Bielski, L. (2007). 'Security is still a study of the basics', *ABA Banking Journal ABI/Inform Global.*
5. Björner, O. (2000). 'Tjänster för att uppnå Informationssäkerhet i hälso- och sjukvården'. *Report nr 3 from the SITHS project* (in Swedish).
6. Blobel, B., Pharow, P., Spiegel, V., Engel, K. (2001). 'Securing interoperability between chip card-based medical information systems and health networks'. *International Journal of Medical Informatics*, Volume 64.
7. Blobel, B. (1997). 'Security Requirements and Solutions in Distributed Electronic Healthcare Records'. *Computers & Security 16*.
8. Blobel, B. (2007). 'Comparing approaches for advanced e-health security infrastructures', *International Journal of Medical Informatics*, Volume 76.
9. Brehmer, B., Singleton, W.T. & Hovden, J. (1987). 'The Psychology of risk', *Risk and Decisions*, John Wiley & Sons Ltd., pp. 25-39.
10. Carelink. (2001). 'Strategier för effektiva och samverkande IT-stöd i sjukvården'. *Carelinkrapport nr 1/2001* (in Swedish).
11. Chen, D. and Doumeingts, G. (2003). 'European initiatives to develop interoperability of enterprise applications – basic concepts, framework and roadmap'. *Annual Reviews in Control*, Volume 27.
12. Courtney, R. (1977). 'Security risk analysis in electronic data processing', AFIPS Conference Proceedings NCC, *AFIPS Press.*
13. Dahlin, B. and Arnesjö, B. (1996). 'Medicinsk informatik'. *Liber Utbildning* (in Swedish).
14. Datainspektionen. (1998). 'Personregistrering vid sjukhus'. *Datainspektionen*, Stockholm (in Swedish).
15. Datainspektionen. (2005). 'Ökad tillgänglighet till patientuppgifter'. Technical report 2005:1, *Datainspektionen* (in Swedish).
16. Douglas, M., Heap, S.H. & Rossi, A. (1990). 'Understanding the enterprise culture', *Edinburgh University Press,* Edinburgh.
17. Douglas, M. (1992). 'Risk and Blame: essays in cultural theory', *Routledge,* London.
18. Dwivedi, A., Bali, K.R. (2003). 'Towards a Practical Healthcare Information Security Model for Healthcare Institutions', *IEEE.*
19. European Commission. (2006), *eHealth action plan – annual progress report*, EMAS
20. Fitzgerald, J. (1978). 'EDP risk analysis for contingency planning'. *EDP Audit Control and Security Newsletter 6, August*, pp.1-8.
21. France, R. (2001). 'Security of health data: requirements and solutions'. *International Journal of Medical Informatics*, Volume 49.
22. Frosdick, S. (1997). 'The techniques of risk analysis are insufficient in themselves', *Disaster Prevention and Management: an International Journal*, vol.6, no.3, pp 165-177.
23. Gurner, U and Thorslund, M. (2003). 'Dirigent saknas I vård och omsorg för äldre – Om nödvändigheten för samordning.' *Natur och Kultur*, Stockholm, Sweden (in Swedish).
24. Hadden, S. G. (1986). 'Read the label: reducing risk by providing information', *Westview.*
25. Halliday, S., Badenhorst, K., von Solms, R. (1996). 'A business approach to effective information technology risk analysis and management, *Information Management and Computer Security*, vol.4, no.1, pp.19-31.
26. Higgins, R. (1990). 'Analysis for Financial Management'. *Irwin Inc,* Singapore.
27. Hälso- och sjukvårdsinstitutet. (1998). 'Införandet av elektroniska patientjournaler – Förutsättningar och krav'. *Spri rapport 473*, (in Swedish).

28. Israel, M., and Hay, I. (2006). 'Research ethics for social scientists: between ethical conduct and regulatory compliance'. *Sage*, London.
29. Jerlvall, L. and Pehrsson, T. (2006). 'IT-stöd inom landstingen i Sverige – inventering på uppdrag av SLIT-gruppen'. *Carelink*, (in Swedish).
30. Johannesson, P., Perjons, E., Wangler, B., Åhlfeldt, R-M. (2005). 'Design Solutions for Interoperability using a Process Manager. In Proceedings of the 1th International Conference on Interoperability of Enterprise Software and Applications'. *INTEROP-ESA'2005*, Geneva, Switzerland.
31. Kasperson, R. and Stallen, P. (1991). 'Communicating risks to the public: technology, risk and society'. *Kluwer Academic Publishers.*
32. Kosanke, K. (2005). 'ISO Standards for Interoperability: a comparison, in Konstantas et al (eds.), Interoperability of Enterprise Software and Applications, Proceedings of the 1st International INTEROP-ESA conference'. *Springer Verlag*, Geneva, Switzerland.
33. KPMG. (2000). 'Risk Survey Report', *KPMG*, Canada.
34. Kvale, S. (1996). 'InterViews: An Introduction to Qualitative Research Interviewing'. *SAGE Publications Inc,* California, USA.
35. Lagerlund, B. (1999). 'Informationssäkerhet i vårdprocessen: Krav beskrivna i generella användningsfall utifrån vårdscenarion'. *Report nr 1 from the SITHS project* (in Swedish).
36. Lichtenstein, S. (1996). 'Factors in the selection of a risk assessment method', *Information Management and Computer Security*, vol.4, no.4, *pp.20-25.*
37. Markowitz, J. (2007). 'E-banking security: Voice biometrics is not enough as a single layer of defense', *Speech Technology ABI/Inform Global*, April issue.
38. Merkhofer, M. & Dordrecht, D. (1987). 'Decision Science and Social Risk Management', *Reidel Publishing Company.*
39. Norden, (2005). 'Health and Social Sectors with an 'e' study of the Nordic countries. *TemaNord 2005:531, Nordic Council of Ministers*, Copenhagen.
40. O'Mara, J. (1985). 'Computer security, a management blind-spot', *Computer Security Institute,* Massachusetts.
41. Perjons, E., Wangler, B., Wäyrynen, J., Åhlfeldt, R-M. (2005). 'Introducing a process manager in healthcare: an experience report'. *Health Informatics Journal*, vol 11 (1).
42. Roberts, J. & Gray, K. (2008). 'The industry responds on privacy', *Modern Healthcare*, Chicago, United States of America.
43. Roper, C.A. (1999). 'Risk management for security professionals', *Butterworth-Heinemann*, United States of America.
44. Sausner, R. (2007). 'There's no substitute for good preparation'. *American Banker*, January 2007.
45. Schaechter, A. (2002). 'Issues in Electronic Banking: An Overview'. *International Monetary Fund.*
46. SEMA, (2005). 'Samhällets Informationssäkerhet – Lägesbedömning 2005'. *Swedish Emergency Management Agency*. Växjö, Grafiska Punkten. 3 (in Swedish).
47. SITHS. (1999). 'Begrepp för IT-säkerhet'. *SITHS*, Stockholm (in Swedish).
48. SOU 2006:82. (2006). 'Patientdatalag. Huvudbetänkande av Patientdatautredningen'. *Statens Offentliga Utredningar*, Stockholm (in Swedish).
49. Sudha, R. & Thiagarajan, A.S. (2007). 'The Security Concern on Internet Banking Adoption Among Malaysian Banking Customers', *Multimedia University*, Cyberjaja, Malaysia. -
50. Sågänger, J. and Utbult, M. (1998). 'Vårdkedjan och informationstekniken'. *Teldok rapport nr 119* (in Swedish).
51. The National Board of Welfare (Socialstyrelsen). (2004). 'Patientsäkerhet vid elektronisk vårddokumentation'. *Rapport från verksamhetstillsyn 2003* (in Swedish).
52. The Royal Society (2006). 'Digital healthcare: the impact of information and communication technologies on health and healthcare'. *The Royal Society*, London, UK.
53. Thorn, M.E. (2001). 'Applications of technology and risk management', *S.A.M. Advanced Management Journal*, vol.66, no.4, pp.4-14.
54. Utbult, M., Holmgren, A., Larsson, R., Lindwall, C.L. (2004). 'Patientdata – brist och överflöd i vården.' *Teldok rapport, Almqvist & Wiksell*, Uppsala, Sweden.
55. Van Bemmel, J.J. and Musen, M.A. (1997). 'Handbook of medical informatics'. *Houten, Bohn Stafleu Van Loghum.*

56. SIS. (2003). 'SIS Handbok 550. Terminologi för Informationssäkerhet.' *SIS Förlag AB*, Stockholm (in Swedish).
57. Singer, J. and Vinson, N.G. (2002). 'Ethical issues in empirical studies of software engineering'. *IEEE Transactions on software engineering*, vol.6, no. 4.
58. UNESCO, 2002. 'Information and Communication Technology in Education – A Curriculum for Schools and Programme of Teacher Development'. *Division of Higher Education*, UNESCO, France.
59. Visintine, V. (2003). 'An Introduction to Information Risk Assessment', *SANS Institute*.
60. Vlek, C. and Stallen, J. (1981). 'Judging risks and benefits in the small and in the large.' *Organizational Behavior and Human Performance 28*: 235-271.
61. Wah, L. (1999). 'Banking on the Internet'. *American Management Association 88 (11)*, pp 44-48.
62. Waring, A. and Glendon, A.I. (1998). 'Managing Risk', *International Thomson Business Press*, London, UK.
63. Whitman, M.E. and Mattord, H.J. (2005). 'Principles of Information Security', *Thomson Course Technology*, United States of America.
64. Yin, R. K. (2003). 'Case study research: design and methods'. *Sage Publications, Thousand Oaks*.
65. Åhlfeldt, R-M. (2006). 'Information Security in a Distributed Healthcare Domain – Exploring the Problems and Needs of Different Healthcare Providers'. *Licentiate Dissertation*

Electronic References

1. Basel Committee. (2003). 'The Basel Committee Report', http://www.bis.org. [Accessed April 2008].
2. DM Review Editorial Staff. 'Top IT Threats To Healthcare Information Security'. www.dmreview.com/news/1048850-1.html. [Accessed April 2008].
3. Carelink. (2003). 'SITHS CA-policy'. www.carelink.se [Accessed April 2008] (in Swedish).
4. Carelink. (2007). 'Nationell patientöversikt', www.carelink.se/utvecklingsarbete/vardinformation/undersida/. [Accessed April 2008].
5. Carelink. (2008). 'SITHS - Säker IT i Hälso- och Sjukvård', www.carelink.se/tjanster/siths. [Accessed April 2008] (in Swedish).
6. eHealthNews. (2006). 'Commission seeks to improve network and information security in Europe'. http://www.ehealthnews.eu/content/view/70/26/. [Accessed Mar 2007].
7. FTC – Federal Trade Commission. (2008). 'Protecting Personal Information – A Guide for Business'. http://www.ftc.gov/bcp/conline/edcams/infosecurity/slides.pdf. [Accessed May 2008]
8. ISO/IEC 17799:2005, 'Code of practice for information security management'. www.iso.org. [Accessed March 2008].
9. Ministry of Health and Social Affairs, (2006), 'National Strategy for eHealth Sweden'. http://www.ehealthnews.eu/content/view/1064/62/. [Accessed April 2008].
10. SFS 1980:100, 'Sekretesslagen' – 'The Secrecy Act'. http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=1980:100. [Accessed May 2008].
11. SFS 1982:763, 'Hälso- och sjukvårdslag' – 'The Health and Medical Care Act'. http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=1982:763. [Accessed May 2008].
12. SFS 1985:562, 'Patientjournallag' - 'The Patient Record Act'. http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=1985:562. [Accessed May 2008].
13. SFS 1998:204, 'Personuppgiftslag' – 'The Personal Data Act'. http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=1998:204. [Accessed May 2008].
14. SFS 1998:544, 'Lag om vårdregister' – 'Act on healthcare records'. http://www.riksdagen.se/Webbnav/index.aspx?nid=3911&bet=1998:544. [Accessed May 2008].
15. SIS (2007), Swedish Standards Institute. http://sis.se. [Accessed March 2008].
16. Svenska Regeringen (The Swedish Government). (2008). http://www.regeringen.se/sb/d/10230. [Accessed June 2008].
17. The Information Security Handbook (Informationssäkerhetshandboken) for Region Skåne. www.skane.se/templates/Page.aspx?id=45633. [Accessed March 2008]
18. The U.S. National Information Systems Security Glossary, 2006. Available at http://security.isu.edu/pdf/4009.pdf [Accessed April 2008].
19. Websense (2005). 'Ensuring Information Security – New Regulatory Challenges'. http://www.websense.com/global/en/ResourceCenter/WhitePapers/security_compliance.php [Accessed April 2008].

Appendix 1

School of Economics and Management, Department of Informatics, Lund University
Emil Wallin & Ying Xu
Lund, 2008-04-25

Interview proposal – *as presented to our interviewees*

Who are we?

We are two students conducting our master thesis in Informatics at the School of Economics and Management at Lund University. Emil is a 26 year old Skåne boy, and Ying is a 25-year-old female International student from China.

The project

Our research project is focused on *information security and risk management in healthcare in Southern Sweden*, and will be presented, when finalized, at a seminar in June at the School of Economics and Management. At the time of writing this, we have reached the practical part of our thesis, which in our case means interviews. We want to do interviews with key persons in healthcare, including doctors, management and IT staff.

What we want to ask about

We have a few different topics to investigate within our research. Main things to ask include:

- What is your role within the organization and for how long have you held that position?
- Have you received education in information security and/or risk management? How?
- How does work with risk management and information security look today in the organization?
- What are the advantages and disadvantages of this work?
- What improvements need to be done with information security, education about security and management as well as technical improvements?

These are a few examples of the questions we wish to ask.

What do we want you to do?

As mentioned above, we have reached the phase where we need to conduct interviews to continue the project. Our plan is to interview different persons in healthcare, ranging from IT personnel to nurses and management. We would need to conduct our interviews in the next two or three weeks, as we need to finalize our report by the end of May. If you don't have any opportunity to participate in an interview, we'd be happy if you gave us names of other people to contact for interviews. Anonymity is guaranteed, if preferred.

We prefer to conduct our interviews in English, but if that is impossible, interviews can be conducted in Swedish (with only the Swedish student attending that interview, of course).

We would be immensely grateful for any received help.

Thank you in advance!

Emil Wallin

Phone: 0731-50 55 78
E-mail: emil.wallin@gmail.com

Ying Xu

Phone: 0704-05 9265
E-mail: imyvet@gmail.com

Appendix 2

Interview Guide – Interview Questions

Our interview questions are divided into different key participants within healthcare (three units; *management*, *IT staff* and *doctors & nurses*). We begin by presenting the interview questions only and later on we present the questions along with a brief explanation to why we choose to ask these questions and what kind of information we hope to receive from the questions (Appendix 3).

Questions for Management

1. For how long have you held your position in the organization and what does it imply?
2. When you were employed, how was your identity checked? How does user identification work?
3. What are the basic principles for patient identification in your organization?
4. What kind of policies do you have describing how the security work should be managed? Do you follow any standards or other guidelines?
5. How are policies followed-up and further developed in your organization?
6. In your opinion, what are the positive aspects of information security (in contrast to problems)?
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?
9. Distribution of regulation information – how are the constitutions or other organizational rules distributed so you can realize them in the organization?

Questions for IT Staff, system & network administrators

1. For how long have you held your position in the organization and what does it imply?
2. When you were employed, how was your identity checked? How does user identification work?
3. What are the basic principles for patient identification in your organization?
4. Have the users received any education in information security? What kind of information have they received?
5. 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?
6. Are there any routines in the organization that have impact on who has access to the patient records? What kinds of access control do you use (role-based?)?
7. How are user registrations managed? How do you manage user accounts? How are the users verified?
8. Are there any other specific tools for authorization, such as Smart cards, biometrical methods etc.? How is unauthorized access to computerized records prevented and how can the protection be improved?
9. What kind of access policy do you use? "Everything is forbidden which not explicit is allowed?" or the opposite "Everything is allowed which is not explicit forbidden?"?
10. How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information encrypted in any way? What kind of encryption is being used? If no encryption, how is the information kept confidential?
11. Is your work being logged? Do you consider logging necessary?

Questions for doctors and nurses

1. For how long have you held your position in the organization and what does it imply?
2. When you were employed, how was your identity checked? How does user identification work?
3. What are the basic principles for patient identification in your organization?
4. What experiences do you have in using computers (and computer-based systems)?
5. Have you received any education in information security? What kind of information did you receive?
6. 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?
7. Are there any routines in the organization that have impact on who has access to the patient records? Are these routines and rules clearly described, how are they followed up in the organization?
8. How is unauthorized access to computerized records prevented and how can protection against unauthorized access improve?
9. How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information encrypted in any way?
10. Is your work being logged? Do you consider logging necessary?

Melior questions *(questions for doctors, nurses and IT personnel):*

1. Do you use different access levels such as read, write and delete and can the user change it? In what way can you change recorded information? What access do you have? *D*, *N*, *I*.
2. How is information stored? *I*.
3. Is the information available or stored in separate storage units? *I*.
4. Can unauthorized people have access to printed information? How often are copies printed out from the record and stored in archive? *D*, *N*, *I*.
5. How often are you provided back-ups of the computerized records? *D*, *N*, *I*.
6. When you sign up as a Melior user, you have to sign an agreement? Did you do this? Is the agreement informative? Would you like more security/information/protection? *D*, *N*, *I*.

Appendix 3

Interview Questions: Explanations to why certain questions are included

This is a repetition of the interview questions (*italic text*), followed by a short explanation (normal text) to why we choose to ask these questions and what information we hope to derive from them. The explanations also include possible follow-up questions to the initial questions.

- ***Questions for management***

1. *For how long have you held your position in the organization and what does it imply?* – We wish to assess what kind of and how much experience the interviewee has within healthcare. We might also ask if they have experience from other business areas. Have they been part of management in other organizations – how did their work look like then?
2. *When you were employed, how was your identity checked? How does user identification work?* – We wish to assess what kind of security procedures are followed when people are employed. What kind of documents must be signed, and what information is received (for example regarding laws).
3. *What are the basic principles for patient identification in your organization?* – A remake of Question 2, with focus on patients and not employees. How can healthcare practitioners be sure that the patient is who he or she says they are?
4. *What kind of policies do you have describing how the security work should be managed? Do you follow any standards or other guidelines?* – Do the organization follow their own principles/guidelines, which 'general' guidelines have they adopted? Why have they adopted those (because of regulations, laws, or for beneficiary purposes)?
5. *How are policies followed-up and further developed in your organization?* – The work of information security and risk management does not end with adopting guidelines – they must be developed continually and we wish to know how this work is maintained in the organization. We might ask who is responsible for the development as well (within the organization, or does the responsibilities exist on a national level?
6. *In your opinion, what are the positive aspects of information security (in contrast to problems)?* – There is too much focus on the negative – we wish to find out what management think are positive aspects of there IS work today.
7. *In your opinion, would the possibility of availability of needed patient information generate new security problems in the future?* – What does management think will become big issues in the future, caused by increased availability (made possible by EHR and likewise)?
8. *What security demands and requirements will then be needed?* – Based on Question 7, what will be required to address these perceived issues?
9. *Distribution of regulation information – how are the constitutions or other organizational rules distributed so you can realize them in the organization?* - Concerns how management distributes information on constitutions and other organizational rules to employee to facilitate realization of these rules in the entire organization.

- ***Questions for IT Staff, system & network administrators***

1. *For how long have you held your position in the organization and what does it imply?* - We wish to assess what kind of and how much experience the interviewee has within healthcare. We might also ask if they have experience from other business areas. Have they been part of IT staff within other organizations? How did their work look like then?
2. *When you were employed, how was your identity checked? How does user identification work?* - We wish to assess what kind of security procedures are followed when people are employed. What kind of documents must be signed, and what information is received (for example regarding laws). Are there any specific regulations for IT staff?
3. *What are the basic principles for patient identification in your organization?* - A remake of Question 2, with focus on patients and not employees. How can healthcare practitioners be sure that the patient is who he or she says they are? How does IT work enhance these principles?
4. *Have the users received any education in information security? What kind of information have they received?* – When people are employed, what are they told? What information is accessible for every employee electronically? How does the work with education look like?
5. *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?* – Is it management that provides knowledge on constitutions and rules or do IT staff apprehend these by themselves? Can users access this information electronically? Do they wish updates of these rules and if that is the case, what kind of updates?
6. *Are there any routines in the organization that have impact on who has access to the patient records? What kinds of access control do you use (role-based?)?* – Who are allowed to access patient records? Do doctors have more rights than nurses?
7. *How are user registrations managed? How do you manage user accounts? How are the users verified?* – A follow-up to Question 2, with focus on technical aspects of registration and what principles are followed when registering users.
8. *Are there any other specific tools for authorization, such as Smart cards, biometrical methods etc.? How is unauthorized access to computerized records prevented and how can the protection be improved?* - Does the organization use Smart cards for access, and do they use any biometrical methods in some areas of hospitals and likewise? More specifically, how do they prevent unauthorized access and what do they do when that occurs? How does the work of development and improvement look like today?
9. *What kind of access policy do you use? "Everything is forbidden which not explicit is allowed?" or the opposite "Everything is allowed which is not explicit forbidden?"?* – More of a general question, with focus on which approach/spirit is pursued regarding access policies.
10. *How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information encrypted in any way? What kind of encryption is being used? If no encryption, how is the information kept confidential?* – How does communication with other healthcare units work? How are the technical aspects created and maintained?
11. *Is your work being logged? Do you consider logging necessary?* – When an employee works, is their work being logged, and if that is the case, how is the information logged? How is the information used, and who has access to it? Why is logging necessary (or unnecessary)?

- ***Questions for doctors and nurses***

1. *For how long have you held your position in the organization and what does it imply?* - We wish to assess what kind of and how much experience the interviewee has within healthcare. We might also ask if they have experience from other business areas. Have they been a doctor/nurse in other organizations or regions? How did their work look like then?
2. *When you were employed, how was your identity checked? How does user identification work?* We wish to assess what kind of security procedures are followed when people are employed. What kind of documents must be signed, and what information is received (for example regarding laws). Are there any specific regulations for doctors/nurses?
3. *What are the basic principles for patient identification in your organization?* – Not like the Question 3 for IT Staff – this questions focuses more on the practical part of how doctors and nurses identify patients (IT Staff and Management should set out Guidelines for the personnel to follow, regarding identification).
4. *What experiences do you have in using computers (and computer-based systems)?* – More experience increases the possibility of proper computer usage and decreases risks of security breaches through human errors such as forgetting to log-off or allowing anyone else to use your account.
5. *Have you received any education in information security? What kind of information did you receive?* – Management should set out principles for how to educate personnel, and we wish to ask the personnel which kind of education they actually received (both upon employment and later on in their work).
6. *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?* – Does management, IT staff, or doctors and nurses themselves or does someone else provide them with information on constitutions and rules? Can users access this information electronically? What should be changed regarding them?
7. *Are there any routines in the organization that have impact on who has access to the patient records? Are these routines and rules clearly described, how are they followed up in the organization?* – What kind of access does the interviewee have? If the users have received information about rules and routines, how well are they followed up in the organization?
8. *How is unauthorized access to computerized records prevented and how can protection against unauthorized access improve?* – How do doctors and nurses work towards preventing computerized records against unauthorized access?
9. *How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information encrypted in any way?* – How do doctors and nurses transfer important information to other healthcare units (phone, e-mail etc.)? Are they aware of any type of encryption when sending information?
10. *Is your work being logged? Do you consider logging necessary?* – Are doctors and nurses aware of any logging of their work? Can they partake in looking into this information at a later stage? Do they find the logging necessary or unnecessary?

- ***Melior questions*** *(questions for doctors, nurses and IT personnel – this questions can be asked about any such system as Melior):*

Melior is the software used for registering electronic health records (patient records) in the hospitals we are investigating into. We wish to find out how this program is used, if the users are satisfied with it and so on.

1. *Do you use different access levels such as read, write and delete and can the user change it? In what way can you change recorded information? What access do you have? D, N, I.* – We want to know what kind of access our interviewee has, and what they can do with it. When asking IT personnel, we can find out how all access levels look like.
2. *How is information stored? I* – A question only for IT personnel, as it is a technique-oriented question.
3. *Is the information available or stored in separate storage units? I.* – Similar to Question 2 – concerns backups and security issues on how information is stored.
4. *Can unauthorized people have access to printed information? How often are copies printed out from the record and stored in archive? D, N, I.* – What happens when recorded information is printed into paper-form? How often does this happen and why does it happen? What happens to the papers when they have been read?
5. *How often are you provided back-ups of the computerized records? D, N, I.* – Follow-up to Question 4. Might be excluded from the interview if sufficient information is derived in the afore-mentioned question.
6. *When you sign up as a Melior user, you have to sign an agreement? Did you do this? Is the agreement informative? Would you like more security/information/protection? D, N, I.* – This agreement is provided as an appendix in our report (translated from Swedish to English). We wish to find out what else information is provided when signing up as a Melior user and if the users find this sufficient.

Appendix 4

Interview Transcriptions

The following interview transcriptions are divided into the five interview subjects, beginning with a brief presentation of the interview subject (and the abbreviation used in Chapter 5, interview results), and then the transcriptions consist of our interview questions and the answers we received on those. The transcriptions are presented in chronological order (based on when they were conducted).

Interview with Lena-Karin Manaridou

Date	May 8, 2008
Duration	75 minutes
Interviewee	Lena-Karin Manaridou (*Abbreviation*: IT1)
Interviewee's title	Information Security Administrator ('Informationssäkerhetsansvarig')
Location	The interviewer's office at Kansli- och serviceavdelningen, UsiL.

The questions are based on our interview guide, but changed slightly during the course of the interview, because of what was discussed and what we wanted to know.

- *For how long have you held your position in the organization and what does it imply?*

For two years now. The former Information Security Administrator quit this work two years ago and I received this employment. When I got my new employment, several things were changed and added into the role, for example electronic document management was added. *More specifically, what do you work with?* I work with information security related questions and with several systems for journals, including Melior, and the implementation of new systems for the Intranet in Region Skåne. One project is SharePoint. My work is coordinated through several different instances - for instance, I am working with a project manager from the communication staff for the SharePoint project which we have much faith in. Also, in healthcare, we are striving towards "one patient – one journal", which is hindered today by the existence of several different journal systems and not only Melior from Siemens. *Would you prefer one common system then?* Not really. If we only had one system, the owner of the system would have too much power. If we use Melior for example, the Siemens would have all the 'power' concerning patient journal systems. Look at dental care which does not need such a system for their journals. They have no need for Melior, and would probably not need it if everyone was 'forced' to use it. *Anything else you work with?* I, along with other Information Security Administrators, work with the revision and updating of the Region Skåne's Information Security Hand book which can be accessed from our homepage.

- *When you were first employed (or re-employed), how was your identity checked? How does user identification work?*

I remember signing an agreement, including some information on laws and likewise. More than that I do not know. I do not work with anything concerning user identification within the organization.

- *Have the users received any education in information security? What kind of information have they received?*

There is an overreliance on education and we should instead focus on why people act the way they do. Why do people print electronic records into paper format? Why won't some personnel follow simple computer-based procedures? It is possible that we need newer generations to take over totally in the organization before many faults committed by users disappear. It's not as much about education as it is about what you're used to: young people bring their laptops, while middle-age persons can be educated but still go back to work and do the same mistakes they always do. There should be more focus on creating such simple systems that no real education is ever needed for users to do their work efficiently.

- *What are people doing wrong today concerning Information Security in Healthcare?*

People print electronic documents, thereby allowing all information to be transferred back into paper form. Maybe we should try to remove the printer from work for one week, and see how much it is actually missed. I have suggested this at work, but so far not received enough positive response to actually do it. Another problem is that some people might not understand exactly what they are allowed to do: for example when they read a patient journal, they do not only read what they are allowed to read, but they read what interests them. Some personnel might only be allowed to look into medication for a patient while others take part of documents concerning psychiatry, and thereby breaking the rules. These mistakes could stem from badly phrased rules or likewise. *Any faults with journal systems today?* Some healthcare units have created their own, tailored, systems for handling patient information. This might work wonderfully for that particular unit, but is not compatible with other systems or might be too dependent on the creator of the system: what happens if he or she quits?

- *What are people doing right today concerning Information Security in Healthcare?*

Our planned work of implementing SharePoint for the Intranet, which hopefully will simplify information access and to find desired information. Implementation of Comprima, which is a database that can be accessed through systems such as Melior. I believe much in this.

- *Are there any other specific tools for authorization, such as Smart cards, biometrical methods etc.? How is unauthorized access to computerized records prevented and how can the protection become improved?*

Personnel have Smart cards with certain pre-programmed access while logging is used to monitor activities. Log checks are done when there is suspicion on unauthorized use and / or access. Sometimes log checks are done on a random basis as well.

- *The future – what are your thoughts on the future vision of cross-border healthcare, web-based solutions etc.?*

I believe that there is a great possibility that the future will consist of web-based patient record solutions. We are on our way towards that. This creates a dilemma; it will be easier for people to access with the right info at the right time in the right place but it also creates a greater risk for data breaches. Banks have, on the other hand, been able to handle personal information for years online, and a large part of the population uses Internet banking services. Hopefully, healthcare (*patient*) information is of less interest than bank information for thieves, crackers and likewise, which implies that it should not pose any new major problems that web-based solutions become standard. What should be considered a risk here is the possibility of sabotage and manipulation of sensitive data. It is easier to access electronic records than paper-based, while it is easier to trace data infringement in electronic records.

- *What is important to focus on and what needs to be done, concerning information security, patient journals, patient privacy & integrity and IT/ICTs?*

The first thing would be to shift focus from "securing the information" to make information "easily available for those in need of it". Sometimes there is too much attention drawn to protecting measures and ease-of-use while accessibility is put into the shadows. The field should also be viewed as a static field, being under constant development. Furthermore, we need to optimize the use of IT. Many users make general mistakes that can easily be avoided. We are better at utilizing IT than before, say 5 years ago, but we can still improve a lot. Many users can't find computerized information and ask others to print the information, and many users print their e-mails, for convenience purposes, while yet others print guide books that only are updated online and therefore might lose updated information from online revisions. One should shift focus to why users act like this. Why are e-mails printed, why is information not found? All information is available for those with the knowledge to find it.

- *Is your work being logged? Do you consider logging necessary?*

All work is being logged. It is necessary for nervous patients to assure that no unauthorized personnel read their journals. I receive phone calls from concerned patients asking to check the logs.

Interview with Paul Andersson

Date	May 9, 2008
Duration	60 minutes
Interviewee	Paul Andersson (*Abbreviation*: Director)
Interviewee's title	Director of psychiatry division, Landskrona.
Location	Conference room at Divisionsstaben, Kioskgatan 1.

The questions are based on our interview guide, but changed slightly during the course of the interview, because of what was discussed and what we wanted to know. Anything with *Italic* text is our own words or questions.

- *For how long have you held your position in the organization and what does it imply?*

I started in healthcare in 1983 and have been working in my current director position for the last three years. I am in charge of the psychiatry division, in Landskrona. My duties of being a director include economics planning & decisions, development of the department in Landskrona, division management and lots of administrative work. Earlier in Sweden, two different persons were responsible for medical treatment and administration, but with the introduction of the project Region Skåne, which is still considered a project in many places, this responsibility was moved to one single director. The project Region Skåne aims to have a united medical database in Skåne. Everything is controlled and monitored by Swedish laws and constitutions telling healthcare how to act.

- *When you were first employed (or re-employed), how was your identity checked? How does user identification work? (We showed him a brochure on secrecy we received from other personnel, which he recognized).*

I signed the standard employment contract. *Do you recognize these brochures (we show him Appendix 6)?* The yellow brochure is a much discussed one, concerning what should be and what should not be included as well as discussion on what is secrecy now that the Region is "one secrecy area". Earlier, secrecy was divided into the clinics, with sensitive information such as information on sexually transmitted diseases or psychic problems the main areas of individual secrecy. Now all this information can be accessed by almost anyone in the Region.

- *What kind of policies do you have describing how the security work should be managed? Do you follow any standards or other guidelines?*

There is no possibility for divisions, clinics or departments to create their own policies. The university hospitals in Lund could be said to consist of four different levels; 1) the Region (Region Skåne), 2) UsiL (the University hospital of Lund), 3), Psychiatry division (in this case; other divisions in other cases) and 4) the clinics. This implies that on level 1 – the Region – policies are created which every unit must follow, and in UsiL yet other policies are created. Furthermore, in psychiatry, some certain policies must be followed, but they are still not created by the actual division. Information security guidelines and principles are mainly constituted in level 1. Again, the entire Region is considered "one secrecy area" which implies that we need common principles.

The aim in the project Region Skåne to create a unified medical database enhances the possibility to provide patients with more effective and 'right' treatment. When the project started in the late '90s, different departments used different systems; up to eight or ten different systems were detected in Lund. This was, of course, a major problem. Patient information could not be transferred between systems because systems they were not compatible with each other. In the city of Malmö even more systems existed. This project is expected to be completed and all the policies to be conducted formally in the near future.

- *In your opinion, what are the positive aspects of information security (in contrast to problems)? And the negative aspects?*

When IT solutions were implemented into healthcare, we moved from paper journals to electronically, more accessible journals. The secrecy of a paper-based journal was obvious as it only existed at one place in the world, which is the treating clinic. With electronic journals, they can exist anywhere. Now, it is possible to check patient journals within a certain region (hopefully realizing cross-region access in the whole of Sweden in the next 5 years) which creates the problem that many people can have access to information that they are not allowed to access. Only the information that has direct impact on the actual treatment of a patient is allowed, by law, to be accessed. This is of course, a positive aspect as well. Doctors are able to find out what they want to know about a patient quickly and easily. Patients might also have easier access to their own records, and also check if some information is false in the journal, which leads to a complaint. Unfortunately, divisions such as primary care, uses totally different systems today.

Furthermore, let me say that the Region has good security in some places, as I never receive any spam e-mail in my work. Compare this to the municipality of Lund where they receive tons of spam every day. Within the Region we also keep logs on all work conducted on computers. These logs are checked on a random basis, where we select a random sample of patient journals to see if any suspicious access has occurred.

- *In your opinion, would the possibility of availability of needed patient information generate new security problems in the future? What will the future hold in hand for healthcare?*

The future challenges could be: first, if chip-based journals are created and thereby connected to patients at all times, how do we identify the card-holder with the person himself/herself to ensure the information security work? Secondly web-based login provides more convenient access on any computer with Internet connection, but seems to provide lower security. Cookies can be left on a hard disk if the person forgets to delete the Internet browsing history. Thirdly, there is too much invalid patient information in patient journals. There is no common writing style for journals and all information provided is not needed for treatment purposes.

- *What security demands and requirements will then be needed? More specifically, what should we focus on in the future?*

Work is directed towards 'one patient – one journal' in the future and I consider this to be realized today within the psychiatry division. Concerning this, I wish to point out that sensitive data in patient records may bring doubts to patient. To reduce such kind of doubts, patients' will must be considered. If a patient is not willing to let some info be known or if the info seems irrelevant for the treatment then a discussion must take place. We must focus on what is relevant information, and what is not. We also need further focus on cross-border healthcare, allowing patients residing in Sweden but being on vacation on, for instance, on Hawaii to receive proper treatment based on parts of their journals being accessible for the Hawaiian hospital.
Any other future issues? Socialstyrelsen might benefit from being less unclear when telling how patient journals should be written and conducted instead of providing negative feedback on already created journals. Today we have not received enough information on exactly how to conduct journals, but instead receive negative feedback when errors are committed. The work of Tillsynsmyndigheten also needs to be focused on. They monitor activities and can argue that certain information is right or wrong.

- *If certain issues arise with the patient journal records software system (e.g. Melior) – how can changes and updates to the software be done?*

Yes, they can be changed, but a difficult process emerges when updates or changes to the software are wished for. This is mainly because software such as Melior is owned by Siemens in Germany. First a question might be asked to a department within Region Skåne, then these questions moves on to the entire Region, then to discussions for Sweden, and furthermore it could be sent to Germany. Upon reaching Germany, questions from other countries are also added, and in the end Siemens might consider the original questions. So changes are difficult, thus forcing Region Skåne to adapt to the system, instead of adapting the system to the Region.

Interview with Per Torlöf

Date	May 9, 2008
Duration	65 minutes
Interviewee	Per Torlöf (*Abbreviation*: IT2)
Interviewee's title	Department of Information Security (avd. för Informationssäkerhet).
Location	Per's office at Regionhuset (Baravägen, 1).

The questions are based on our interview guide, but changed slightly during the course of the interview, because of what was discussed and what we wanted to know. Anything with *Italic* text is our own words or questions.

- *For how long have you held your position in the organization and what does it imply?*

The corridor at 'avd. för Informationssäkerhet' where I work is mainly concerned with information security in healthcare. I believe that too few help in healthcare and my primary wish is to help Sweden implement their national strategy for IT. My academic background is a technical university (1962) and I worked further within neurophysiology.

- *Upon employment, how is identity checked and further developed in the organization?*

New employees sign certificates in order to receive Smart cards implemented into their ID cards. These Smart Cards function as access cards for doors, as well as login cards for computers. They can be inserted into a computer and the computer will know who the person is and act accordingly. The Smart Card contains information on exactly who the user is (name, role etc.) and works as a regular Swedish identification card with the words Region Skåne labeled onto it.
Any further details on those Smart Cards? They contain public infrastructure (PI) and private as well as public keys (PKI); digital signatures for computer use. Smart Cards work in some ways as devices for internet banks; they function as login cards as well as signature cards enable users to sign e-mails, or records in patient journals stating who read or wrote certain parts, so that monitoring personnel can see who did what. These Smart Cards can even be used to access the Intranet and certain software at home. Smart Cards therefore contain two different keys; one for authorization and one for digital signatures. There exist other types of cards within the region with several units at the main hospital, Blocket, using their own access cards as well as Smart Cards and this should be changed so that all cards are inserted into one, single, card.

- *What information should be allowed to be handled by certain personnel?*

Only the information that treating personnel need for the health care should be available to, or rather, handled by the personnel. Systems today do not work accordingly with Swedish laws which state that only needed parts may be handled. Access can be controlled, however, for example via a few instances, one of them being my department; a doctor might wish to see a certain patient journal and therefore calls, stating his business. The doctor may then be allowed, for a predefined amount of time, to have access to needed information. These types of protocols can also allow access to certain parts of journals, instead of the entire journal. Patients can also gain access to parts of their journals, utilizing Smart Cards. When patients wish for information to be changed in their journals, they should contact Patientnämnden and explain to them their issues with the recorded information.

- *How are user registrations managed? How do you achieve a Smart Card*

A new employee signs an agreement / a certificate upon employment. This document says where the person works, what his or her role is and when she will start working. This information is then sent to HAS and then later sent to SITHS, who supply employees with certificates. These certificates are proof that the employee works within healthcare and that his or her work will be conducted at a certain place in a certain way. At the same time, this information is sent to BIF authentication service (*'BIF's autentiseringstjänst' in Swedish*) which checks the user's attributes as well as controlling them and adding/removing attributes to certain systems such as access in Melior. These attributes can be obtained via the use of Smart Cards, but do not exist within the

Smart Card. Instead, by using the Smart Card, a user can obtain a 'ticket' from BIF's authentication service, which will then be used to log on to systems. The system will use the ticket to see if the user is allowed access. This also simplifies logging, which is done on all work. The language of rules of access controls is defined by something called OASIS and XACML , XML for Access Controls.

- *What needs to be considered for the future, concerning information security?*

The notion that many healthcare employees print e-mails, patient journals and other information needed in their work is an obvious step backwards. Patient journals should not be allowed to be printed at all. Maybe disallow printing totally on certain information would be a good idea.

- *What kind of access policy do you use? "Everything is forbidden which is not explicit is allowed" or the opposite "Everything is allowed which is not explicit forbidden?"?*

What access controls does not allow, is forbidden. Logs will provide a safety net to ensure that rules are followed, although checkup on logs are done on a random basis only.

Interview with Camilla Roos

Date	May 13, 2008
Duration	60 minutes
Interviewee	Camilla Roos (*Abbreviation*: Doc1)
Interviewee's title	Doctor
Location	The interviewer's office at BUP Måsen, Lund.

The questions are based on our interview guide, but changed slightly during the course of the interview, because of what was discussed and what we wanted to know. Sometimes, we needed to explain our questions a bit further, but the explanation is not provided in this transcription. Melior (and other patient journal systems) Questions with an M in front of the questions. Anything with *Italic* text is our own words or questions.

- *What is your position in healthcare? Describe your position and what you do.*

I work as a doctor and I treat kids and youth up to 18 years old, within psychiatry. For the moment I have three different employments, in Lund, Eslöv and Landskrona.

- *When you were first employed (or re-employed), how was your identity checked? How does user identification work?*

I signed an employment contract, but have no memory of certain security agreement. I do not recognize any of the folders you show me (*three different folders, Appendix 6*), although I've seen similar ones when working as a temp. I did, however, sign an agreement for usage of Melior as well.

- *What are the basic principles for patient identification in your organization?*

When patients arrive for the first time, they have to show ID to the nurse or maybe the secretary. Concerning e-mails from patients, we almost never reply on them, unless treating personnel have a certain agreement with a patient to keep e-mail contact with them.

- *Have you received any education in information security, patient security or likewise?? What kind of information have you received?*

Within the medical training, we received education and information on information security. It should be considered a continuing learning process where information is received from time to time.

- *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?*

No particular information is received except for the information that is embedded into education and work. We get e-mail from Socialstyrelsen concerning what is happening, seminars and such. Regarding changes in policies within the organization, I have no memory of big changes in my time working here, so I cannot answer that.

- *How is unauthorized access to computerized records prevented and how can protection against unauthorized access improve?*

I have not experienced that we have any problems with unauthorized access. There is a large responsibility on individuals not to provide others with login information or printed records. Healthcare personnel should also individually assure that they do not read journals they know they should not read. All that is needed to access a journal is a valid login, which is bad for security. But I still claim that electronic patient journals are way more preferable than paper based journals.

- *How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information sent encrypted in any way?*

We send information within Melior, using a monitoring system, so called Bevakningssystem, where we can send information on a certain patient to another doctor or nurse at another care unit, containing information on measures that need to be carried out regarding that particular patient. This provides a good overview, although replying on messages are somewhat complicated and writing is limited as it disallows the usage of spaces in text or the button 'enter'. Bevakningssystem can function as an aide-mémoire with several patients included. When sending messages, we use some kind of homemade encryption. For instance, instead of writing full names, we use initials. I have no information on encryption techniques concerning e-mails, but mainly people should be careful what they send in their e-mails.

- *Is your work being logged? What are your opinions on this? Necessary / unnecessary?*

I think it is sad that we need to be logged, although it might be needed. *Would you say that some personnel find it more or less useful than other?* IT personnel might consider it more necessary, since they "have" to, while healthcare practitioners might find it less relevant.

- *The future – what are your thoughts on the future vision of cross-border healthcare? What is most important to focus on?*

I wish for even more access to patient information to provide better care by doing better and complete judgments on treatment. This implies less focus on securing the information and more focus on providing the right people with access to the right information when needed. A discussion on the conflict regarding what information and patient security really is should be focused on. Is it to protect the information at all costs or making sure that patients are not harmed by the use of information? It might be more secure for a patient if all information about him or her is available to treating personnel wherever he or she is.
Of course I also wish for fewer different systems in the Region. One common patient journal system, for example Melior, would simplify and streamline work a lot. A Smart Card for log-in, thus not forcing personnel to remember five different passwords that must be changed all the time, would be preferable.
It is also not lucid what relevant information in patient journals is. Some people write too much information, and maybe not using a telegraphic language while others use it, while others follow the rule that journals should save space by not using the 'space' and 'enter' buttons which, in my opinion, makes it difficult to read.

- *M1: Do you use different access levels such as read, write and delete? In what way can you change recorded information? What access do you have? Can you print journals?*

A doctor is allowed to do "anything" in Melior. Reading, writing, changing and printing. Other job types might have less authority. *What access do patients have?* Patients are allowed access to the information they ask for.

- *M2: Have you received any Melior education? Do you feel that your Melior knowledge is sufficient for you work?*

We had one occasion of Melior training during our medical education, but none since I started working in the Region. This implies that knowledge is missing with many healthcare workers, for example secretaries. I cannot always ask anyone else at work if I have difficulties with the program. It is a self-learning process in many ways. Of course, the generation gap plays a big part in differences and attitudes in computer and software knowledge and usage.

- *M3: How often are you provided back-ups of the computerized records? How often are copies printed out form the record and stored in the archive? Why do people bother printing, when we wish remove paper based work and computerize it?*

Since you have no opportunity of simple browsing in Melior, many might feel the need to print records instead of reading them on the screen. I do not print any records myself, although I am allowed to print journal records. Printed journals are supposed to enter the shredder after we finish working with them. This is not always the case, which is a problem. Another problem is that you cannot have several documents open at the same time within Melior as only one document is allowed to be open simultaneously, which also might make people consider printing records to simplify their work. This should be changed in Melior, so that you can have more than one document open at the same time, instead of opening and closing them all the time.

Interview with Catrin Blomstrand

Date	May 13, 2008
Duration	55 minutes
Interviewee	Catrin Blomstrand (*Abbreviation*: Doc)
Interviewee's title	Pre-registration physician (ej legitimerad läkare, vikarierande underläkare).
Location	An office room at the Administrative center for BUP, Annetorp, Lund.

The questions are based on our interview guide, but changed slightly during the course of the interview, because of what was discussed and what we wanted to know. Melior (and other patient journal systems) Questions comes with an M in front of the question. Anything with *Italic* text is our own words or questions.

- *For how long have you held your position in the organization and what does it imply?*

I am working as a temp for the moment. I've been working at BUP Lund since March this year, and I worked in Hässleholm earlier. I work mostly with care centre – related work, such as meeting patients, working with journals and such. I work daytime in Landskrona and have night-time duties in Lund.

- *When you were first employed (or re-employed), how was your identity checked? How does user identification work?*

I was first interviewed by the director of the clinic (*verksamhetschef*), where we discussed working conditions and employment contracts. The actual paper – the employment contract - is not very informative, at least regarding information and patient security. *Did you sign any papers for using the journal systems?* Yes, later, when needing a Melior account, I signed an agreement regarding that software as well. Concerning the folders you show me (*Appendix 6*), I recognize the thick yellow one concerning secrecy but not the other two.

- *What are the basic principles for patient identification in your organization?*

When patient first arrives, nurses check their ID as well as their parents, and after that they are considered to be the persons they say they are. When information about who the patients are have been received as well as a preliminary assessment of needed treatment has been done, we are obliged by law to add this information into an existing patient journal or to create a new one if no journal exists at all.

- *What experience do you have using computers? From education and work?*

I have not received any specific computer training, although computers have been an integral part of our medical education. We used it a lot in our practice as well as in my work now. I feel that I have sufficient knowledge on how to use the computers.

- *Have you received any education in information security, patient security or likewise? What kind of information have you received? (We show her the flysheets we received on secrecy and such)*

No particular education concerning this has been provided to me, except for the parts embedded in my education. *Do you feel that some persons suffer from lack of education in healthcare in Skåne?* Obviously, foreign doctors working in Skåne have problems with the Swedish language as well as using Melior. *Do you believe that we suffer from a generation gap, where older personnel are less inclined to use new technology?* Yes, in some ways.

- *How do you get knowledge about constitutions and other rules and how they can be used in your daily* *work (for examples new updates to existing laws, or even brand new laws/constitutions)?*

I believe that we have to find most information for ourselves, for instance by reading doctor's magazines such as Läkartidningen or by connecting to the Intranet skane.se. I have not received any specific information on this.

- *How is unauthorized access to computerized records prevented?*

Some personnel are a bit careless regarding which information they leave visible. For example leaving lists of patient records containing social security numbers and such visible on desktops. I have not experienced any particular unauthorized access into computerized records.
Any other access-related problems? Today we use several systems, such as Melior, Pasis/Prima, and KundRad and so forth. These systems are used for different purposes; patient journals, referrals, certificates and so on. We must remember several different passwords for these systems, and it would be much more flexible if this could be combined into one common system, with only one password needed.

- *How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information sent encrypted in any way?*

When patient information is being sent to other units, we either call the specific personnel we wish to talk to at the particular unit or we use the Bevakningssystem existent in Melior. The problem with using this is that sometimes you can have too much information in that system, although the system itself works well. Another problem is that we have different versions of Melior in different cities, with different functions. The newer version of Melior, used in Hässleholm, has a better Bevakningssystem. We are about to change versions, I've heard. This Bevakningssystem is pretty well protected, since you can specify to whom the information will be sent.
Furthermore, we never receive any spam e-mails, thus showing that at least one part is rather secure.
When transferring information to other cities, the process can sometimes become a bit complicated. You might need to make several phone calls to several secretaries and the process could take up to one week. I wish for a common system in the Region. *Would you prefer a common system, or a common database that you can connect to with any of the systems used today in the Region?* I would prefer a common system in all units, but if a database is on the agenda that would still be better than how it is today. I think that using computer-based systems is much better than the older paper-based system, especially since information does not disappear. When working with paper-based journals, a piece of paper could easily go missing. But computer-based journals can sometimes consist of too much information, thus making it difficult for me to find needed information easily.

- *Is your work being logged? What are your opinions on this?*

Yes, my work is being logged. I think this is good, especially from the point of view of patient security. I have no idea how this logged information is used, and I guess that it will be a lot of information in that log eventually. *Any good examples where logging can be used to control access?* I do not think it is a good idea that healthcare personnel quitting at one unit, could access information at their "old" unit without working there if they do not have a very valid cause for it.

- *M1: Do you use different access levels, such as read, write and delete? What access do you have? Can you change recorded information? Can you print journals?*

As a doctor I have access to most functions. I have no knowledge on other access levels. I am fairly satisfied with how things are now, concerning access levels. I want access to as much information as possible, to enable for a correct and good judgment on patients and the treatment they will need. If certain information is missing, or not accessible, I feel it will become more complicated to do my work.

- *M2: How often are copies printed out from the record and stored in the archive? How often are you provided back-ups of the computerized records?*

Sometimes backups are printed, mostly to allow for a discussion on a specific patient with other personnel.

This printed record does not contain the entire journal and is sent to the paper shredder after we are through using it.

- *M3: When you sign as a Melior user, you have to sign an agreement. Did you sign this? Was the agreement informative? Would you like more information?*

Yes, I signed that agreement. *Is it informative enough?* I think it should contain at least a bit more information.

- *M5: Have you received any Melior education? Do you feel that your Melior knowledge is sufficient?*

I received some education in my former employment in Hässleholm, but I have not received any since coming to Lund. Sometimes I have questions that I might need to ask, which maybe could have been avoided if more training or education had been conducted. *Is there a support number you could call when you have problems?* I have no knowledge on any such number, but I guess that it exists.

- *Future Question: What do you consider the most important aspects to focus on in the near future, concerning information security, patient information, information accessibility and so on?*

I believe, in some ways, that we could benefit a lot from having information from primary care in our journals, although they do not use the same systems as we do. I want more accessibility, and this will in the end be more secure for patients, as we can provide good care to them by using the correct information on medical treatment and such. *What is most important – to focus on availability of correct information, or focus on protecting the information?* In some ways, I believe that correct information should overrule protection. As a doctor, it will be easier to provide good healthcare if the right information is available for me. *Do you wish that it should be more concretized exactly what information is allowed to read?* Yes, I think so. It is not enough to day.

Appendix 5

Universitetssjukhuset i Lund (UsiL)

Division Psykiatri (Division of Psychiatry)

USER-ID + PASSWORD FOR MELIOR

Name:	
User ID:	
Password to use when logging in for the first time in Melior:	
• **Switch this password immediately after logging in for the first time by following this procedure:** • Start >program >Melior tools > new Melior Password > follow the instructions in the dialogue box	
Signature in Melior:	

IMPORTANT INFO ON COMPUTER SECURITY

Patientjournallagen – The patient record Act (SFS 1985:562)
Pins down the responsibility to document in healthcare and how to document, claiming that only the personnel working at the specific care unit are allowed to read the documented patient journal.
Sekretesslagen – The Secrecy Act (SFS 1980:100)
States what information is classified. All healthcare personnel have a duty to keep secret what they know about patients. Classified information may only be shared when one can be certain that no harm will come to the patient or the patients' relatives.
Personuppgiftslagen – The Personal Data Act (SFS 1998:204)
The main purpose is block inappropriate intrusion into personal integrity.
Vårdregisterlagen – The Act on Healthcare Record (SFS 1998:544)
Pins down conditions on how to treat personal records in healthcare.

For Melior users: it is *not* allowed to open a patient journal if you have no relation to the patient. You may not even open a journal of your relative without permission from treating doctor – that is called a data trespass and is illegal. A log is kept every time a user is signed on.

Logging control
Controls who regularly reads patient journals.

Logging off
Take care to **log off your computer when leaving the room**, alternatively lock the computer. If someone else uses your computer to access a patient journal, you will be held responsible.

I hereby acknowledge that I have read and agreed with and will adhere to the above-mentioned laws on computer security. (Sign one ex and give to your boss and keep one for yourself)

City and date: Signature:

Appendix 6

Scanned folders

Folder 1 concerns secrecy and contain laws and descriptions to these laws.

Folder 2 concerns handling personal records

Folder 3 concerns who is allowed access to what information.

1. Tystnadsplikt & Sekretess (Duty to keep secret & secrecy)

REGION SKÅNE

Tystnadsplikt & sekretess

Vad innebär tystnadsplikt
och sekretess för dig i vården?
Den här broschyren ger dig information.

2. Hur mina personuppgifter behandlas i Region Skåne (how personal records are handled in Region Skåne

3. Vårdinformation – tillgänglig för vem? (Healthcare information – available to whom?).

REGION SKÅNE

Hur mina

Personuppgifter

behandlas i Region Skåne

Denna skrift vänder sig till dig som arbetar inom Hälso- och Sjukvården, Tandvården eller Habilitering & Hjälpmedel i Region Skåne

Vårdinformatio

Tillgänglig för vem?

SKÅNE

(Folders 2 & 3)