NTNU
Innovation and Creativity

Information Security in Distribued Health Information Systems in Scandinavia

A Comparative Study of External Conditions and Solutions for Exchange and Sharing of Sensitive Health Information in Denmark, Norway and Sweden

Elin Anette Brox

Master of Science in Computer Science
Submission date: June 2006
Supervisor: Torbjørn Skramstad, IDI
Co-supervisor: Lillian Røstad, IDI
Louise Yngström, Kungliga Tekniska högskolan (KTH)

Norwegian University of Science and Technology
Department of Computer and Information Science

Problem Description

Exchange and sharing of sensitive health information ought to happen according to prevailing external conditions established by laws, regulations and liable authorities. These external conditions create various limitations, making requests for adaptative health information systems. Especially, when developing new system solutions, defining the balance between protection of personal privacy and availability of information, is a great challenge.

According to the current legislation, it is difficult to share sensitive health information within an organisation, but sharing across organisational borders is even more problematic. In this thesis, some of the problems will be considered. Main focus will be on the Scandinavian countries Denmark, Norway and Sweden in order to do a comparison of external conditions and the corresponding technological solutions.

Assignment given: 20. January 2006
Supervisor: Torbjørn Skramstad, IDI

Preface

This report concludes my master thesis for the degree *Master of Science* at the Norwegian University of Science and Technology (NTNU). The thesis has been conducted at the Department of Computer and Systems Sciences at The Royal Institute of Technology (KTH) in Stockholm during my period as an exchange student.

First and foremost, I would like to thank my supervisors Lillian Røstad at Sintef/NTNU and Louise Yngström at KTH for professional guidance. Lillian; thank you for your conscientious follow-up despite of the geographical distance. Louise; our discussions have been a great inspiration to me.

I would also like to thank the following persons who have contributed with research data, given general advices, or commented my work:
Herbjørn Andresen (Universitetet i Oslo), Jan Arild Audestad (Høyskolen i Gjøvik), Louise Arvidsson (Carelink), Magnus Bergström (Datainspektionen), Torbjörn Dahlin (Brainpool), Anders Grimsmo (NSEP), Edvard T. Helling (VismaUnique), Ib Johansen (MedCom), Torbjørn Nystadnes (KITH), Øystein Nytrø (IDI/NSEP), Jens Rahbek Nørgaard (MedCom), Aksel Sogstad (Rikshospitalet), Inger-Anne Tøndel (Sintef) and Benkt Wangler (Högskolan i Skövde). Your help has been invaluable.

Stockholm, 2006-06-28

Elin Anette Brox

Abstract

Exchange and sharing of sensitive health information have to happen according to prevailing external conditions established by laws, regulations and liable authorities. These external conditions create various limitations, making requests for adaptative health information systems. Especially, when developing new solutions, defining the balance between protection of personal privacy and availability of information, is a great challenge.

Several projects are working on possible solutions to the problem of sharing health information in a distributed way. Based on two different pilot projects in each of the countries Denmark, Norway and Sweden, and seen from an information security perspective, this thesis does a comparison of external conditions and various approaches to these conditions. Main focus is on the Scandinavian health legislation, but organisation of health services will also be considered briefly. The objective is to acquire new knowledge about and to contribute to the debate concerning exchange and sharing of health information.

The results of this project are founded on an inductive multiple case study, and empirical data have been collected through semi-structured interviews.

Through this thesis, it has become evident that health care in the Scandinavian countries is upon the whole equally organised and struggles with many of the same technological challenges.

All three countries' health legislation promotes personal integrity, with Sweden as the most expressive. Nevertheless, there is a tendency towards enhancement of the patient's autonomy and a request for more united health care processes, leading to needs for new types of technological tools to ensure information security. In order to meet these requests, common national technological standards, concepts and infrastructure have become more important. In addition, the systems made have to be in accordance with Acts

and regulations. Parts of the prevailing legislation are to a hindrance for exchange and sharing of information across organisational borders.

The technological solutions chosen within the scope of the limiting external conditions are generally well-defined, high quality systems which have information security in focus. Still, there has become evident that some weak points exist, and there is room for improvements.

In order to make health care of higher quality and ensure information security to an even larger degree, legal amendments and a more extensive national co-operation will arrange for the possibility of developing better information security solutions.

Contents

List of Figures

List of Tables

❖ 1

Introduction

This chapter will give an introduction to the thesis' problem and a plan for how a solution will be developed.

Throughout the thesis, various terms which have different names in English compared to Danish, Norwegian or Swedish will be mentioned, e.g. Acts. The English term will be used as a standard, but the original one will be included in a list of terms, see Appendix B.

1.1 Background

In 'IT i Vården', an attachment to the newspaper 'Computer Sweden' on March 8, 2006, Carelink has an advertisement with the heading (translated from Swedish):

> *How can something so easily understandable be so complicated to implement?*

Further, it is mentioned in the advertisement that it should not be necessary to register patient data more than one time, and that this information should be accessible in an easy and secure way, independent of time and location in the health service. Carelink, an organisation which promotes national cooperation to develop the use of IT in Swedish healthcare, states that this is feasible. But, collaboration on a national level is required in order to find answers to essential questions.

An essential demand from every user of an information system is that the correct information is available at the right time to the person with the appropriate interest and authorisation. This demand establishes in other words what information security is resting on; confidentiality, integrity and availability.

The challenge for an organisation is to make information processing and exchange as optimal as possible, while at the same time assuring that the information is secured in a proper way corresponding to the concepts previously mentioned. Health care is one of the domains which this is of great importance. This information-intensive area generates huge volumes of data from hospitals, primary care surgeries, clinics and laboratories. Historically, such organisations have consisted of autonomous and independent units with little or no information sharing [Grimson et al. 2000]. Information regarding a patient has been saved at hospitals, medical offices or other health care institutions where the patient was given care and thereby the information originated from. Because of this, it is hard for health care professionals to get a complete overview of a patient's case history in each individual incident. Such an overview is desirable, and also often required, to be able to offer high quality health services.

The health care domain has become more computerised in the last decades. To take advantage of this progress, information sharing is a necessity to increase the efficiency and quality of care. The exchange of information is no longer only done between different units in the same organisation, but also across organisational borders [Nohlberg and Åhlfeldt 2005]. At the same time, the security issue has become far more complex as the evolution has lead to a decentralised world of networked personal computers and workstations. This means that as the demands of information sharing is increasing, the needs for information security will increase equally in complexity and importance.

1.2 Definitions

The concept *information security* has various interpretations according to which context it is used in. In this case, it is defined as the activities which concentrates on determining what to protect and why, what it needs to be protected from, and how this protection should be done [Alberts and Dorofee 2002]. Further, *confidentiality* is defined as the concealment of information or resources. It also concerns existence of data, which can be more revealing than the data itself. *Integrity* refers to how trustworthy data or resources are, while *availability* is defined as the ability to use the desired information or resource [Bishop 2003].

This thesis considers information security in distributed health information systems. In this context, *distributed* systems are understood as information systems used by health personnel working within the same organisation, but possibly in different wards, but also by personnel who collaborate

across organisational borders. Further, exchange and sharing of health information will be investigated. *Exchange* means information which is distributed in order to inform, but the information is on an unchangeable form, e.g. electronically sent epicrises from a hospital to a general practitioner. As opposed to exchange, *shared* information can be changed by both sender and receiver, e.g. a common health record used by several care providers.

External conditions are in this context defined as prerequisites for processing of sensitive health information, stated by external authorities and/or public administration. These conditions make demands on how information security shall be ensured in health information systems, in addition to restricting usage of sensitive health information. Neither owners, users nor vendors of a health information system can directly change them, but in many situations, they might have an influence on possible amendments. Typical examples on such conditions are various health Acts and regulations.

Requirements are defined as the specific information security requirements which have formed the basis for each of the pilot projects solutions. These requirements can be influenced by both owners, users and vendors of the system, and they are divided into 'functional' or 'non-functional'. *Functional* requirements are associated with specific functions, tasks or behaviours the system must support, while *non-functional* requirements are constraints on various attributes of these functions or tasks. *System solutions* are the implemented version of the previously described requirements.

The terms *primary* and *secondary* health sectors are generally used in the same way in Scandinavia. In this thesis, the primary sector is understood to include the patient's general practitioner, emergency wards and maternal and child health centres amongst others. The secondary sector includes hospitals, ambulance service and the specialist service. A more fine-grained division is not necessary in this context.

More definitions of concepts and terms relevant for this thesis are included in Appendix C.

1.3 Purpose

In this thesis, some of the challenges at the information security level will be identified, and the underlying factors creating these challenges and limitations, will be discussed. Also, various existing technical solutions will be examined and compared against each other. This identification and comparison will be done from a Scandinavian point of view; the three countries Denmark, Norway and Sweden (henceforth mentioned in alphabetical order) will be included.

At the present moment, exchange of sensitive health information happens to some degree, but sharing is still a challenge and is not tested out to any great extent. Therefore, the conditions and possible methods for sharing will be investigated. In addition, how information is exchanged will also be identified.

1.4 Problem

Exchange and sharing of sensitive health information have to happen according to prevailing external conditions established by laws, regulations and liable authorities. These external conditions create various limitations, making requests for adaptative health information systems. Especially, when developing new solutions, defining the balance between protection of personal privacy and availability of information, is a great challenge.

According to the current legislation, it is difficult to share sensitive health information within an organisation, but sharing across organisational borders is even more problematic. In this thesis, some of the problems will be considered. Main focus will be on the Scandinavian countries Denmark, Norway and Sweden in order to:

- do a comparison of external conditions and various approaches to these conditions to give new insight and contribute knowledge into the debate and the development of health information sharing.
- evaluate selected pilot projects, in this thesis called 'cases', to make a comparison of the chosen solutions and the requirements these solutions are based on. Also, the solutions in connection to the external conditions in the three countries will be compared.
- do a comparison of the external conditions with a view to a possible future coordination of regulations to be able to share information across organisational, and possibly national, borders.

Several ongoing pilot projects are working on possible solutions to the problem of sharing health information in a distributed way. Based on two different pilot projects ('cases') in each of the countries Denmark, Norway and Sweden, and seen from an information security perspective, this thesis will try to find answers to the questions listed below. Figure 1.1 includes a corresponding illustration on how the identification and the comparisons will be accomplished. Concepts like **Identification 1** and **Comparison 1** etc. are all shown in the figure.

From a background perspective:

- **Identification 1:** Which external conditions in the three different countries must be taken into consideration?
- **Identification 2:** Which requirements have formed the basis for the different cases?
- **Identification 3:** Which technical solutions have these requirements resulted in?

Comparison 1: External Conditions' Influence on Requirements:

- How have the external conditions influenced the requirements made in the cases?

Comparison 2: Different Solutions in Cases:

- How and why have *different* external requirements resulted in different solutions?
- How and why have *similar* external requirements resulted in different solutions?

Comparison 3: Different Solutions in Countries:

- Could all solutions be implemented in all three countries? If not, which are not realisable?
- Which strengths and/or weaknesses are found in the different cases?

1.5 Goal

This thesis' goal is to acquire new knowledge about and to contribute to the debate concerning development of health information sharing techniques in the Scandinavian countries Denmark, Norway and Sweden, both within each country and across the national borders.

1.6 Method

To reach this project's goal, an inductive approach will be utilised. A literature study will first be conducted. Then, correspondence with representatives from the six different pilot projects, or cases, will be held in order to collect empirical data. These data will be analysed, and the result will form the basis for the comparisons. A more thorough description of the method is found in chapter 2.

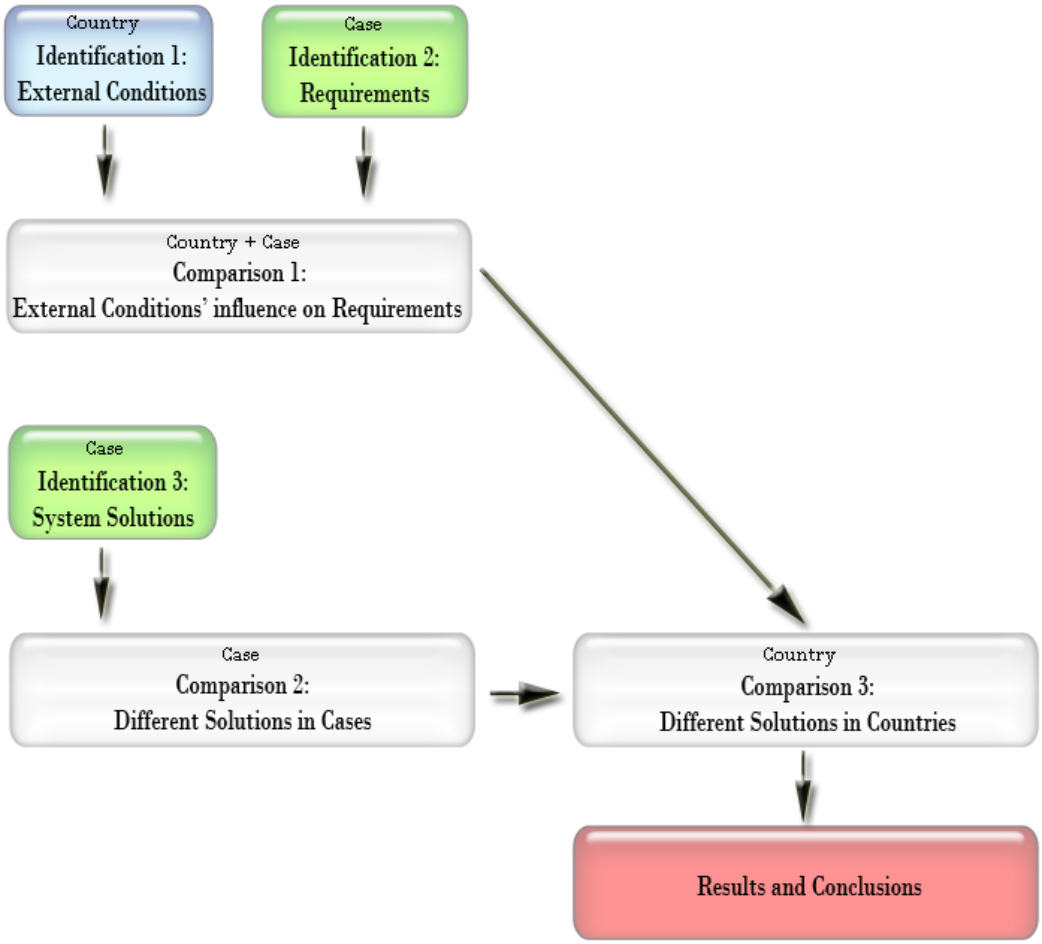


Fig. 1.1. Plan for identification of external conditions and requirements, and comparison of findings

1.7 Contribution

This thesis is aiming to make a contribution to the debate concerning sharing of sensitive information in health care. Hopefully, it will create new insight in how health legislation in Denmark, Norway and Sweden differ from each other, and, based on this, how the differences create dissimilar foundation for development of information sharing solutions. Further, through evaluation and comparison of information security mechanisms, beneficial practices will be revealed. It is also a goal to discover if some of these practices are transferable, and if sensitive information can be shared across national borders in the future.

1.8 Report Structure

This thesis is structured as follows:

- Chapter 1 - Introduction
  Gives an introduction to the thesis' problem and a plan for how a solution will be developed.
- Chapter 2 - Research Method
  A more supplementary description of the chosen research method.
- Chapter 3 - External Conditions
  A thorough review of the external conditions in the three different countries.
- Chapter 4 - Requirements and System Solutions
  A presentation of the six different cases, an identification of the underlying requirements and a description of the corresponding solutions.
- Chapter 5 - Comparisons of Projects
  Comparisons of external conditions, requirements and system solutions.
- Chapter 6 - Analysis and Discussion
  An analysis and discussion of the results.
- Chapter 7 - Conclusion and Future Work
  A summing up and conclusion of the results, and proposals for future work.

❖ 2

Research Method

In this chapter, the chosen research method and strategy will be described in more detail.

2.1 Motivation for Choice of Method

The results of this project will be founded on an inductive research method. This method implies that empirical data is collected, and from the analysis of the data, a conclusion is formulated [Roberts 1997]. The reason for this choice lies in the nature of this thesis' problem formulation. The problem is of an explorative kind; there exists no knowledge about a possible result at the start of the investigation.

In addition, it has been said that studies within the information systems domain cannot only include technological aspects, but also have to consider behaviour and organisation [Galliers and Land 1987]. This study will involve a comparison on how sensitive health information is shared within each of the Scandinavian countries, and possibly also across national borders. To get a holistic picture, the comparison cannot be seen from a technological view only, but also has to include external conditions such as Acts and regulations. Because of the limited scope of this thesis, the emphasis will be on the legislation in Scandinavia, but organisation of health care will also be considered. This type of information is not measurable, and therefore, this thesis' problem will be sought to be answered through a qualitative research approach.

2.2 Research Strategy

The chosen research strategy is a type of *case study*. A case study is an in depth investigation of a single or a small number of units or cases [Hancock 1998]. It is not defined as a methodological choice, but a choice of what to

be studied in the form of interest in one or a few individual cases. Different types of case studies have been defined, and in this thesis a *multiple case study* will be performed. According to [Stake 2005], a multiple case study involves several cases examined to provide insight into an issue or to redraw a generalisation. In this context, the six various pilot projects are considered six different cases to be studied. Even though the cases are examined in depth, they are of secondary interest. They play a supportive role, and they facilitate the understanding of how sensitive health information is exchanged and shared, and which problems and challenges this results in.

The techniques for exchange and sharing of sensitive health information are considered to be strongly contextual dependent and under constant development. What is sought to be understood through this thesis can therefore be defined as a contemporary phenomenon, and a multiple case study is considered appropriate. This choice is justified based on the nature of case studies; the desire to provide new insight into a general issue by means of the study of a few specific cases [Stake 2005].

2.3 Motivation for choice of Research Domain and Cases

The three Scandinavian countries Denmark, Norway and Sweden are chosen because of their similarities in public organisation and structure, meaning that the fundamental basis for the comparison is quite equal. Nevertheless, a resembling framework can result in various solutions with different positive and negative twists.

The six cases have been chosen because they are quite similar. They have in common that they all process sensitive health information which are exchanged/shared between health personnel and possibly the patient, either within or across organisational borders. It is also believed that understanding them can lead to better comprehension, and perhaps theorising, about a still larger collection of cases. In addition, the inclusion of two cases from each country can also make it possible to do a comparison within each country, and possibly reveal internal differences. All six cases represent systems used and administrated by the public health care sector.

2.4 Methods for Collection of Empirical Data

A literature study will first be done. Then, a series of semi-structured interviews with representatives from the six different pilot projects will be held in order to get an overview of the projects' various requirements, solutions,

and possible development problems. Also, various project documents will be studied to supplement the interviews.

2.4.1 Literature Study

The study will include general literature concerning information security and the health care domain, and particularly literature which concerns these two topics in combination. Also, a study of laws and regulations having an impact on information technology in healthcare in Scandinavia will be done. In addition, literature that brings research methodologies with a qualitative approach into focus will also be studied.

The motivation for the literature study is to get a better knowledge of information security in general, in addition to become acquainted with information systems used in health care. The study is also meant to give an overview of relevant prevailing legislation.

2.4.2 Interviews and Correspondence

Representatives from the six different pilot projects will be interviewed in order to collect necessary empirical data. Since the representatives reside in different geographical locations, the interviews will be done both orally and in writing, dependent on where the interviewee is. When written communication is the option, the correspondence will be done via electronic mail.

The semi-structured interview style involves a series of open-ended questions based on the area of interest. The open-ended nature of the questions defines the topic under investigation but gives both the interviewer and the interviewee the opportunity to discuss some topics in more detail. The semi-structured style is useful when it is not possible to draw up a list of possible pre-codes because little is known about the subject area. However, one has to bear in mind that analysing the interview data from open-ended questions is more problematic and time-consuming than when closed questions are used. The reason for this is that work has to be done before often diverse responses from subjects can be compared [Mathers, Fox, and Hunn 1998]. A general interview guide has been constructed (see appendix A).

In addition to using interviews to collect data, various documents describing the different projects will be studied, e.g. requirement specifications and security policies.

2.5 Methods for Analysis of Empirical Data

The collected empirical data will be categorised and analysed in order to form a basis for the identifications and comparisons that shall be done, see Figure 1.1. Below follows descriptions of the necessary frameworks for the categorisation and analysation, divided into a legal and technological viewpoint, respectively.

2.5.1 Identification 1: External Conditions

To be able to make the comparison of the three different countries' health legislation on a most equal basis as possible, various terms will first be defined, see Appendix C.2. Then, the relevant legal questions will be classified according to different subject areas, and then compared. The classification shall assure that resembling legal concepts are compared on an equal foundation. The legal categories are chosen in order to be in correspondence with the selected information security aspects as described in the next section. Below follows an overview of the categories and a corresponding description:

Table 2.1. Overview of legal categories and corresponding descriptions

CATEGORY	DESCRIPTION
Provisions on Information Security in General	What the legislation says about confidentiality, integrity and availability in general
Protection of Personal Privacy	Which requirements are made concerning protection of personal privacy, including the duty of secrecy
Electronic Health Records	Regulations concerning electronic keeping of records
Right of Access	Patient's right of access to sensitive personal data
Internal Control with importance to Logging	Requirements concerning internal control of health systems, and especially logging routines
Exchange and Sharing, and the Patient's Consent	How sensitive personal data can be exchanged and shared, and when and how the patient has to give his consent for such processing

The classification and comparison of external conditions ('Identification 1') will be done in chapter 3, 'External Conditions'.

2.5.2 Identification 2 and 3: Requirements and System Solutions

Information Security is an extensive concept. On the basis of the limitations of this thesis, it is therefore necessary to reduce the number of factors that will be considered. Table 2.2 includes the chosen information security aspects. This concept framework will be used for identification of system requirements and solutions (identification 2 and 3), and also in the subsequent comparison of the projects. The chosen aspects are divided into *functional* and *non-functional* categories and place emphasis on information security mechanisms *within* a system / application. In addition, only security mechanisms concerning live users, e.g. authentication of natural persons, are examined. The information type involved is primarily information which is directly relevant for the patient, and not information used for research.

Identification 2 and **3** (see Figure 1.1) will be carried out in chapter 4, 'Requirements and System Solutions'. The collection of the necessary data will be done by means of the previously mentioned interview guide, see Appendix A.

Table 2.2. Overview of relevant information security aspects

	FUNCTIONAL	NON-FUNCTIONAL
Access Control in general	Type - built-in - external (defined outside system) Dependence on other systems - none - database - ldap - service - others Allocation / revocation of access - how Emergency access - how - time span	Allocation / revocation of access - by whom Emergency access - who can allocate
Identification	Types - User (tied to a single entity) - Group (users grouped into a set) - Role (ties membership to function) How are users, groups and roles - allocated - revoked	How are users, groups and roles - defined
Authentication	Mechanisms - Passwords - Challenge-Response - Biometrics - Multiple methods (combinations) Single Sign-On	Administration - Distribution - Maintenance (frequent password changes etc)
Logging	Content of report - Source - Timestamp - Type - Level of priority Processing of information - Automated - Searchable Archiving	What is being logged - Accessing (read) - Changes (write) - Error corrections Auditing - Analysis - Notification of abnormalities Responsibility / administration Patient's right of inspection

Exchange/ sharing of Information	Patient's consent
	- Automated administration
	  - Registration
	  - Status
		Exchange / Sharing
		- within a system
		- between several systems
		- dependent on patient's consent

❖ 3

External Conditions

In this chapter, external conditions relevant for the pilot projects will be reviewed. Main focus is on the Scandinavian health legislation, but introductorily, a short summary of the organisation of health services will be given.

The health care legislation will be described, followed by an investigation of the legislation with regards to information security, categorized as in table 2.1. The main differences will be pointed out in table 3.9, before a discussion on the variations will be done.

In the investigation of the three different countries' legislation, certain words are underlined. These words are considered to be legal key terms in this context, and are therefore defined in more detail in Appendix C.2. When references to literary sources are not included, there shall be assumed that the Act, regulation etc. which are previously mentioned, is the source.

3.1 Organisation of Health Services

Health services are a public matter in the Scandinavian countries. All of them have well-established systems of primary health care, and generally well developed hospital services with advanced specialist treatment. Health services are provided in accordance to legislation, and they are largely financed by public spending or through compulsory health insurance schemes. In addition, there are some patient charges for treatment and pharmaceutical products [NOMESCO 2005].

Table 3.1 includes a summary of health service aspects in Scandinavia in order to create an overview of organisation of health services and belonging information security services. Most of the information are extracted from [NOMESCO 2005], but various web sites have also been utilized (sundhed.dk, epj-oservatoriet.dk, shdir.no, kith.no, carelink.se and regeringen.se).

Table 3.1. Organisation of health services in Scandinavia

	DENMARK	NORWAY	SWEDEN
ORGANISATIONAL STRUCTURE			
Overall	Counties will be replaced by 5 new regions in 2007. Reduction in the number of municipalities	5 regions administrated by the Ministry of Health and Care Services	18 county and three regional authorities with relatively large internal freedom to manoeuvre
Financing	Mostly at regional level by the state, the rest through contribution by municipalities	Regional health trusts funded by state. Primary health care financed by municipalities	County, regional authorities and municipalities equally responsible for funding
AREA OF RESPONSIBILITY			
Hospital Services	County (replaced by regions 2007)	State (owner), regions (admin.)	County and regional authorities
Primary Health Care	Municipalities	Municipalities	County and regional authorities
Pharmacies	Private (public control)	Private (public control)	State
NATIONAL SERVICES			
Health Net	Yes (MedCom)	Yes (Norsk Helsenett)	Yes (Sjunet)
Patient-oriented Health Portal	Yes (Sundhed.dk)	No	No
IT Strategy	Yes (introduced 2003)	Yes (introduced 2004)	Yes (introduced 2006)
Information Security Policy	For hospitals. General version in process	In process	No, but a prioritised subject in the national IT strategy
PKI	Governmental. Web based. Both for citizens and health personnel	In process, not yet implemented	In process, not yet implemented (SITHS)
EHR standards ('EHR' defined in Appendix C.1)	Architecture and requirements specification	Architecture, archiving, access control and information content. Access control part: mostly implemented by all suppliers	Not yet agreed upon a national concept model (status Oct. 2005)

It should be noted that, even though various standards have been produced, it is often not a request for nationwide adoption from the authorities. Therefore, the application of the standards can be limited.

3.2 Scandinavian Health Legislation

In this section, Danish, Norwegian and Swedish health legislation will be described in general.

Danish Legislation

Recently, a new and comprehensive Act, called the *Health Act*, has been carried in Denmark. This Act shall function as a constitution for the Danish health services, and has the purpose of promoting the population's healthiness, prevention and treatment of illness, and suffering and functional limitations for the individual. The Act establishes requirements on Danish health care with a view to ensure respect for each individual and his integrity and autonomy. Among other factors, it concerns persons' right to health services and the patient's legal position. The Act will come into force the 1. January 2007 [Ministry of the Interior and Health 2005].

In addition to this 'constitutional' Act, the *Act on Processing of Personal Data* and the *Register Act* are of relevance. The former shall assure that data is processed in accordance with good practices for processing of data, while the latter concerns the activity of public registers.

There are also various regulations which are relevant in this context; e.g. the *Statutory order concerning doctors' duty of keeping orderly notes (keep records)*, and the *Statutory order concerning security measures for protection of personal data which is processed for the public administration*.

Norwegian Legislation

Two Acts which are of importance in Norwegian health legislation are the *Act relating to Patients' Rights* and the *Personal Health Data Filing System Act*. The purpose of the first is to help to ensure that all citizens have equal access to good quality health care by granting patients rights in their relations with the health service [Ministry of Health and Care Services 1999a]. The second shall contribute towards providing public health services with information and knowledge, without violating the right to privacy, so as to ensure that medical assistance may be provided in an adequate, effective manner.

In addition, the *Act relating to the Processing of Personal Data*, has the purpose of protecting natural persons from violation of their right to privacy

through the processing of personal data [Ministry of Justice and the Police 2000]. The *Health Personnel Act* shall contribute to safety for patients and quality within the health service, as well as trust in both health personnel and the health service [Ministry of Health and Care Services 1999b].

The *Regulations on the Processing of Personal Data* and the *Regulations relating to Patients' Medical Records* go into more detail concerning processing of personal data and the usage of electronic health records.

Swedish Legislation

Swedish health care is regulated by various Acts, regulations and statues. *The Health and Medical Service Act* concerns health care in general. Its goal is to assure the entire population of good health and care on equal terms, by providing health and medical services [SFS 1982]. In addition, there are five specific Acts which effect electronic health records in particular; *The Freedom of the Press Act, The Secrecy Act, The Patient Register Act, The Act on Healthcare Records and The Personal Data Act* [Utbult et al. 2004].

The Swedish legislation concerning the health sector shows signs of being outdated and not well coordinated, and in the light of this, being to hindrance when it comes to introduction of new technology. At the present moment, the development of a more coherent legislation is commenced. Because of this, how the various Acts relates to each other in addition to some of the existing problems will be discussed briefly in Appendix D. Also, the legal amendment work will be described.

3.3 Provisions on Information Security in General

Denmark

The *Act on Processing of Personal Data* states that the controller shall implement appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation of the provisions laid down in this Act. The same shall apply to processors [Danish Data Protection Agency 2000].

Further, the *Statutory order concerning security measures for protection of personal data which is processed for the public administration*, says that the data controller shall establish more explicitly internal regulations concerning security arrangements in the organisation, which details the rules as they appear in this statutory order. The regulations shall particularly involve organisational conditions and physical securing, including security organisation,

administration of access control - and authorisation arrangements, and also control with authorisations. Additionally, it shall be laid down instructions which determine the responsibility for and describes processing and destruction of in - and out data, and usage of edb equipment. Guidelines for the authorities' supervision shall also be determined [Ministry of the Interior and Health 2000].

Norway

The *Act relating to the Processing of Personal Data* and the *Health Care Personnel Act* state that the controller and the processor shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity, quality and accessibility in connection with the processing of personal health data. To achieve this, the controller and the processor shall document the data system and the security measures. Such documentation shall be accessible to the staff of the controller and the processor, in addition to the supervisory authorities.

Any controller who allows other persons to have access to personal health data, e.g. a data processor or other persons performing tasks in connection with the data system, shall ensure that they fulfil certain requirements.

Sweden

The *Personal Data Act* states that the controller of personal data shall implement appropriate technical and organisational measures to protect the personal data that is processed. The measures shall provide a level of security that is appropriate having regard to the technical possibilities available, what it would cost to implement the measures, the special risks that exist with processing of personal data, and how sensitive the personal data processed really is. A personal data assistant and a person or those persons who work under the assistant's or the controller of personal data's direction may only process personal data in accordance with instructions from the controller of personal data [SFS 1998b].

3.4 Protection of Personal Privacy

Denmark

According to the *Health Act*, a patient is entitled to health personnel's compliance with the duty of confidentiality concerning health care and other personal and private information, which they become acquainted with in their capacity as health personnel.

The *Act on Processing of Personal Data* states that personal data may be processed only if the data subject has given his explicit consent, or in order to protect his vital interests, or for compliance with a legal obligation, or for the performance of a task carried out in the public interest or in the exercise of an official authority. Finally, processing may be done if the purposes are of legitimate interests pursued by the controller or by the third party to whom the data are disclosed, and these are not overridden by the data subject's interests. The data subject may withdraw his consent.

A data subject may at any time object in relation to the controller to the processing of data relating to him, and where this objection is justified, the processing may no longer involve those data.

Sensitive personal data may not be processed, unless the data subject has given his explicit consent, the processing is necessary to protect his vital interests or of another person where the person concerned is physically or legally incapable of giving his consent, or if the processing relates to data which have been made public by the data subject, or if the processing is necessary for the establishment, exercise or defence of legal claims.

Further, sensitive personal data may be processed if the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health services, and where those data are processed by health personnel subject to a statutory obligation of professional secrecy.

Norway

The purpose of the *Act relating to the Processing of Personal Data* is to protect natural persons from violation of their right to privacy through the processing of personal data. Personal data shall be processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality.

The *Personal Health Data Filing System Act* states that any person who processes personal health data has a duty of confidentiality.

The *Health Care Personnel Act* says that health personnel shall prevent others from gaining access to or knowledge of information relating to people's health or medical condition or other personal information that they get to know in their capacity as personnel. This duty of confidentiality is not stated to prevent information from being known to persons who already have knowledge of it, or from being provided when no valid interests indicate secrecy, or from being passed on when identifying characteristics have

been omitted, or from being passed on if exceptional grounds make it legitimate to pass on the information.

The provisions relating to the duty of confidentiality shall apply correspondingly for personnel employed in patient administration.

Supervisory authorities shall also be subject to the duty of secrecy, according to the *Act relating to the Processing of Personal Data*. The duty also applies to information concerning security measures.

The *Act relating to Patients' Rights* says that a patient has the right to protection against the dissemination of information. This means that health-related and other personal information shall be treated in accordance with the current provisions regarding confidentiality, and with caution and respect for the integrity of the person whom the information concerns. The duty of confidentiality ceases to apply to the extent that the person entitled to confidentiality so consents.

Sweden

The *Personal Data Act's* purpose is to protect people against the violation of their personal integrity by processing of personal data [Ministry of Justice 1998]. It makes demands on how personal information shall be handled electronically, stating that personal data may be processed only if the registered person has given his consent to this, or if the processing is necessary according to different regulations, e.g. that the controller should be able to comply with a legal obligation, or that the vital interests of the registered person should be protected. The registered person is entitled to revoke at any time consent that has been given.

Further, sensitive personal data may be processed for health and hospital care purposes, provided that it is for preventive medicine and health care, medical diagnosis, health care or treatment, or management of health and hospital care services. A person who is professionally operational within the health care sector and is subject to the duty of confidentiality may process sensitive personal data that is subject to the duty of confidentiality.

The primary purpose of the *Secrecy Act*, is to protect people's privacy. It concerns regulations about the obligation to observe professional secrecy in public business and prohibits the distribution of public documents. The Act includes limitations of the regulations for the rights of access of public documents provided in *The Freedom of the Press Act*. The regulations concern the prohibitions to display information either verbally or by distributing public documents in other ways. The Act states that duty of confidentiality applies to information concerning a person's state of health or other personal cir-

cumstances, as long as it is not explicitly stated that the information can be revealed without doing any harm to the person or his next of kin.

The *Health and Medical Services (Professional Activity) Act* states that persons who are or have been professionally operational within the health care sector cannot reveal what they, through their profession, have got to know concerning a private persons state of health or other personal circumstances, without authorisation. Activities which concern professional obligations according to laws and regulations are not considered as unauthorised revelation.

Duty of confidentiality which concerns information about a patient's state of health shall also apply for the patient himself, if it out of consideration of the purpose of health care is of exceptional importance that this information is not given to the patient. Duty of confidentiality also applies in situations where it can be presumed there is a risk that the person, who discloses the information or his next of kin, can be a subject to violence or other serious injury if the information is revealed.

3.5 Electronic Health Records

Denmark

According to the *Act on Processing of Personal Data*, data covered by this Act may be transferred to storage in a filing system under the rules laid down in the legislation on files.

The *Statutory order concerning doctors' duty of keeping orderly notes (keep records)*, states that a record can be kept both manually and on electronic media. Further, it is stated that a health record shall include information about, that there has been given access to the record, which information has been distributed, and to who, including possible authorisations.

Records shall be stored in a properly way, and it shall be assured that persons not concerned do not get access to the information. Further, if an electronic record has been changed through corrections or additions, the original electronic version of the altered information shall still be available [Ministry of the Interior and Health 2003].

Norway

The *Personal Health Data Filing System Act* says that personal health data may only be processed by automatic means when this is permitted according to the *Act relating to the Processing of Personal Data*. This Act states that

sensitive personal data may only be processed if the processing satisfies certain conditions, e.g. that the data subject consents, there is statutory authority for such processing, it is necessary to protect a person's interest, but he is incapable of giving his consent, or the processing relates to data which the data subject has voluntarily and manifestly made public. Further, a licence from the Data Inspectorate is required for the processing of sensitive personal data.

The Act also states that personal health data filing systems established for therapeutic purposes may be kept by automatic means. It shall be evident from the filing system who has recorded the data. This may be done by means of an electronic signature or corresponding secure documentation [Ministry of Health and Care Services 2001].

According to *Act relating to the Processing of Personal Data*, personal data may only be processed if the data subject has consented thereto or there is statutory authority for such processing.

Sweden

The Freedom of the Press Act, which is one of the Swedish constitutional laws, states that every Swedish citizen has the right to publish written matter, without prior hindrance by a public authority or other public body. Further, all persons shall have the right to procure information on any subject whatsoever [SFS 1949]. When it comes to health care, the act is interpreted in such a way that all health records in public health care are considered to be public documents. This is not compatible with patient privacy requirements, and the Freedom of the Press Act is therefore complemented by the *Secrecy Act* which concerns regulations about the obligation to observe professional secrecy in public business and prohibits the distribution of public documents [SFS 1980]. The act includes limitations of the regulations for the rights of access of public documents provided in *The Freedom of the Press Act*. The regulations concern the prohibitions to display information either verbally or by distributing public documents in other ways.

The *Patient Register Act* includes principal rules concerning keeping and handling of records in health care, irrespective of the record is kept on electronic or paper format [SOSFS 1993].

The *Act on Healthcare Records* states that those providing health care can process personal data by automatic means in health registers. Further, personal data can be processed for documentation of health care or for administration which concerns patients and the purpose is to provide care for a private individual. Personal data may also be processed by the economic administration which is caused by providing care for a private individual.

According to the *Act on Healthcare Records*, data which is defined as sensitive cannot be used as searchable terms in the record, but data which concerns the ailment and the patient's state of health can be utilized. Only health personnel, who need the information in order to perform their work, can have access to the data in the record, and only the data which is necessary in the given situation shall be accessible [SFS 1998a].

3.6 Right of Access

Denmark

The *Health Act* states that on a patient's request, he shall have information about whether personal data related to him is processed. If such processing takes place, it shall on the patient's request, be given information, in an understandable way, about which information is processed, the purpose of the processing, the categories of receivers of the information, and where this information originates from. Nevertheless, the patient's right of access can be limited, if the patient's interest in becoming acquainted with the information should be given away because of vital considerations for the patient himself or other private interests.

According to *Act on Processing of Personal Data*, where a person submits a request to that effect, the controller shall inform him whether or not data relating to him are being processed. Where such data are being processed, communication to him shall take place in an intelligible form about the data that are being processed, the purposes of the processing, the categories of recipients of the data, and any available information as to the source of such data. Notwithstanding, this shall not apply if the data subject's interest in obtaining this information is found to be overridden by vital private interests, including the interests of the data subject himself, or overridden by vital public interests, e.g. national and public security.

Further, the data subject has the right to be informed of the identity of the controller and of his representative and the rules on the right of access to and the right to rectify the data relating to the data subject.

Norway

According to the *Personal Health Data Filing System Act*, any person who requests so has a right of access insofar as this is authorised in accordance with the *Act relating to Patients' Rights*. This Act states that a patient is entitled to have access to his medical records, and also can request a copy. If such access

can be endangering for the patient's life or can seriously damage his state of health, access can be denied. A representative of the patient can be entitled to have access to the information to which the patient is denied access, unless the representative is considered to be unfit for this. A physician or lawyer may not be denied access, unless special reasons so dictate. The next of kin are entitled to have access to medical records after a patient's death, unless special reasons dictate otherwise.

The data subject has also the right to be informed of the categories of data concerning himself that are being processed, and the security measures that are implemented in connection with the processing.

Sweden

The *Patient Register Act* states that on a patient's request, he shall have his medical record for reading or transcription on the spot, or receiving a transcript or copy, in readiness as soon as possible, as long as the duty of confidentiality does not apply according to regulations described in section 3.4.

3.7 Internal Control with importance to Logging

Denmark

The *Statutory order concerning security measures for protection of personal data which is processed for the public administration* states that all use of personal data shall be logged. The registration shall at a minimum include information about point of time, user, type of usage and report of which person that the information concerned, or the used search criteria. The log shall be kept for six months, after which it shall be deleted. Authorities with special requirements can keep the log for until five years.

Norway

The *Act relating to Public Supervision of the Health Service* states that any person that provides health care shall establish an internal control system for the organisation and assure that operations and services are planned, performed and maintained in accordance with requirements in laws and regulations.

In *Regulations relating to the Processing of Personal Data*, it is said that security measures shall prevent unauthorised use of the information system and make it possible to detect attempts to make such use. Further, measures shall be taken to prevent unauthorised changes in personal data where integrity

is necessary, and also prevent unauthorised changes in other data of significance for data security. Documentation of the measures shall be stored for at least five years.

Registration of unauthorised use of information systems and attempts to carry through such unauthorised use shall be registered. The registrations shall be stored for at least three months. This also applies for registrations of all other events of significance for the information security.

Sweden

The controller shall implement appropriate technical and organisational measures to protect the personal data that is processed. The measures shall provide a level of security that is appropriate having regard to the technical possibilities available, what it would cost to implement the measures, the special risks that exist with processing of personal data, and how sensitive the personal data processed really is.

The supervisory authority may in an individual case decide on which security measures the controller shall implement.

3.8 Exchange and Sharing, and the Patient's Consent

Denmark

The *Health Act* states that information about a patient's state of health and other personal circumstances can be given by health personnel to co-operating personnel as long as the patient has given his consent to this, and it is in connection with providing care. Information can be given without the patient's consent when it is necessary as regards a current treatment course and the distribution happens according to the patient's interests and needs, or when the distribution involves an epicrises written by a hospital doctor to the patient's general practitioner. Also, distribution without consent can happen when it is necessary to ensure an evident public interest or of vital considerations for the patient or the health personnel, or the distribution happens between the patient's general practitioner to a person who acts as a substitute for this one.

The consent can be given verbally or in writing, and can be made to the health personnel who distributes the information, or to the personnel who is the receiver. The consent shall be registered in the patient's health record.

The *Statutory order concerning doctors' duty of keeping orderly notes (keep records)* states that the health record shall include notes about which infor-

mation that has been processed, including distribution, to which purpose, and to who on which basis.

Concerning transfer of personal data to other countries, the *Act on Processing of Personal Data* states that transfer of data to a third country may take place only if the third country in question ensures an adequate level of protection. The adequacy of the level afforded shall be assessed in the light of all the circumstances surrounding a data transfer operation, in particular the nature of the data, the purpose and duration of the processing operation, the country of origin and country of final destination, the rules of law in force in the third country in question and the professional rules and security measures which are complied with in that country.

Norway

According to the *Personal Health Data Filing System Act*, establishments and health personnel who offer or provide health care have a duty to disclose or transfer data as prescribed in various regulations.

The *Health Care Personnel Act* states that confidential information may be given to co-operating personnel when this is necessary in order to provide responsible health care, unless the patient objects thereto. Information may also be given to the management of a facility in order to provide health care or for the purposes of internal control or quality assurance.

The *Act relating to Patients' Rights* states that the patient shall have the possibility of receiving information that is necessary to obtain an insight into his health condition and the content of the health care. He shall also be informed of possible risks and side effects. Information shall not be given against the expressed will of the patient, unless it is necessary in order to prevent harmful effects. Information may be omitted if it is absolutely necessary in order to prevent endangering the patient's life or serious damage to his health.

If the patient consents thereto or circumstances justify it, the patient's next of kin shall receive information concerning the patient's health condition and the care that is being provided.

Further, the Act says that the patient can object to disclosure of information in his medical records, or information may not be disclosed if there is reason to believe that the patient would have objected if asked. Nonetheless, information can be disclosed if weighty grounds dictate.

The *Health Care Personnel Act* states that unless the patient objects thereto, health personnel may give the patient record or information therein to others who provide health care when this is necessary in order to provide health care in a responsible manner. It shall be evident from the patient record that other health personnel have been given access.

When it comes to transfer of personal data to other countries, the *Act relating to the Processing of Personal Data* states that personal data may only be transferred to countries which ensure an adequate level of protection of the data. Countries which have implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data meet these requirements. All the Nordic countries have done the implementation.

Sweden

In the *Secrecy Act*, it is stated that personal data can be distributed without hindrance of the duty of confidentiality, to health personnel if the information is necessary in order to provide care, and it is of exceptional importance that the information is distributed.

The *Act on Healthcare Records* says that only persons that for the purposes of documentation and administration of care, statistical representations, quality assurance, or data distribution provided in laws and regulations, need access to personal data to be able to perform their duties as professionals within the health care sector, can be given direct access to the information in a record. Access shall only be given to the information which is necessary in order to perform the duties. Further, personal data may only be distributed on medium for automatic processing if the data is necessary for the purposes previously mentioned, or for research purposes [Swedish Data Inspection Board 2000].

According to the *Patient Register Act*, a notification shall be done in the record if parts or the entire record have been transcribed or copied and distributed. The person who received it, what he received and time shall be documented.

The *Act on personal data* states that it is prohibited to transfer to a third country personal data that is undergoing processing unless the third country has an adequate level of protection for personal data. The provision also applies to transfer of personal data for processing in a third country. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding the transfer. Particular consideration shall be given to the nature of the data, the purpose of the processing, the duration of the processing, the country of origin, the country of final destination and the rules that exist for the processing in the third country. Nevertheless, it is permitted to transfer personal data to a third country if the registered person has given his consent to it, or if it is necessary for certain reasons according to §34 in the *Personal Data Act*. It is

also permitted to transfer personal data for use only in a state that has acceded to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Directive 95/46/EC).

3.9 Summary in Tabular Form

On the following pages, a summary of relevant legal questions will be given in tabular form. Again, the categorisation as described in table 2.1 will be used.

Table 3.2. Summary of relevant legal questions

	DENMARK	NORWAY	SWEDEN
INFORMATION SECURITY IN GENERAL			
Responsibility of the Controller	Implement appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation with the law. More explicitly internal regulations concerning security arrangements, i.e. security organisation, administration of access control- and authorisation arrangements, shall also be established.	By means of planned, systematic measures, the controller shall ensure satisfactory data security with regard to confidentiality, integrity, quality and accessibility in connection with processing personal data. Responsible for ensuring that persons (e.g. the processor) who access personal data fulfil certain requirements.	Implement appropriate technical and organisational measures to protect personal data that is processed. The measures shall provide a level of security that is appropriate having regard to the technical possibilities available, what it would cost to implement the measures, the special risks that exist, and how sensitive the personal data really is.
Responsibility of the processor/ assistant	Implement appropriate technical and organisational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorised disclosure, abuse or other processing in violation with the law.	By means of planned, systematic measures, the processor shall ensure satisfactory data security with regard to confidentiality, integrity, quality and accessibility in connection with processing personal data.	An assistant and persons working under the his or the controller's direction may only process personal data in accordance with instructions from the controller.
Supervision by the authorities	Guidelines for supervision shall be determined by the controller.	The data system and the security measures shall be documented by the controller and processor, and be accessible by the supervisory authorities.	The supervisory authority is entitled for its supervision to obtain on request access to personal data that is processed, in addition to information about, and documentation and security of the processing.

Continued on next page

	DENMARK	NORWAY	SWEDEN
PROTECTION OF PERSONAL PRIVACY			
Duty of confidentiality	A patient is entitled to health personnel's compliance with the duty of confidentiality concerning health care and other personal and private information, which they become acquainted with in their capacity as health personnel.	Any person who processes personal health data has a duty of confidentiality. Further, health personnel shall prevent others from gaining access to or knowledge of information relating to people's health or medical condition or other personal information. The provisions applies correspondingly for personnel employed in administration and supervisory authorities.	Persons who are or have been professionally operational within the health care sector cannot reveal what they, through their profession, have got to know concerning a private persons state of health or other personal circumstances, without authorisation. Duty of confidentiality which concerns information about a patient's state of health shall also apply for the patient himself, if it out of consideration of the purpose of health care is of exceptional importance that this information is not given to the patient.
Processing of personal data	May only happen if - data subject has consented - in order to protect data subject's vital interests - it is required for the purposes of preventive medicine, medical diagnosis, the provision of care or management of health care services - it is processed by health personnel subject to a statutory obligation of professional secrecy	Personal data shall be processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that the data is of adequate quality.	May only happen if - the registered person has given his consent to this - the vital interests of the registered person should be protected - it is for health and hospital care purposes (preventive medicine and health care, medical diagnosis, treatment, or management of health and hospital care services)
Patient's co-determination	May withdraw consent at any time. He may at any time object in relation to the controller to the processing of data relating to him.	The duty of confidentiality ceases to apply to the extent that the person entitled to confidentiality so consents.	May withdraw consent at any time.

Continued on next page

	DENMARK	NORWAY	SWEDEN
ELECTRONIC HEALTH RECORDS			
General Security Provisions	Records shall be stored in a properly way, and it shall be assured that persons not concerned do not get access to the information. Further, if an electronic record has been changed through corrections or additions, the original electronic version of the altered information shall still be available.	It shall be evident from the filing system who has recorded the data. This may be done by means of an electronic signature or corresponding secure documentation.	Data which is defined as sensitive cannot be used as searchable terms in the record.
Usage of one record by several organisations	Not possible	Not possible	Not possible
RIGHT OF ACCESS			
Patient's right of Access	Shall be available on request: - whether or not personal data is processed, and if so; - which information - the purpose of the processing - the categories of receivers of the information - where does the information originate from - the identity of the controller and of his representative - the rules concerning the right of access and the right to rectify data	Any person who requests so, has a right of access insofar as this is authorised according to legislation. The patient is entitled to: - get access to his medical records - receive a copy - be informed of the categories of data concerning himself that are being processed - the security measures that are implemented	On a patient's request, he shall have his medical record for reading or transcription on the spot, or receiving a transcript or copy, in readiness as soon as possible.

Continued on next page

	DENMARK	NORWAY	SWEDEN
		RIGHT OF ACCESS	
Access Rights Limitations	The rights mentioned above shall not apply if the data subject's interest in obtaining this information is found to be overridden by vital private interests, including the interests of the data subject himself or other private interests, or overridden by vital public interests.	If such access can be endangering for the patient's life or can seriously damage his state of health, access can be denied. A representative of the patient can be entitled to have access to the information to which the patient is denied access. A physician or lawyer may not be denied access, unless special reasons so dictate. The next of kin are entitled to have access to medical records after a patient's death, unless special reasons dictate otherwise.	The rights mentioned above shall not apply if it out of considerations of the purpose of health care is of exceptional importance that this information is not given to the patient. Duty of confidentiality also applies in situations where it can be presumed there is a risk that the person who discloses the information or his next of kin, can be a subject to violence or other serious injury if the information is revealed.
		INTERNAL CONTROL WITH IMPORTANCE TO LOGGING	
General Provisions	All use of personal data shall be logged.	Registration of unauthorised use of information systems and attempts to carry through such unauthorised use shall be registered.	The controller shall implement appropriate technical and organisational measures to protect the personal data that is processed.
Log Content	Minimum content: - point of time - user - type of usage - report of which person that the information concerned, or used search criteria	Not explicitly established.	Not explicitly established.
Storage Time	Six months, after which it shall be deleted. Certain authorities can keep it for until five years.	Three months at a minimum.	Not explicitly established.

Continued on next page

	DENMARK	NORWAY	SWEDEN
EXCHANGE AND SHARING, AND THE PATIENT'S CONSENT			
Exchange within org. and between org.	No difference.	No difference as long as the organisations are within the same regional health authority.	Limitations, borders not clearly defined.
Conditions: exchange between personnel within an organisation	Can be given from personnel to co-operating personnel if: - patient has given his consent, and - it is in connection with providing care	Can be given from personnel to co-operating personnel if: - patient has not objected thereto - patient consents to set aside duty of confidentiality Information may also be given to the management of a facility to provide health care or for the purposes of internal control or quality assurance.	Personal data can be distributed without hindrance of the duty of confidentiality, to health personnel if the information is necessary in order to provide care, and it is of exceptional importance that the information is distributed.
Conditions: exchange between personnel in different organisations	Can be given from personnel to co-operating personnel in another organisation if: - patient has given his consent, and - it is in connection with providing care	Can be given from personnel to co-operating personnel in another organisation if: - patient has not objected thereto - patient consents to set aside duty of confidentiality	The legislation is vague and conditions are not clearly defined. Amendments are in progress, see Appendix D.
Submission of consent	Consent: - Verbally or in writing - Can be made to the health personnel who distributes the information, or to the personnel who is the receiver - Shall be registered in the patient's health record	Verbally or in writing.	[Patient's consent not decision basis for exchange]

Continued on next page

	DENMARK	NORWAY	SWEDEN
EXCHANGE AND SHARING, AND THE PATIENT'S CONSENT			
Situations when patient's consent is not requested	Consent not necessary when: - Information regards a current treatment course and distribution happens according to patient's interests and needs - Distribution involves an epicrises written by a hospital doctor to the patient's general practitioner - Distribution happens between general practioner to a person who acts as a substitute for this one - Necessary to ensure an evident public interest	The patient can object to disclosure of information, or information may not be disclosed if there is reason to believe that the patient would have objected if asked. Nonetheless, information can be disclosed if weighty grounds dictate.	[Patient's consent not decision basis for exchange]
Emergency Access/ Exchange	Information can be given without the patient's consent when it is necessary as regards a current treatment course and it happens according to the patient's interests and needs.	Exchange can be done even if the patient opposes to this.	[Patient's consent not decision basis for exchange]
Exchange across national borders	Yes, as long as the EU Directive 95/46/EC is implemented.		

3.10 Discussion

In this section, the primary problems and challenges in the health legislation in Denmark, Norway and Sweden are discussed and compared with each other.

Organisation of Health Services

There is a difference between how the health services are organised in Sweden compared to Denmark and Norway. The two latter have chosen a relatively centralised model by means of five regional health authorities (will be introduced in Denmark in 2007), with the state as the owner. In Norway, all hospitals are organised as enterprises owned by the state. Principal health policy objectives and frameworks are therefore determined by the central government.

On the other hand, in Sweden, there are 18 counties and three regional authorities with comparatively large internal freedom to manoeuvre. Nils Blom, chief lawyer at the National Board of Health and Welfare in Sweden, says that a fundamental legally problem is the Swedish society model; responsibility for health care is divided and decentralised to several county councils and municipalities. In addition, health care is operated in different ways. The number of care providers, and by this, decision-makers, are therefore often a hinder for a common information processing mindset. [Utbult et al. 2004]

Health Record Acts - Paper vs. Electronic

The Danish *Register Act* is the most important Act concerning health records. It includes regulations concerning public registers and is technological neutral, but calls for use of electronic records [The Folketing 2002].

The Norwegian legislation concerning health records is aimed at being technological neutral and is relatively new, with the *Act relating to the Processing of Personal Data* from 2000, and the *Personal Health Data Filing System Act* from 2001. Together with the *Regulations relating to Patients' Medical Records*, they make requests on how to keep records, independent of whether they are in paper or electronic version.

The relevant Swedish record laws are the *Act on Healthcare Records* from 1985 and the *Patient Register Act* from 1998. The former is said to be technical neutral, but shows sign of being out of date. Formally, it does not hinder the use of technology, but it does make it harder to introduce new solutions, e.g. concerning digital signing and how to do corrections in an electronic record.

Patient's Right of Access

In all three countries, the patient has a statutory right of access to information in his own record. In addition, limitations are also stated in the three countries; a patient can be denied access if it out of considerations for his interests are found to be the most appropriate solution.

The Duty of Confidentiality, the Patient's Consent and Exchange of Information

In Denmark, a basic rule is that the information which is entrusted health personnel by a patient, stays between the personnel and the patient, and is not distributed to persons not concerned. Nevertheless, information about the patient's state of health and other personal information in connection with treatment of a patient can be given to other health personnel if the patient has consented to this. In addition, information can be exchanged without the patient's consent in certain concrete situations, e.g. it is necessary regarding a current treatment course and it is done in the patient's best interests and needs. It is stated that such exchange can be done between health personnel in different sections in a hospital, and also across county borders [Madsen 2004].

Concerning consent, a fundamental principle in Denmark is that the patient owns and has to his disposal the personal data which concerns himself. This means that distribution and exchange of information cannot happen without the patient's consent. But, to assure patient safety, the legislation concretely describes certain situations where personal data can be available to a third party without the patient consenting thereto, e.g. acute illness.

In Norway, the main rule is that health personnel have to keep the duty of confidentiality concerning personal data, but there are no regulations stating that the duty of confidentiality has to be complied with concerning exchange between health authorities. Therefore, personal data may be exchanged as long as it is relevant for the current treatment of a patient. Nevertheless, it is the patient who shall be protected by means of the duty of confidentiality, and therefore, the person concerned has the right to relinquish this protection [Ohnstad 2003]. This is based on the patient's autonomy, i.e. his right to have control over himself, which again implies that he also has the right to control information concerning him. In addition, the relevant Acts states that personal data can be given to co-operating health personnel in order to provide properly health care, as long as the patient has not objected thereto.

Sweden has taken the opposite stand; patient information are here governed by the Freedom of the Press Act, stating that the information is in principle public, and thereby not owned by the patient. Naturally, the patient has the right to take part in his own health information, but it is determined by means of legislation, and especially the *Secrecy Act*, when and how personal information can be exchanged. This Act focuses on the patient's vital interests, but unfortunately, there are many situations where health personnel are uncertain of whether they can disclose information or not [Utbult et al. 2004].

This problem originates from the fact that the Swedish legislation tends to favour personal integrity before the availability of personal data. The various interpretations of the Secrecy Act have lead to confusion around where the 'secrecy limit' shall be going; within a clinic, within a hospital, or encircling a county council. It has been suggested that the limitation shall be at the county councils, which means that within a county, co-operative health personnel shall be able to exchange information independent of organisational borders. This is the current practice. A national perspective is not yet included [Utbult et al. 2004].

Consequently, Danish and Norwegian health legislation favours personal integrity in a lower degree than the Swedish does. Still, there has to be said that personal integrity are of great importance in the entire Scandinavia.

An interesting observation concerning consent and the legal definition of how this shall be given, is that in all three countries, it is requested that the consent shall be *informed* (see definition of consent in Appendix C.2). This means that health personnel are responsible for informing the patient about the the consequences of the consent before it is stated. But, common for all countries is the vagueness in the definition of *informed*. It is difficult to determine how much information the patient is entitled to receive, and based on this, it might be hard to assure that a registered consent really is informed.

Exchange vs. Sharing of Information

According to Danish legislation, there are no regulations that explicitly prevent information from being exchanged between several health care organisations in Denmark. By virtue of this, a project called 'SUP' has been initiated in order to make electronically registered patient data available across county borders (see section 4.2). At the present moment, a pilot is under implementation, but the Danish Data Protection Agency has stopped the activa-

tion of the pilot system because it is not compatible with the security regulations in the Act on Processing of Personal Data. The Data Protection Agency thinks the system makes too much information available for too many care providers [Danish Data Protection Agency 2006]. This project could be seen as the first step to a shared record, but at the present moment, it is not entirely clarified how exchange of health information shall be done. Therefore, sharing of health information in a common record is probably not realizable in the nearest future.

In Norway, exchange of information across organisational borders is possible as long as the organisations are members of the same regional health authority. But, it is not possible to exchange information between e.g. hospitals that belongs to two different regional health authorities. This is the result of the definition of a regional health authority; they are not executive, meaning that they do not provide patient care. However, exchange within one regional health authority is legal.

When it comes to sharing of information, there is a dissension whether it is necessary or not with legal amendments in order to share an electronic health record between several organisations. Most likely, it is possible with the prevailing legislation in Norway to implement a type of record which includes a limited amount of information, and is based on the patient's consent. If the patient does not consent, it will not be possible to share the record, either.

The Swedish National Board of Health and Welfare has in an investigation suggested that a patient's information should in high degree follow the patient through health care processes, meaning that a patient should have one record used by several health organisations. The Swedish Data Inspection Board was negative to the suggestion, and at the current moment, it is not possible for several care providers to share one patient record, according to the legislation [Utbult et al. 2004]. This problem is one of the topics for discussion in the on-going Patient Data Investigation. The conditions for and the benefits from a common record for each patient, either on national or county level, shall be examined [SOU 2006].

Exchange of Information across National Borders in Scandinavia

The *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal*

data and on the free movement of such data is implemented in both Denmark, Norway and Sweden. Each country shall draw up their legislation in such a way that the requirements in the directive are ensured. On the basis of this, all three countries approve exchange of information across national borders as long as the directive is implemented [European Parliament 1995].

Interpretations of the Acts seen from a Technological View

From a technological viewpoint, the more concrete and explicit an Act or regulation is expressed, the more advantageous it is for the persons developing new health care information systems. Examples of this are Denmarks legislation; concerning logging, a minimum log content is requested, and the storage time is set to six months. When it comes to distribution of information without the patient's consent, e.g. this can happen when distribution involves an epicrises written by a hospital doctor to the patient's general practitioner.

Such concrete rules and requests make it easier for technologists to plan and develop a system. It will most likely also facilitate exchange and sharing of information between systems and organisations, since the systems ought to be based on equal rules and regulations. But, on the other hand, more concrete rules might lead to legislation which is less technological neutral, and thereby slowing down adequate technology changes. The most appropriate solution is probably to have legislation which principally is technological neutral, but is updated according to technological changes of a certain extent.

❖ 4

Requirements and System Solutions

In this chapter, **identification 2** and **3** will be done (see figure 1.1). The six cases, or pilot projects, will first be presented briefly in table 4.1, before they are investigated more thoroughly one at a time. Each single investigation will include a short introduction of the case, a presentation of the involved stakeholders, a brief discussion concerning relevant legislation, and a description of the systems requirements. In addition, for each case, the relevant security aspects in the system solution will be described thoroughly in accordance with the categorisation shown in table 2.2.

Table 4.1. Overview of the six pilot projects, or 'cases'

CASE	DESCRIPTION
1: mini-IRSK (Danish)	Secure electronic communication of standard messages (epicrises, referrals etc.) between hospitals.
2: SUP (Danish)	Making hospital data available to other hospitals and primary care across county borders.
3: Klinisk Portal (Norwegian)	A portal which links several hospital applications together and presents them in an united interface.
4: SamPro (Norwegian)	Secure electronic interaction between several participators concerning an individual plan.
5: GVD (Swedish)	Common electronic health record used by all care providers taking part in a patient's care.
6: NPÖ (Swedish)	A national patient register facilitating co-operation between care providers across organisational borders.

4.1 Case 1: InterRegionale SygehusKommunikationsprojekt - mini-IRSK

The objective of the project InterRegionalte SygehusKommunikationsprojekt (IRSK), which can be called Inter Regional Hospital Communication project in English, is to increase the use of electronic communication between hospitals in Denmark.

A pilot project, mini-IRSK, has been implemented. In the context of the project, some of the communication in the hospital sector will be converted from manual to electronic managed. The number of types of messages is small, but they are heavily used. The purpose is to create uniform and less time-consuming procedures combined with increased security in patient treatment. The background for Mini-IRSK is that electronic communication over the last decade has expanded in the primary sector and between the primary sector and secondary sector, but electronic communication between hospitals is not as widespread. The Mini-IRSK project is aimed at rectifying this situation and the strategy is for all Danish hospitals to exchange a small number of heavily used messages in electronic form. All counties have joined the project, which will be exclusively carried out in relation to IT systems which are in use today:

- Patient Administration Systems (PAS)
- Clinical Biochemistry
- Existing Electronic Health Record systems (EHR)

When the project is accomplished, the hospitals of the counties involved will be able to communicate discharge letters and patient referrals to each other regardless of system used in the individual county. Hospital departments will be able to correspond with other departments, local authorities, pharmacies, general practitioners, specialists, physiotherapists, chiropractors and psychologists throughout the country. Biochemistry laboratories will be able to exchange electronic laboratory results [MedCom 2005].

MedCom's 'sundhedsdatanet' (a nationwide Internet based health net used for secure communication by the National Health Service's partners) will be used for all communication in the project.

In addition to the referred sources, Ib Johansen at MedCom has contributed with information concerning mini-IRSK via mail correspondence.

4.1.1 Stakeholders

MedCom is the initiator of the project. In addition, various software suppliers who have developed systems in the different counties, have been involved, e.g. CSC, Acure, WM-data, CSC-Labka, Capio diagnostic and Misys.

Implementation of the project began in 2005, and 14 counties have signed an agreement on participation. At the present moment, 11 counties have the pilot running.

4.1.2 Legislation

Only the *Act on Processing of Personal Data* and the *the Patients' Rights Act* have been necessary to take into consideration, but none of the parts in the legislation have been to hindrance under the development work.

4.1.3 Requirements

The system requirements have been proposed by MedCom. In a previous project, MedCom has made standards for Electronic Data Interchange (EDI) communication in the health care sector. In connection with this project, a set of security requirements was stated to assure secure communication of the EDI documents. The same security requirements are made for the mini-IRSK project, and therefore, it does not exist an own requirements specification.

The requirements specification for the EDI project has not been possible to receive from MedCom, but according to them, the requirements for the SUP project (see Appendix E, Case 2) are analogue to the mini-IRSK project.

4.1.4 System Solutions in mini-IRSK

Access Control in general

Since the mini-IRSK project implies a method for secure exchange of sensitive health information, and not a system on its own, it does not have any explicit access control mechanisms, but relies on the mechanisms already implemented in the source systems.

Emergency Access Control

As mentioned above, mini-IRSK does not include any own access control mechanisms.

Identification

Users are identified in their home environemt system, e.g. in Pasient Administrative Systems (PAS) and Management Information Systems (LedelsesInformationsSystem - LIS). The users are authorised via their home system.

Authentication

Authentication is explicitly done at each organisation which takes part in the project. Generally, user identities and passwords are used, in combination with certificates in order to logon to the 'Sundhedsdatanet'. Administration and maintenance of the authentication mechanisms are locally regulated.

Single sign-on is not implemented in any of the participating systems.

Logging

All distribution of data is logged. What shall be logged has been determined in accordance with the *Act on Processing of Personal Data*:

- point of time
- user
- type of usage
- report of which person that the information concerned, or used search criteria

The content is stated in local instructions which are approved by the Data Protection Agency. Local routines are followed for auditing, archiving and patient access of the log.

Consent and exchange/sharing of information

Exchange of information is done by means of the communication standards developed in the mini-IRSK standard. It is not possible to share information across organisational borders.

The patient gives his consent for exchange of information verbally.

4.2 Case 2: Standardiseret Udtræk af Patientdata - SUP

The Danish project Standariseret Utræk af Patientdata - SUP, which can be called 'standardised patient data extraction' in English, shall make electronically registered patient data available across county borders. The philosophy behind the SUP-solution is that one hospital can place clinical data concerning present and former hospitalisated patients at other hospitals' disposal, both within and outside its own county. This will be beneficial with a view to treatment outside the patient's home-county, and also the possibility to make inquiries concerning external treatment at a later occasion.

Data that shall be made available is delivered from existing patient administrative systems (PAS) and electronic health record systems (EHR). The extracted data is transported by means of a nationwide XML standard to a SUP database/browser, which again makes it possible to get access to selected health information via an Internet browser. The SUP database/browser can be established as a database for either one county or as a shared database between several counties [MedCom 2003].

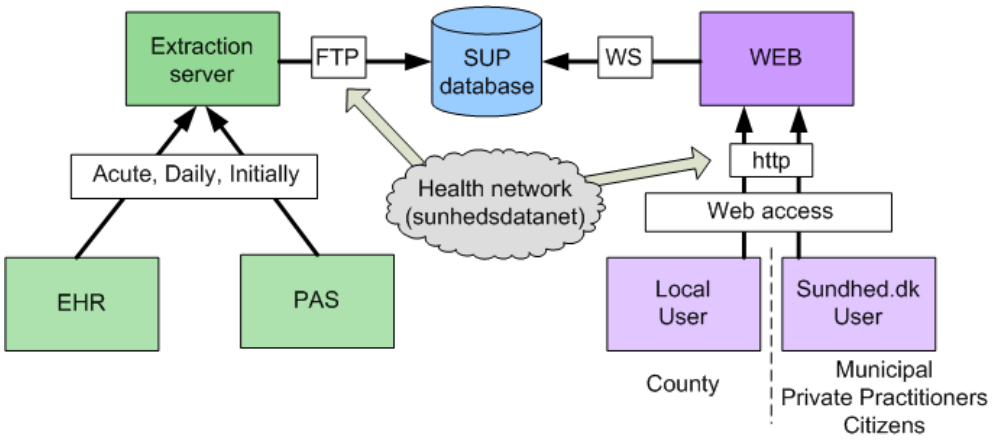


Fig. 4.1. Infrastructure in SUP

As can be seen from Figure 4.1, all communication regarding SUP is done in an encrypted way by means of MedCom's 'sunhedsdatanet'. Inquiries can either be done through the common governmental health portal Sundhedsportalen (Sundhed.dk) or through a local solution [Hulbæk 2005].

Consultant Jens Rahbek Nørgaard at MedCom has contributed with information about SUP via mail correspondence, in addition to the referred sources.

4.2.1 Stakeholders

MedCom is the initiator of the SUP project, but the interest group Danish Regions and Sundhedsportalen (sundhed.dk) have also been involved. At the present moment, seven counties at the provinces Jylland and Funen have participated so far. The system requirements have been produced by MedCom in co-operation with Vejle County.

A pilot project was implemented in 2002-2003 in the Vejle, Viborg and Århus Counties. The project is continued under MedCom's direction and the objective is to introduce SUP in all counties in Denmark.

The central, technical solution has been developed by IBM/Acure (supplier of the SUP-database), WM-data (supplier of the SUP-browser solution) and Vejle County (supplier of the operational environment).

4.2.2 Legislation

The *Act on Processing of Personal Data* and the *Patients' Rights Act* have been taken into consideration under the development of SUP. In addition, it has been necessary to receive special permission from the Danish authorities (the Data Protection Agency).

At the present moment, health personnel's possibility to access patients' hospital records via web has been closed by the Data Protection Agency, a situation which means that the implementation of SUP in several counties cannot become completed. This is now a political problem where the interest group Danish Regions criticises the government for not making a legal clarification in time. Danish Regions are expecting that the government either convinces the Data Protection Agency that they have been too strict, or that a legal alteration should be done.

The Data Protection Agency has stated that the launching of the planned system is difficult to make consistent with the requirements for personal protection in the Act on Processing of Personal Data. The Agency is also worried about the former approvals they have given SUP, and by this, permissions to exchange health information across organisational borders.

At the current moment, status is that it is technically possible to exchange health information between care providers in Denmark, but the application of the technology is limited because of legal restrictions [Danish Regions 2006].

4.2.3 Requirements

The requirements concerning security in SUP are included in Appendix E, Case 2. They will also be described in the next section concerning implemented system solutions.

4.2.4 System Solutions in SUP

Access Control in general

The two main groups of users in SUP are **health personnel** and **patients**. A role-based access control is used for health personnel where roles are defined on the basis of profession. Patients are allocated access based on personal identification.

Health personnel's right of access to SUP is decided by the hospital administration. Personnel who are allocated access are granted a personnel certificate.

As a patient, to be able to access own health information via Sundhedsportalen (sundhed.dk), it is necessary to hold a personal certificate. The certificate is issued by TDC A/S and is freely available for Danish citizens.

Emergency Access Control

The same paramount procedures for standard access control are used for emergency access control. Personnel state that there is an acute need for access to health information, and that there is no consent statement from the patient. The allocation of emergency access shall only be used when the patient is unable to give is consent. It is required that the patient is informed at a later moment. The allocation of access lasts for 30 minutes and is being logged.

Identification

As previously mentioned, SUP distinguishes between user identities for personnel and patients. The health personnel identities are every night authorised by means of synchronisation with the National Board of Health's personnel database.

Authentication

The SUP solution consists of several various components which can physically be in different organisational contexts. This means that the solution

shall be able to handle a number of different scenarios. (Examples of scenarios can be when external users (e.g. doctors from a different county) access a county's SUP-web application and SUP-database, or when external users use their own SUP-web application to access another county's SUP-database).

To be able to handle these scenarios, SUP makes use of a PKI solution with digital signatures by means of certificates called OCES (Offentlige Certifikater til Elektronisk Service). These certificates can be used for a number of public services in Denmark, i.e. applications for higher education and student loan, applications for day-care centres and posting of tax forms [National IT and Telecom Agency 2006].

At the present moment, there are two different authentication entries; via a simple web application or via Sundhedsportalen (Sundhed.dk). The web application is an interim solution before the work with the authentication mechanism via Sundhedsportalen is completed. In the web application, each user is created separately.

Health personnel are authenticated by means of a user identity and associated password, in addition to a personnel certificate with an associated private key. Patients are also authenticated with user identity plus password, but the certificate is a personal version with an associated private key.

Single sign-on is not yet implemented, but investigations on the subject have been made.

Logging

What shall be logged has been determined in accordance with the Act on Processing of Personal Data:

- point of time
- user
- type of usage
- report of which person that the information concerned, or used search criteria

The content is stated in local instructions which are approved by the Data Protection Agency. The log is analysed locally, but MedCom extracts specific information for compilation of statistics (e.g. number of logons, information distribution per month). If abnormalities are discovered, the local administrator contacts the involved users. The log is archived and kept for five years on a database server which can be accessed by MedCom. They are also responsible for the log.

The patient can access the log concerning his own health information via Sundhedsportalen (sundhed.dk).

Consent and exchange/sharing of information

For health personnel, in order to access a patient's data, the patient has to give his consent to this. In addition, there has to exist a care relation between the personnel and the patient. When health personnel try to access a patient's health information via the SUP-web application, they have to choose between the following alternatives:

- **Yes** - I have had the patient's consent for reading healthcare information
- **Acute** - I have an acute need for reading healthcare information
- **No** - I have no consent and I do not wish to continue

The choice being made is logged.

4.3 Case 3: Klinisk Portal

Klinisk portal, or Clinical Portal in English, is a portal developed at Rikshospitalet university hospital in Norway. By means of Internet technology, the portal links six disparate IT systems employed throughout the hospital and presents them in a united user interface. It also provides secure access for patients who want to examine their own medical data via web [Rikshospitalet 2006].

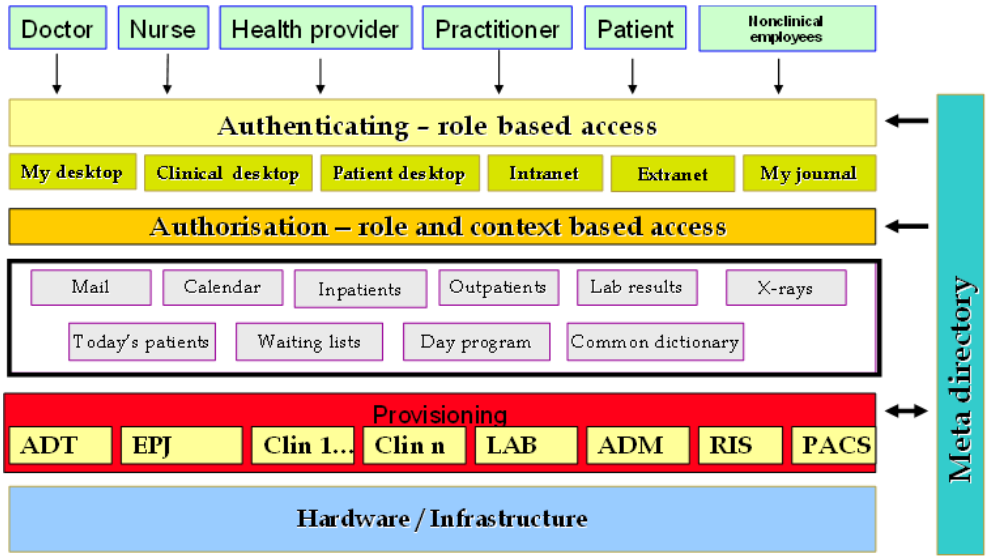


Fig. 4.2. Concept view: the security architecture in Klinisk Portal

As seen from Figure 4.2 (reproduced from [Buen 2005]), the interface consists of six different logical parts (marked in olive-green) divided into three different working areas; internal, external and administrative. This is further described in table 4.2.

Aksel Sogstad, Protection of Privacy Representative at Rikshospitalet and Sintef's research project 'iAccess' have, together with the referred sources, contributed with information concerning Klinisk Portal.

4.3.1 Stakeholders

Klinisk Portal has been developed by employees at the IT section at Rikshospitalet University Hospital. The development team has employed medical personnel at the hospital as managers and knowledge resources.

Table 4.2. The logical parts in Klinisk Portal

NAME	AREA	DESCRIPTION
My desktop	Internal	Non-clinical information for personnel
Clinical desktop	Internal	Overview of clinical information at the current ward
Patient desktop	Internal	Clinical information concerning a specific patient
Intranet	Administrative	Functions for hospital administration
Extranet	External	Information for co-operative personnel
My journal	External	Patient's access portal to own health information

4.3.2 Legislation

It has not been reported any legal hindrances of an extent worth mentioning, mainly because Klinisk Portal is a solution which so far is used within one hospital, only. Nevertheless, access to information between hospitals and across regional borders is still a challenge.

4.3.3 Requirements

Rikshospitalet University Hospital and the Norwegian Radium Hospital have together formed a Health Authority. At the present, Rikshospitalet University Hospital are doing a complete implementation of Klinisk Portal at the Norwegian Radium Hospital, and the workload on both system developers and administrators are extensive. Because of this, their possibilities to contribute to this thesis have been limited, and, amongst other factors, the requirements specification has not been available.

4.3.4 System Solutions in Klinisk Portal

Access Control in general

As shown in Figure 4.2, the authentication of users in Klinisk Portal is role-based. In addition, the access control mechanisms in the underlying systems of the portal are used to a large extent. The attributes 'organisational belonging', 'profession' and 'function' are used for authorisation in the access control.

Emergency Access Control

In principle, it is not possible for a user to access a journal through the portal if he does not have the patient in his access profile. A user who has not access to the ward a patient is associated with, can only find this person through searching by means of the patient's personalia and use emergency access (establish a temporary contact relation). The user has to state a reason. The reason will be logged together with all activity done.

Not all users have the right to do an emergency accessing, but all doctors and some nurses have the possibility. It has to be noted that even though this type of accessing is categorised as 'emergency access', it is used as a part of the general access control ('exception access' would probably be a better name in this context).

Identification

Users are authorised for access to services based on organisational belonging, role, profession and/or function. The portal uses LDAP catalogues for identity management, which makes it possible to synchronise user identities and passwords.

Authentication

Health personnel are authenticated by means of user identities and passwords which are common for all clinical systems (common password policy). Through Klinisk Portal, single sign-on has been implemented. Personnel receive a one-time password associated with their user identity via letter post. This is used the first time they logon, after which it has to be changed by the user.

Patients who want to get access to their health information via the patient portal 'Min Journal' are allocated access through strong authentication by means of a PKI solution (certificates). For the time being, the patient portal is available for only a small patient group.

Logging

Two different logs are connected to the portal; an activity log and an emergency access log. The activity log contains which user has accessed which journal at which time. The emergency access log contains who has done the accessing and why.

The logs are kept for at least three months, which is in accordance with the law. The logs are checked for unauthorised use either through sampling tests or concrete controls.

A patient has the right of inspection of the log concerning his health record, and therefore, logs can also be controlled on patients' requests. It is planned that the patient should be able to do this by himself via Internet (VPN).

Consent and exchange/sharing of information

Since Klinisk Portal only units several health care information systems within the same health authority, an explicitly given consent for information processing and distribution via the portal is not necessary.

4.4 Case 4: PlanBasert Samarbeidsjournal - SamPro

Pursuant to *Regulations relating to Individual Plans according to the Health Legislation*, persons with need for coordinated health services over a long period of time have the right to the formulation of an individual plan (IP) [Ministry of Health and Care Services 2004].

The purpose of the Norwegian SamPro project has been to develop an architecture and software pilot which support electronic interaction concerning individual plan. Information security has been a central problem area, and the project has developed solutions which provide access control and secure communication of sensitive health information over open networks in accordance with the health legislation [Røstad 2004].

The pilot is web-based and the plan-owner (patient) will have full access to his plan at any time, and he decides who else shall be given access.

Potential users of the system can include the plan-owner himself, health personnel, the plan-owner's closest friends and next of kin, and persons related to the plan-owner through social activities, work training etc.

In addition to the referred sources, system developer Edvard T. Helling at VismaUnique has contributed with information via mail correspondence.

4.4.1 Stakeholders

SamPro has been developed through a co-operative project between Sintef, Central Norway Regional Health Authority (RHA) and Hiadata AS (now Visma Unique), with financial support from the Directorate for Health and Social Affairs, Hiadata AS and the Research Council of Norway [Visma Unique 2006].

The web-based pilot has been tested in three different user environments in Central Norway RHA:

1 Namsos municipal in co-operation with Namsos Hospital, section for adult psychiatry and children's rehabilitation
2 Nordmøre and Romsdal Hospital Trust in co-operation with four local municipals for adults with mental sufferings over a long period of time
3 Trondheim municipal in co-operation with St Olav's Hospital Trust for rehabilitation for children and youth

4.4.2 Legislation

An individual plan is legally defined to be a part of the health record, and are therefore regulated by the Acts which applies for health records. But, in

addition, individual plans are regulated by the *Regulations relating to Individual Plans according to the Health Legislation*, and therefore, certain special rules apply. E.g. it is not necessary to apply for a licence from the Data Inspectorate to establish a plan register. It is also stated that health information shall be *shared* between the participators in the plan [Røstad 2004].

4.4.3 Requirements

Sintef was responsible for the security architecture in the first version of SamPro and developed a requirements specification which can be seen in Appendix E. These requirements have formed the basis for the current version developed by VismaUnique. The implemented version will be examined in the section below.

4.4.4 System Solutions in SamPro

Access Control in general

The access control in SamPro is role-based, meaning that all persons participating in the work with a plan are allocated a role. All roles are allocated a set of rights in relation to access to different information types. The rights which are possible to activate / deactivate are shown in table 4.3.

Table 4.3. The rights in SamPro

RIGHT	PROPERTY
New	Create an information element of this type
Read	Read information of this type
Write	Change information of this type
Delete	Delete information of this type
Delegate	Must hold this right in order to change rights
Print	Do a print
Role	Edit roles

The rights to a role can be overridden either on information type level or information element level (e.g. 'initiative' can be an information type, while an instance of 'initiative' is an information element).

Rights to a role are inherited. If the rights are not specified on an information element, it will inherit information type, which again can inherit from the role's rights on information type. A user cannot set rights which he does not hold.

Emergency Access Control

In SamPro, it is not relevant with emergency access because an individual plan does not contain detailed clinical information.

Identification

According to *Regulations relating to Individual Plans according to the Health Legislation*, a coordinator shall be responsible for the supervision of the plan. When a new plan is made, it will automatically be created two participators in the plan; the plan-owner and a coordinator.

The coordinator is allocated the role 'coordinator' which holds all rights in the plan. The plan-owner is allocated the role 'user' which has the rights 'new', 'read' and 'write'. The plan-owner and the coordinator can add participators to the plan and allocate rights to these.

Generally, the coordinator will have rights to create a user account for a participator. As a rule, it will also be the coordinator and the plan-owner who can delete a participator or change rights (the coordinator holds the rights, but deletions or changes are done in co-operation with the plan-owner).

Each establishment using the system has a local administrator which can allocate the following rights:

- Create a new plan
- Create a user account
- Add a person to an establishment
- Edit information concerning a person

A local administrator will generally not be participating in any plans.

Authentication

Authentication is based on security mechanisms in .Net (not further detailed in the available project documentation). The authentication of a user is done through two steps:

1. ASP.Net Forms authentication: user name and password
2. One-time pin code sent by mail or SMS

In the second step, the user can chose whether he will receive the one-time pin code via electronic mail or SMS. If the user chooses mail, he is informed about the password being sent uncrypted and the risks associated with such communication. This step will most likely be replaced by a PKI solution in the future.

Single sign-on is not relevant in this context since SamPro is a free-standing system not dependent on other clinical systems, e.g. EHR systems.

Logging

In SamPro, both authorised and unauthorised operations are logged. Typically, the person who did the operation, what was done and which element was the operation done on, are logged.

Participators can see changes in a plan based on the log and the associated rights each participator holds. The log is kept for indefinite time.

Consent and exchange/sharing of information

A foundation for all communication concerning an individual plan is the statement of consent. This statement consists of two parts;

- Consent to the establishment of an individual plan
- Registration of participators in the plan work who shall have access to the plan

Consequently, before an individual plan can be created, there shall be a written, informed consent from the user (plan-owner). Further, a participator's access rights to information in the plan are based on the plan-owner consenting to this (decision made together with the coordinator). The plan-owner can also decide that a participator only will have access to parts of the plan. In table 4.4, the status a consent can have is described.

Table 4.4. Consent status in SamPro

STATUS	DESCRIPTION
Zero position	Participators can be added and deleted and they can be allocated rights. Participators can view the contents of a plan, but it cannot be edited.
Valid	Participators can be allocated rights and plan can be edited. Participators can not be added or deleted.
Expired	Plan can be read only.

Only the plan-owner and a coordinator can have access to a plan which have an 'initialised' or 'expired' consent. A participator can participate for a limited period of time in the period consented to.

4.5 Case 5: Gemensam Vårddokumentation - GVD

Gemensam Vårddokumentation, meaning common health care documentation in English, is a project executed in Stockholm County in Sweden. The purpose is to make it easier for different care providers, e.g. a care centre and a hospital, to co-operate and exchange information within the county. Irrespective of which health institution the patient are in contact with, necessary and appropriate patient information shall be available to health care professionals in order to facilitate adequate care.

The vision is 'one patient - one record - through the whole life', meaning that all care providers taking part in a patient's care shall have access to the one and the same electronic patient record belonging to a patient through his whole life.

Through GVD, all care documents, e.g. electronic patient records and laboratory reports, will be collected in a database which is common for all medical services. When an employee logs in at his computer, he will only gain access to the information he is authorised to see.

The patient will also get a better general view of his contacts with different health services. Through a patient portal, a patient will have access to information concerning medication and laboratory reports, in addition to a medical booking service.

Seen from a technical perspective, GVD is an IT architecture, a technical platform and IT support. If the project's vision shall be real, all the enterprises' different IT systems have to be connected together to one common system. To some extent, the already existing IT systems can be adapted to operate within the frames of the new structure, but a great deal have to be altered [SLL 2006].

At the present moment, GVD is under development, and care providers will be connected to the service during autumn 2006. The support service BAT&Portal (further described in section 4.5.3) is now running as a pilot in test mode.

4.5.1 Stakeholders

Stockholm County Council is the initiator, financier and owner of GVD. Carelink, through the project Carelink PLUS (PLattformsUtveckling i Sverige), has also contributed to the project.

WM-Data, Brainpool and Oracle have developed the technical platform and the storage service. HewlettPackard has the responsibility for the development of an application - and logon portal including authorisation support-

ing services and logging. HP will also be responsible for training, support and operation.

4.5.2 Legislation

The project has taken the Swedish health legislation, and especially the *Secrecy Act, the Patient Register Act* and the *Act on Healthcare Records*, into consideration. There have not been any hindrances of larger importance, but a challenge is the rules for exchange of information, as discussed in section 3.9. Since GVD is developed for use primarily within Stockholm County, this is not a problem in the present situation.

4.5.3 Requirements

'BAT&Portal' is a support service that is developed parallel to GVD. The purpose with this service is to have a platform in readiness for uniform and effective administration and access control to applications within Stockholm County Council. Thus, many of the technical requirements concerning information security in BAT&Portal are representative for GVD and therefore, they are here presented as requirements for GVD directly. An extract from the requirements specification is given in E.

Figure 4.3 (rewritten from [SLL 2004b]) describes the parts in the BAT&Portal service which collaborate in a common architecture, indicated by yellow. The parts that are relevant in this context are marked with a darker yellow colour. Existing applications and systems are indicated by green.

4.5.4 System Solutions in GVD

Access Control in general

In this context, users shall be interpreted in a wide meaning; an entity which performs a certain activity on a certain resource. A user is typically a person, but can also be a software component, an application or a certain IT system which needs to execute a specific activity.

An authorisation model has been made in order to determine which access rights the user shall have. Possible attributes and objects in this model are:

- Role or user
- Resource (can be an application or a data object)
- Authentication context (in which context is the authentication done, e.g. which authentication method was used)

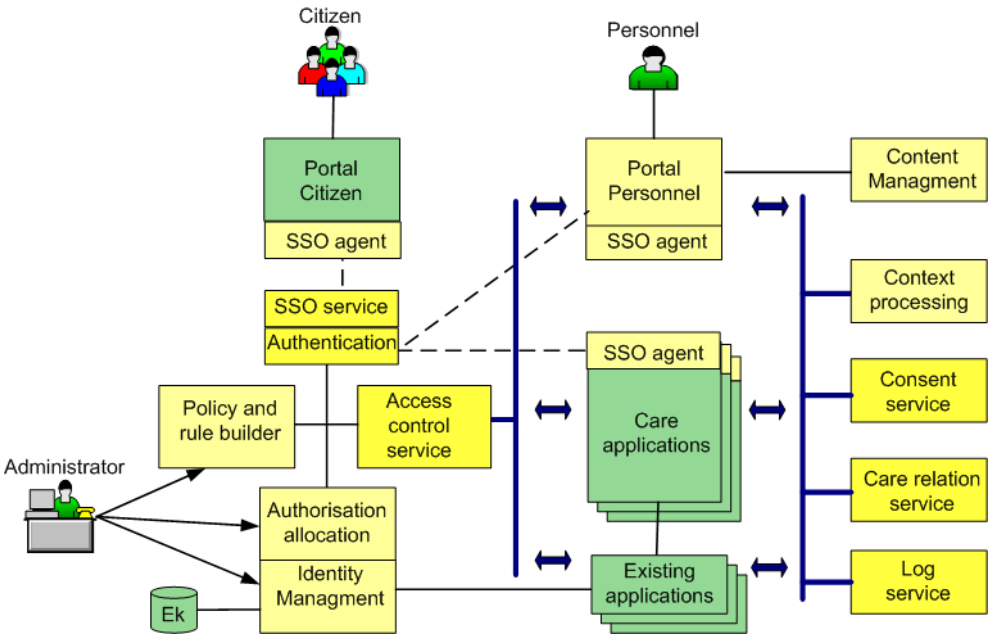


Fig. 4.3. The BAT&Portal architecture

- The user's organisational possession
- Requested emergency access

The reason for access rests upon the administration of the users' rights. The person or function responsible for the information should also control which roles or individuals who shall be allocated access. This means that the administration should be possible to do both centralised and decentralised. The administration can be minimized through the utilisation of roles, role hierarchies and inheritance of rights.

Emergency Access Control

In GVD, certain users, or users connected to certain roles shall be able to use emergency access in order to pass by authorisation hindrances and access necessary information.

Identification

In BAT&Portal, two different user groups are defined:

- **A physical person**
- **A system component**

The user group *physical person* is divided into two different roles:

- **Personnel** - persons who use BAT&Portal through their occupation.
- **Citizen** - patients or other private individual who need to access GVD's services.

These two roles log logically in through two different portals, as seen in Figure 4.3.

Initially, Stockholm County's electronic catalogue of personnel (EK) will support Bat&Portal with personnel information and thereby form the basis for a secure identification.

Authentication

Authentication will be done through different methods, but the main track will be PKI based logon and certificates. To achieve a successful realisation, there are made requests for flexibility and adaptivity, meaning that it should be possible to add and replace mechanisms. Other possible methods are user identities plus passwords and one-time passwords (e.g. distributed by means of SMS).

A PKI solution for health care called SITHS (Säker IT i Hälso- och Sjukvård), has been developed. It is based on HCC (Health Care Certificates) from specific SITHS-CAs. HCC shall be available in three different categories: personal, functional (system/server) and organisational certificate.

Bat&Portal will include a solution for single sign-on, meaning that the user, after logon, shall be able to navigate between connected applications which he has access to, without further logons or strengthening of identity.

Strictly speaking, SSO can be seen as a way to arrange/assure a user to be identified and authenticated. This can be done through a signed ticket containing information about the user, or it can be a packet including user identity and password which can be used for logon to the specific application.

SSO presupposes that there are components supporting automatic logon to the connected applications. Since different technical environments can be making different requirements on a SSO function, it is important that the solution is flexible and can handle various environments and situations.

Logging

The log service shall be able to log security related events, automatically consolidate and process the information, and also have in readiness a graphical user interface for looking through and do extractions from the log. It shall

also have functionality for archiving. Since the log itself can be sensitive, it is important that it also is handled securely.

A log message shall consist of:

- Message source, a named entity, which is used to describe where the message originates from
- Log level, i.e. the level of priority the message must have in order to be accepted and saved (Fatal, Error, Warn, Info, Debug or user defined).
- Log type which categories the message, (e.g. Application, Security and Event).
- The message

Consent and exchange/sharing of information

The consent service in BAT&Portal gives answers to whether a patient or next of kin has given his consent to distribution of health information between care organisations or not. The consent can limit which persons that can get access to the information, and also have a limited validity period. In those situations where the care information is classified, this shall be included as prerequisites in the consent.

The main responsibility for the consent service is to administer consents and guarantee their validity. A consent is actively given by the patient, and therefore, the registration of the consent cannot happen through an automatic procedure, - a graphical user interface must always be used. The consent information will form the basis for access control.

Documentation of the consent shall be happening at and be valid for the current care provider or by the care provider who requests the information. Henceforth, the consent will be documented and maintained by the patient himself.

The service shall be configurable both for actively and presumed consents. 'Actively' means that there has to be an actively registered consent if the service shall support distribution. 'Presumed' means that it is not necessary that a consent is registered for distribution to happen. The patient has always the possibility to drop the presumed consents and by this, block distribution of parts or all of his health information.

4.6 Case 6: Nationell Patientöversikt - NPÖ

In collaboration with Carelink, the county councils have created a national patient register pilot; Nationell Patientöversikt. The purpose of the project is to facilitate cooperation between different care providers in Swedish health care and to give the patient access to own health care information. In addition, it is an objective to establish common services in a health care IT infrastructure in Sweden.

The pilot version includes the following information:

- basic patient data
- patient's contact in primary care
- lab results from clinical chemistry
- x-ray results on textual format
- diagnosis
- prescribed medicine
- epicrises from institutional care
- log

For health personnel, in order to access health information, the patient has to consent to this. In addition, the pilot requests that the personnel are using the common services for logging, consent and connection of existing systems. Personnel can do a connection in order to only read, or both read and distribute information. In extraordinary circumstances, e.g. an emergency, will special access rules apply.

As seen from Figure 4.4 (rewritten from [Carelink 2005a]) and the subsequent table 4.5, the pilot consists of services for patient data processing and a connection layer to existing source systems and portals in the participating counties. In addition, services for the patient register, logging, consent and security are included [Carelink 2005a].

NPÖ has been running as a pilot since autumn 2005 and has recently been evaluated. The continuance of the project shall be based on the results of the pilot, but the exact development strategy is not yet determined.

In addition to the referred sources, Torbjörn Dahlin at Brainpool, one of the suppliers, has contributed with information through interviews.

4.6.1 Stakeholders

In 2004, all the county directors decided to develop Nationell Patientöversikt. The initiative was supported by the Association of Private Care Providers and the Swedish Association of Local Authorities and Regions. Carelink has

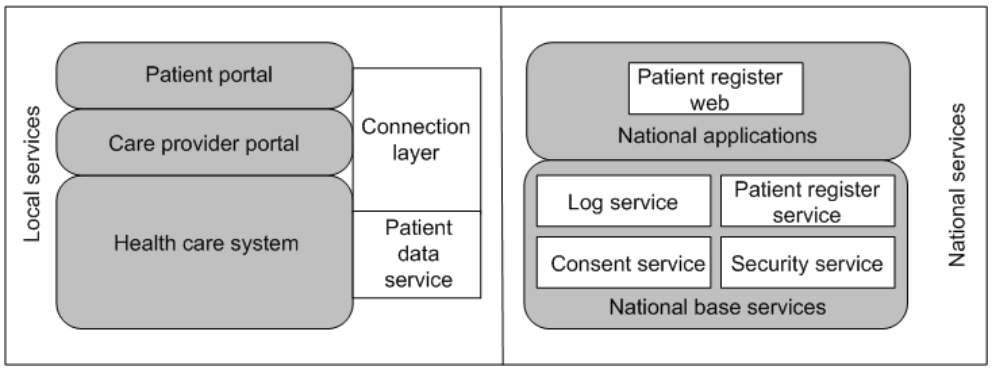


Fig. 4.4. Local and national services in the NPÖ architecture

Table 4.5. Services in Nationell Patientöversikt

SERVICE	DESCRIPTION
Patient register web	A generic service which forms the interface towards the user's IT environment. Connected to a health care information system from where the user in his ordinary graphical user interface starts the patient register service.
Patient register service	Collects health care documentation from all Patient data services and compiles them.
Patient data service	Reads data from an existing health register, translates the data to XML format and sends the data to the Patient register web.
Consent service	Assures that both the consent 1 concerning distribution in general and the specific consent 2 concerning each specific distribution instance, are valid.
Log service	Logs all transactions.
Security service	Issues tickets for each care provider who does a query. The qualification for receiving a ticket is that the user is authenticated and correctly authorised. The ticket is both an admission ticket for the various health care systems and a way to document who has requested what (it is logged).

had the responsibility for the implementation of the project, but seven different suppliers have contributed. The National Board of Health and Welfare, the Swedish Pharmacy Chain and health care representatives have been members of the managerial committee.

Four counties have connected to the pilot version; Norrbotten, Uppsala, Östergotland and Jönköping.

4.6.2 Legislation

A fundamental problem for NPÖ is the fact that, according to the legislation, it is not allowed to exchange information between authorities, which in practice means that information cannot be exchanged across county borders. In NPÖ, the solution has been to define the extracted information as a *view*, and not an *exchange* of the information. This results in a system where it is possible to display patient information, but not to change it. In addition, when the patient has consented to this form of distribution of his information, the process is considered legal.

Nevertheless, it is uncertain whether the chosen solution really are in accordance with the legislation, and it is therefore appointed a project group especially for the legal challenges. In parallel with the development of the pilot, the group has been working on proposals for amendments in the Swedish health legislation in a longer perspective. The result shall be used for input in the Patient Data Investigation, described in Appendix D.3.

The project group has done a wide interpretation of the current health legislation, resulting in a model where the patient himself decides if and how his health information shall be distributed to which care providers, when needs of care arise [Carelink 2005d]. A more thoroughly review of the limitations in the current legislation is found in section 5.6.

4.6.3 Requirements

Specified requirements concerning information security are shown in Appendix E, but are also described in the subsequent section concerning system solutions.

4.6.4 System Solutions in NPÖ

Access Control in general

The pilot of Nationell Patientöversikt does not have any own identification or authentication mechanisms, but rests on already existing mechanisms in the users' home IT environment.

Emergency Access Control

In a case of emergency, with specific logging routines, it is possible to access information without having the patient's consent. How this is solved in the pilot is not further described.

Identification

As shown in Figure 4.4, the pilot includes a security service which issues a ticket to each care provider when he has done a query. The prerequisite for achieving a ticket is that the user (health personnel or patient) is authenticated and is authorised to access the information included in the national patient register. The ticket makes it possible to document which information that has been requested by whom, meaning that it is being logged.

Authentication

The pilot does not contain any own authentication mechanisms, but relies on the underlying systems. This means that health personnel are authenticated in their 'home' health information system. If the authentication is approved here, they are also authenticated for NPÖ. This is further described in table 4.6, in addition to authentication of patients.

Table 4.6. Authentication in Nationell Patientöversikt

USER	METHOD
Health Personnel	When personnel make use of the patient register service (PRS), it is assumed that the local logon mechanism transparently controls the access to PRS and thereby authenticates the user. Identification happens through the local authorisation control system which issues a certificate or ticket. This gives the user access.
Patients	Patients are authenticated through one of two methods: a The first alternative is used by patients holding citizen certificates in order to be authenticated towards the patient portal in PRS. The portal verifies the certificate against a Certificate Authority and gives the patient access to PRS. The portal does a control towards an internal list of acceptable national identity numbers to assure that not anyone who holds a citizen certificate shall get access to PRS. b The second method is used by patients with generated one-time passwords in order to be authenticated towards the patient portal, where authorised patients and their national identity numbers are already registered. If the user is authorised for PRS, he is granted access. Both methods assume that the patient portal controls the access to the patient register service.

Logging

As seen in Figure 4.4, one of the base services in the pilot is logging. NPÖ logs all accessing of information, while the counties log all information they distribute. The following will be included in the log:

- Occupation or title
- County, clinic, unit
- Time of information extraction
- Information amount that has been sought

The patient has access to his own access log indicating which care providers have accessed his information.

Logging happens both centrally and distributed, but without any connection between each other (time stamps etc).

Consent and exchange/sharing of information

In order to make a patient's documentation of former received care available for other care providers than those involved, the patient has to consent to this. Further, when the patient is in need for care and visits a care provider hitherto unknown of the patient's health status, the patient can consent to allocate access to his health information for the care provider.

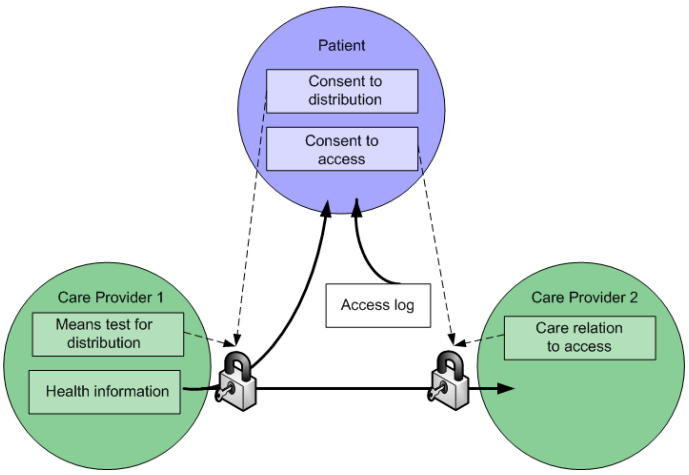


Fig. 4.5. Mechanisms for distribution of and access to data in NPÖ

As seen from Figure 4.5 (rewritten from [Carelink 2005a]), access is managed through the two following consent steps:

1 The patient consents to distribution of information. Then, the care provider does a means test which can result in restrictions in what to be distributed to other care providers and to the patient himself. The means test is done once only and for the entire information set. The consent and the means test are documented at the care provider responsible for the means test. It cannot be displayed in the system that the patient is registered before this consent is given.
2 In the next step, the patient will give his consent to other care providers accessing the information. This consent will both be documented by the distributing care provider and the providers who are allocated access. In a case of emergency, with specific logging routines, it is possible to access information without having the patient's consent. The accessing is documented in a log which is available to the patient. The second consent has to be given in every single case and to every care provider that shall take part in the distribution. On request, the consent is submitted verbally. Both consents are registered in the system.

❖ 5

Comparison of Projects

In this chapter, each case will be examined thoroughly concerning information security aspects. It will also be discussed whether the implemented version differs from the requirements specification, and the possible effects if a difference is found. In addition, potential improvements will be proposed for each case.

At the end of the chapter, a comparison of the projects in tabular form will be presented (see table 5.1).

5.1 Case 1: InterRegionale SygehusKommunikationsprojekt - mini-IRSK

It has not been stated explicit security requirements in connection with the mini-IRSK project, but previous requirements concerning secure communication have been considered to be sufficient. These requirements have unfortunately not been available from MedCom. Therefore, an evaluation of the specified requirements compared with the implemented system cannot be done.

The project has just been set in operation. Since it makes use of existing security mechanisms, it is difficult to do a thorough investigation of the chosen solutions. Something which can be commented, are the verbally given consent. In those situations where the patient's consent are necessary in order to exchange health information electronically, the consent should be documented, e.g. in the patient's health record.

It has to be noted that it is surprising that there has not been recorded any explicit security requirements for this project. Even though the existing requirements are considered to be adequate, this should be documented in the project description. Based on this, it is difficult to make any proposals for improvements.

5.2 Case 2: Standardiseret Udtræk af Patientdata - SUP

The requirements specification included in Appendix E concerning SUP is an updated edition and is in accordance with the current version of the pilot.

The pilot is now under implementation in seven counties. As mentioned in section 4.2.2, the Danish Data Protection Agency has temporarily stopped the implementation because of information security reasons. When the pilot is implemented after the plan, 3 500 doctors will be able to access hospital records belonging to approximately two million citizens. The agency finds that the solution conflicts with the regulations in the Act on Processing of Personal Data, and especially the parts concerning implementation of appropriate technical and organisational security measures [Danish Data Protection Agency 2006].

The main problem is the fact that all doctors who are authorised to access the system, also can access all health records, even when there is no care relation between the doctor and the patient. The security mechanisms for avoidance of unathorised use are the patient's consent and the log; the latter can be accessed by the patient himself. But, these are mechanisms which detects improper use after the harm has been done. The system does not have any preventive mechanisms except for the general authentication process. A more restrictive authorisation model would be appropriate, e.g. requiring a care relation between the doctor and the patient before the doctor is authorised for access.

Another weakness is the interim one-factor authentication mechanism used at the present moment. This mechanism authenticates health personnel (so far only doctors) by means of user identities and passwords. Based on the number of patients involved, a one-factor authentication mechanism is too weak, even though it is a temporary solution.

Proposals for improvements:

- Only authorise doctors for access to a patient's record after a care relation has been proved. E.g. register a relation when an epicrisis is sent to personnel in primary care and/ or let the patient administrate the relations himself. All relations should be time-limited.
- Start to use the strong authentication mechanism by means of certificates and access via Sundhedsportalen from the beginning of the pilot period (avoid the interim one-factor solution).

5.3 Case 3: Klinisk Portal

The requirements specification for Klinisk Portal has not been available due to the system developers' limited possibilities to contribute with information to this thesis because of extensive workload. Therefore, an evaluation of the specified requirements versus the implemented system cannot be executed.

Summarised, Klinisk Portal appear as a well-secured system for its area of application. If there shall be indicated some possible areas for strengthening of the security, there can be called attention to the mechanism for authentication of health personnel. This one-factor mechanism is based on user identities and passwords. In addition come the entrance cards necessary for personnel in order to psychically enter a building, but these are not directly connected to the authentication process. There are many well-known risks concerning passwords (easy to guess, written down in order to remember, shared between colleagues, reused etc), and it would therefore be beneficial to strengthen this authentication with a second factor, e.g. biometric methods. Of course, the authentication process must be seen in relation to user-friendliness.

Emergency access, or 'exception access' as would be a more appropriate term in this context, is used as a part of normal access control. This means that the utilisation of this function is quite widespread. An advantage is that all accessing of this type are explicitly logged. But, from an information security point of view, it would be advantageous to limit this use to a minimum, but this requires extensive changes in the fundamental authorisation model. A further discussion of the matter is too comprehensive to be included in this thesis.

A challenge for the future can be exchange and also sharing of information between hospitals and other health care organisations, e.g. primary care institutions, via Klinisk Portal.

Proposals for improvements:

- Increase the authentication mechanism for personnel from one-factor to two-factor on a minimum
- Limit the use of emergency access

5.4 Case 4: PlanBasert Samarbeidsjournal - SamPro

All requirements as described in Appendix E concerning SamPro are implemented, except from requirement 4.3.2 ('The system shall support inte-

gration towards existing user databases in the domain'). A PKI-solution, as mentioned in requirement 4.2, is not implemented, either.

The first version of SamPro went through internal investigations, risk- and vulnerability analyses, and an examination done by the Norwegian Data Inspectorate. New security requirements were made, and the present edition is a developed version where the security is well ensured. Still, there is one part that can be improved; the mechanism used for authentication of participators in a plan.

In a larger time-frame, a reasonable solution would be to make use of a PKI solution for the authentication, as is planned. Hopefully, the underlying reason for the so far deficient realisation is that one wants to benefit from the planned national PKI standard.

The provisional authentication solution is a strong mechanism by means of user identity, password and a one-time pin code. The pin code is sent to the user by SMS or by uncrypted mail. The latter alternative has been investigated in a risk analysis, and was found to be adequate as long as the user is informed of the risks. The objection to this solution must be that a plan has several users, i.e. plan-owner, coordinator and various participators. These users may have a different personal view on information's degree of sensitivity, and by this, the extent of the risk for unauthorised use. Most likely, it is the plan-owner who finds the information most valuable, and therefore, it ought to be his decision whether pin codes can be sent uncrypted or not, and not a choice which can be made by each participator.

Proposals for improvements:

- Implement national PKI-solution when this is fully-developed
- In the meantime; allow only transference of one-time pin code via SMS, or
- Let plan-owner decide whether it should be possible to send the pin code uncrypted via mail

5.5 Case 5: Gemensam Vårddokumentation - GVD

The support service BAT & Portal (Behörighetsadministrativ tjänst & Portal), shall offer a service for effective and uniform administration and control of access to health applications in Stockholm County. This means that the solution calls for both scalability and flexibility, resulting in several alternatives, e.g. authentication by means of PKI, user identities plus passwords, or one-time passwords (portwise mID). Unfortunately, exact status on which parts

that is implemented and what functions they include, has been difficult to obtain from the suppliers. But, the implemented version does not differ from the requirements specification in a large degree.

The overall impression of the system is positive, and the choice of security solutions appears to be very well-founded and also satisfactory.

Proposals for improvements:

- Define routines for emergency access more clearly

5.6 Case 6: Nationell Patientöversikt - NPÖ

The current version of the pilot fulfils most of the requirements as stated in Appendix E. But, some of the requirements concerning traceability (6.1.2 and 6.1.4) are so far not satisfactory fulfilled. In addition, it is mentioned that emergency access shall be possible 'with specific logging routines'. How this are to be solved is not further defined.

One of the great benefits from a national patient register ought to be the possibility for accessing health information originating from another health organisation in a case of emergency. Even though this is a pilot version, the fact that routines for such accessing is not defined, have to be considered a weak point.

Other weaknesses are the identification of users and the authentication mechanisms. The current authorisation control consists of a trust in the existing information source systems' controls. E.g. validation of national identity numbers is not done. There are not made any specific requirements to the existing mechanisms, either.

No data are saved centrally, but are extracted locally from source systems each time an inquiry is done. This may lead to situations where data are unavailable, delayed or lost because of errors in the source system or under transference.

The log does not identify a user by user identity, but via a ticket issued by the system when the user is authorised. Since the reliability of the authentication mechanisms can be discussed, the log cannot be seen as trustworthy, either. In addition, logging happens both centrally (inquires in NPÖ) and locally (distribution from source systems), but these logs are not synchronised.

A conclusion on the project pilot work done by the project group is that the security level has to be raised. This conclusion is shared with the Data Inspection Board. An auditing of the project has been done by the independent consulting firm Gartner, and they have pointed out the handling of security as the weakest part. Therefore, parallel with the further development of

the Nationell Patientöversikt, there ought to be done a collective work including specification, developing and implementation of a common security solution.

Another hindrance is the current legislation. In the project, a working group focusing on health legislation has examined the possibilities for distribution and exchange of health care information. The group has made the conclusion that the current legislation is hard to interpret, and, because of this, is not applied the same way by all care providers. The patient's right to access documentation concerning received care which are stored at different care providers, is not fulfilled in an adequate way, as long as the exchange is done by means of paper versions. At the present moment, it is practically impossible for the patient to have in readiness an updated version of his documentation concerning received care by another provider. The reason for this is the slowness in the distribution processes [Ståhl and Andersson 2005].

If the pilot shall be used by large patient groups, especially the routines for consent have to be changed. Legally, there should not be necessary with the first step of the current consent process (having to consent to distribution of information in general). A patient consenting to distribution of information in each specific case should be adequate regarding protection of the patient's personal integrity [Carelink 2005d].

Proposals for improvements:

- Define how emergency access shall be done. At the present moment, this shall happen by means of 'specific logging routines'. Logging routines are useful for detecting unauthorised use after it has happened, but appropriate configuration of the access control, and hereby emergency access, is more important in order to *prevent* unauthorised access.
- Implement own authentication mechanisms, alternatively make concrete requirements on the existing mechanisms (strong authentication as a minimum).
- Synchronisation of logs.
- Abolish the first consent step in order to decrease administration, both for personnel and patients (necessary with legal amendments).

5.7 Comparison in Tabular Form

On the subsequent pages, a summary of the previously done comparison will be presented in tabular form.

Table 5.1. Comparison of the six projects concerning information security

	Case 1: mini-IRSK	Case 2: SUP	Case 3: Klinisk Portal	Case 4: SamPro	Case 5: GVD	Case 6: NPÖ
Access control in general						
Access attributes	Role.	Role.	Organsational belonging, role, profession, function.	Role.	Role or user, organisational possession, resource (application or a data object), authentication context, requested emergency access	Does not have any own access control (rests on existing mechanisms in users' home IT environment).
Allocation of access	Administrated locally at source systems.	Health personnel: by means of a personnel certificate granted by hospital administration Patients: by means of a personal certificate granted by authorities.	Health personnel: user administration grants access on personnel aministrator's request Patients: by means of a PKI solution.	Local administrator allocates access to main roles (patient and coordinator). Further, these allocate to other roles (participators).	The person or function responsible for the relevant information should control which roles or individuals shall be allocated access. Both centralised and decentralised administration should be possible. Patient's consent part of access control rules.	Does not have any own access control (rests on existing mechanisms in users' home IT environment).
Emergency access						
How	Administrated locally at source systems.	Same paramount procedures as for standard access control, plus registration of acute need of information.	User finds patient through searching by means of the patient's personalia and establishes a temporary contact relation. The user has to state a reason.	[Not relevant]	Possible if the user/role has the necessary rights (not further defined).	By means of specific logging routines (not further described).
By whom	Administrated locally at source systems.	Doctors.	Doctors, some nurses.	[Not relevant]	Certain users, or users connected to certain roles.	[Unknown]
Time-limited	Administrated locally at source systems.	30 minutes.	[Unknown]	[Not relevant]	Possible to set time limitations.	[Unknown]
Identification						
Identity Management	Administrated locally at source systems.	Local database.	metacatalog (LDAP).	Local administrator.	Stockholm County's electronic catalogue of personnel (EK).	Identities managed in home environment.
Authorisation of identity	Administrated locally at source systems.	Synchronised with the National Board of Health's database every night.	Based on organisational belonging, role, profession and/or function.	Coordinator authorises participators. Rights to a role are inherited.	User's rights determined on basis of authorisation model. Rrole hierarchies and inheritance of rights.	The user is issued a ticket if he is correctly authorised and authenticated in his home-environment.

Continued on next page

	Case 1: mini-IRSK	Case 2: SUP	Case 3: Klinisk Portal	Case 4: SamPro	Case 5: GVD	Case 6: NPÖ
Authentication						
Technology	PKI (for authentication to the 'Sundhedsdatanet').	PKI.	PKI or user identity plus password.	Based on security mechanisms in .Net.	PKI and/or user identity, password plus one-time pin.	Does not have any own authentication mechanism (rests on existing mechanisms in users' home IT environment).

Type	Strong. By means of user identity and password, plus certificate.	Strong. Two steps:
		1. User identity and password
		2. Certificate (*personnel* or *private person* version) and associated private key
		At the present moment, a temporarily two-factor mechanism for personnel by means of user identification and passwords are used.
			Two-factor (personnel), strong (patients):
			- Health personnel: user identity and password
			- Patients: PKI solution (certificates)
				Strong. Two steps:
				1. User name and password
				2. One-time pin code sent by mail or SMS
					Various alternatives. Stronger authentication gives higher rights:
					- User name and password
					- One-time pin code sent by SMS
					- Certificates:
					  - Personnel: HCC (Health Care Certificates)
					  - Patients: Citizen certifcates
						Various alternatives:
						Health personnel
						- assumed that home-environment transparently authenticates user
						Patients (one of the following):
						- Citizen certificate verified by CA. National ID of holder controlled towards list of accepted national identity numbers.
						- Patient already authorised and national ID registered. Uses a one-time password.

Single sign-on	No.	No.	Yes.	[Not relevant]	Yes. Shall be possible to use several applications without further logons or strengthening of identity.	No.
Logging						
Transaction types	All.	All.	All (Two logs: activity and emergency access).	All	Security related events. Central log service logs all applications connecting to the service.	All.
Content	- User - Type of usage - Point of time - Person that the information concerned or used search criteria	- User - Type of usage - Point of time - Person that the information concerned or used search criteria	Activity log: user, record, time stamp Emergency access log: user, record, reason, time stamp.	User, operation, information element concerned, time stamp.	Log message: Message source, log level, log type which categories the message, the message, time stamp.	Occupation or title, county, clinic and unit, time stamp, information that has been sought.

Continued on next page

	Case 1: mini-IRSK	Case 2: SUP	Case 3: Klinisk Portal	Case 4: SamPro	Case 5: GVD	Case 6: NPÖ
Logging						
Storage time	Min. six months.	Five years.	Min. three months (in practice for indefinite time).	Kept for indefinite time.	Information out of date is archived. Local system owner decides for how long.	[Unknown]
Auditing routines	Analysed locally.	Analysed locally. Local administrator contacts involved users if abnormalities are discovered.	Checked for unauthorised use either through sampling tests or concrete controls.	[Unknown]	Automatically consolidate and process the information. Operators shall electronically be informed about detected events.	Functions for follow-up and inspections of log are planned, but not implemented yet.
Patient's access rights	Locally administrated.	Via Sundhedsportalen.	On request. Planned to be done via Internet (VPN).	Can see changes based on the log.	[Unknown]	Via the system.
Consent and exchange / sharing of information						
Difference between *exchange* and *sharing*	Yes. Information can only be exchanged.	Yes. Information can only be exchanged.	No. The portal unites information and makes both exchange and sharing possible within a hospital.	Yes. Regulated through the rights *Read* and *Write*.	No.	Yes. Information can only be exchanged.
Application of consent	Exchange of health information.	Health personnel accessing health information.	[Not Relevant] (Consent implicitly given for the system)].	Patient consents to: 1. Establishment of plan 2. Allocating access to participators in plan	Distribution of health information between care organisations. Two types: - Actively: there has to be an actively registered consent - Presumed: not necessary that a consent is registered for distribution to happen	Patient consents to: 1. Making documentation of former received care available 2. Accessing in each specific case
Type	Verbally.	Written.	[Not Relevant] (Consent implicitly given for the system)	Written.	Written.	Written or verbally.
Time-limited	[Unknown]	Consent has to be registered at each accessing.	[Not Relevant] (Consent implicitly given for the system).	Yes, through different statuses.	Yes. Shall be valid for relevant care provider. Documented and maintained by the patient himself.	First step done once, second step done in each single case.
Comments						
Planned improvements			Patient shall be able to access 'his' log via Internet (VPN)	The second authentication step will most likely be replaced by a PKI solution.		Legal amendments should make consent step 2 redundant.

❖ 6

Analysis and Discussion

Through this thesis, it has become evident that technological solutions within health care are dependent on external conditions. In this chapter, both the external conditions and the resulting technological solutions will be discussed.

6.1 External Conditions

A principal difference between the three countries is the organisation of health care, where Sweden stands out with a relatively large number of counties, and where each county generally has a higher degree of autonomy than what is the case in Denmark and Norway. This is necessarily not negative, but the need for a common foundation concerning terms, classifications and technical standards becomes clearer. In the GVD project, there has become evident how important it is to define a common concept platform, something which is now in progress within Stockholm County. This is positive, but the work should be lifted up to a national level.

For the time being, there is no common, defined EHR standard in Sweden, which makes project like NPÖ more difficult to carry through. A national standard has been made in Norway, but it is not compulsory to implement it. Nor has there been allocated any funds by the government for the implementation. Still, most central suppliers have taken it into their future development plans. Denmark is ahead with their national concept model 'G-EPJ'. The model is under implementation, and the work is supported by the government, together with health care interest groups.

A positive observation is the fact that all countries have developed a national IT strategy for health care.

The two Swedish projects, GVD and NPÖ, can both be seen as extensive and ambitious as regards system functions and number of users. They are

also of those cases most in need for legal amendments in order to fully implement the planned solutions. But, comprehensive projects of this type can be just what might actuate the legal alteration work necessary to achieve a more wholly interaction picture in Swedish health care. A result of the NPÖ project is a report used as input to the ongoing Patient Data Investigation. This governmental investigation shall examine all health legislation concerning patient information and result in a proposal for amendments, including the premises for and the usefulness of creating a united health record for each patient. The result of the investigation will be of great importance for the future work with the Nationell Patientöversikt (NPÖ) and Gemensam Vårddokumentation (GVD) in Sweden.

In Denmark, the legislation opens for exchange independent of organisational borders, but the technical solutions made so far are not yet sufficient to make information distribution applicable in a large scale. The SUP project, which can be seen as the first step towards one virtual health record for each patient, has been closed temporarily by the Danish Data Protection Agency because of deficient adequate information security mechanisms.

The problem is classic seen from an information security point of view: the access control, where the goal is to determine who shall be able to access which resources they need in order to provide care, and nothing more, nor less, is not restrictive enough. In SUP, all doctors are given access to a disproportionate number of records, disclosing more sensitive information than necessary.

The interest group Danish Regions have declared that they find the Danish Data Protection Agency's interpretation of the legislation too strict. Based on the extent of this project and the number of patients involved, such a restrictive attitude is appropriate in order to ensure personal integrity. In addition, the technological solution has potential for improvements concerning the access control and the authorisation model.

Exchange of information across organisational borders is possible in Norway also, as long as the organisations are members of the same regional health authority. Therefore, none of the two Norwegian projects have been restrained by the legislation. This is also connected to the projects' scope; Klinisk Portal is developed for use at one hospital organisation, meaning that information is not exchanged across organisational boundaries at all. SamPro arranges for interaction concerning an individual plan, and is the project which is closest to implementing functionality for electronic sharing of health information. But, individual plans are regulated by an own reg-

ulation which says that information shall be shared between various care providers, and also which providers that are supposed to participate. This is what makes sharing possible from a legal point of view. Since there is no such Act or regulation for sharing of electronic health records, this is more difficult to carry out.

Sharing of parts or a complete health record between several health organisations have not yet been tested in Norway. It would be of great interest to see how an implementation of a project like SUP or NPÖ would turn out, and whether any legal hindrances would stop it, like in Denmark. A recently started Norwegian project called 'electronic medical card' shall develop solutions for exchange of automatic medical messages between a general practitioner and cooperating authorities such as home nursing care, hospitals and pharmacies. Possibly, the project will have parts in common with SUP. But, it is still on an early stage, and therefore, it is difficult to foretell any outcomes. Nevertheless, it will be very interesting to see the results.

When it comes to exchange and sharing across national borders, it is legally possible as long as the country has implemented the EU Directive 95/46/EC concerning processing of personal data and the free movement of such data. All the three countries have done the implementation, and therefore, theoretically, there are no formal reasons in the way. But, as seen in this thesis, exchange and sharing within each country are still not easy to carry through. Therefore, solutions for electronic exchange and sharing of health information across national borders are unrealistic for the time being.

An ever returning legal challenge is the fine line between personal integrity and effective health care by means of information technology. IT can make it easier for health personnel to co-operate, both within an organisation and between several organisations. Information which follows the patient through various health processes will make health care more efficient and of better quality, and by this, increase the patient safety. But, when it is opened for a larger throughput of information between various providers, the chance of infringements of the personal integrity unfortunately increases.

As seen in Sweden, the restrictive information exchange regulations in order to ensure personal integrity, and especially the Secrecy Act, have laid ties on the possibilities to implement new technology solutions. The same has just happened with SUP in Denmark, but in this case, the relationship between personal integrity and patient safety are a bit more balanced. And this is the core of the problem; to define where the balance line shall be.

A common tendency in Scandinavia is to a higher degree focus on the patient and his needs and rights. In the spirit of this process, it might be appropriate to explore the patient's viewpoint and find out whether most patients prefer personal integrity or information availability when they are in contact with health care. A natural evolution would be to enhance the patient's autonomy, meaning that he shall be able to take part in the decision of where the balance line shall be. The patient should be able to determine to which degree his information can be exchanged electronically, and also in which situations it is most important to protect the personal integrity.

But, from a realistic point of view, when developing new solutions, it is important to include the group of users who do not have the competence or knowledge necessary to administrate own health information. The objective with health care is to help people, and a natural part of this will be to avoid setting the technological standards too high for the ordinary user. Therefore, increasing the patient's autonomy can be positive in many situations, but adequate alternatives have to exist in parallel.

6.2 Technological Solutions

In the previous section, there has become evident that the development of technological solutions is limited by external conditions. But, it has also become known that the solutions itself are not always satisfactorily implemented regarding secure information processing, even though the legislation is not a hindrance.

When making technological choices, again, the national perspective is of great importance. All three countries have a health net used for secure communication between health organisations. In addition, Denmark has introduced a national PKI solution used for several public services. Sweden's SITH (Säker IT i Hälso- och Sjukvård) solution are under development. SITH is specifically made for health care because of the high security requirements concerning health information. Norway has had an ongoing PKI project for several years, but the project is still not fully implemented yet. This solution is also specific for the health care sector. These are positive initiatives, but it can be advantageous to include other high sensitive information services in the future, like the Danish solution.

Concerning other authentication mechanisms, some of the projects have chosen interim solutions while pending on authentication by means of PKI. Unfortunately, it has been discovered that some of these solutions make use of one-factor mechanisms, normally based on user identities and passwords.

Even though the projects are running as pilots 'only', they still process sensitive information concerning live patients. In this context, a mechanism based on only one factor for authentication cannot be considered anything else than too weak.

Another finding is the discovery of some of the projects' insufficient descriptions of requirements on emergency access solutions. Generally, access control of a user is easy to define; the user is either authorised to access the information, or not. But within the health care sector, situations arise when exceptions to the standard access control rules have to be made. One of the strengths of these systems would therefore be to implement concrete rules on how emergency access shall be allocated and revoked. Many of the projects have well-defined logging routines which make it possible to disclose when emergency access has been abused, but detecting mechanisms, e.g. better authorisation models, should also be included.

When it comes to logging, all the projects have well incorporated routines, both for logging and auditing / administration. In all three countries, the patient has the right to see the log concerning his health information. Four of the projects have implemented or are planning to implement functionality for the patient to access the content of the log, which is very positive.

The chosen solutions for registration and maintenance of patient's consent differ a bit from each other. The project where the patient is most autonomic is SamPro. Here, via the plan portal the patient allocates access rights for health personnel and decides which information each one shall be able to see. In GVD, the patient will also document and maintain consents himself, but in addition, there is a consent called *presumed* where it is assumed that the patient will consent to distribution. In SUP, the patient's consent has to be registered, but the registration is done by the health personnel. Generally, in accordance with the tendency of increasing patient autonomy, the patient should be able to administrate his consents by himself to the highest possible extent.

❖ 7

Conclusion and Future Work

In this chapter, a final conclusion will first be presented, followed by proposals for future work. At the end, a review of the work with this thesis will be given.

7.1 Conclusion

Through this thesis, it has become evident that health care in the Scandinavian countries Denmark, Norway and Sweden are upon the whole equally organised and struggle with many of the same legal and technological challenges.

All three countries' health legislation promotes personal integrity, with Sweden as the most expressive. Nevertheless, there is a tendency towards enhancement of the patient's autonomy and a request for more united health care processes, requiring the information to follow the patient through the health services in a higher degree. This evolution leads to needs for new types of technological tools which arrange for exchange and sharing of information, and thereby making it easier for health personnel to co-operate. Again, this has resulted in higher requests for information security solutions, where one of the most extensive challenges is to find the balance between personal integrity and the availability of information independent of time and location.

In order to meet these requests, the need for common national technological standards, concepts and infrastructure within health care has become more important, something which has been illustrated in this thesis. Denmark is in several areas ahead of their neighbouring countries, and many factors indicate that the reason for this is their ability to co-operate on a national plan.

In addition, the systems made have to be in accordance with Acts and regulations. Parts of the prevailing legislation are to a hindrance for exchange of information across organisational borders, and particularly the Swedish health legislation is in need for amendments. Sharing of health information, and especially by means of one health record for each patient used by several care providers, are nearly impossible to achieve in practice with the legal situation in Scandinavia of today.

The technological solutions chosen within the scope of the limiting external conditions are generally well-defined, high quality systems which have information security in focus. Still, there has become evident that some weak points exist, like one-factor authentication mechanisms for health personnel. The fact that the projects have been running as pilots is not an excuse when the information is as sensitive as it is in this context. Therefore, there is room for improvements in order to increase the information security.

In order to make health care of higher quality and ensure information security to an even larger degree, legal amendments and a more extensive national co-operation will arrange for the possibility of developing better information security solutions.

7.2 Future Work

When it comes to future work in general, there are many interesting problems which can be further investigated.

An objective in all three countries is to arrange for electronic co-operation and interaction, both within and across organisational borders. Denmark and Sweden have tested out national solutions for exchange of information with varying success so far. The national perspective is of course important, but investigations in Sweden have discovered that a majority of care cases concerns patients connected to the county that provides the care. In addition, the number of acute care cases outside the patient's home county amount to only 5 percent of the total number [Carelink 2005c]. Based on the many similarities in the organisation of health care in Scandinavia, these numbers are most likely transferable to Denmark and Norway too.

With these facts as basis, organising for exchange and sharing can be done through different models. One solution is to limit exchange on a regular basis to happen within a county / region. Solutions for national exchange can be activated when exceptions arise, e.g. a patient is referred to a health care provider which is located outside his home county. In this case, the patient can consent to exchange, thereby opening for distribution of his information

on a national plan. The patient should be able to administrate consents via web. A prerequisite would be that the consent is informed, stated after consultation with health personnel, and also time-limited. When the patient is not capable of doing the administration himself, responsible health personnel should.

Another possible solution is to develop a central overview of the patient's case history by means of an electronic lifeline. Every single contact the patient has had with health care, from primary care to hospitalisation, is registered centrally. From the lifeline, it is possible to obtain more information concerning each case by being redirected to the information locally saved at each care provider. Also here is the patient in charge of which information shall be available to whom; the patient should decide which care providers shall be able to access which cases at which time. Generally, the cases in the lifeline are listed chronologically, but it should also be possible to sort on care provider or type of case, i.e. disease. By such a solution, the challenge will be to implement a common authentication mechanism for accessing from the centrally stored lifeline to the locally stored data. Also, avoiding errors during transference of data can be a problem.

A third alternative can be to classify health information according to their degree of importance. Essential lifesaving information like Cave and serious diseases or injuries can be stored centrally in a register. The rest of the patient's health information is kept on a smart card held by the patient. A backup of the card should be kept e.g. by the patient's general practitioner. When it comes to research purposes, the patient can consent to registration of his information in anonymised records.

This idea requires that the patient takes responsibility for his own information. Unfortunately, this is a solution which cannot be used by everyone. Those which is not capable of safeguard their own information should be given other options. The authentication mechanisms and emergency access routines are also of vital importance in this model. In addition, the classification of information could be a challenge.

These and similar solutions will avoid health records being accessible at any time by a disproportionate number of health personnel. Still, they will arrange for better cooperation by means of technology across organisational borders, while at the same time give the patient more ownership of own information. Information security has to be in focus if suggestions like these shall be realisable. A prerequisite is also the utilisation of common security

mechanism, e.g. PKI solutions for authentication and restrictive authorisation models.

As regards future work concerning this thesis in particular, it would be of great interest to conduct a similar case study between countries which have a much more differentiated picture regarding organisation of health care and definition of legislation, and also cultural aspects, e.g. Scandinavia and an Asian country with well-established health care. Most likely, there would be discovered larger dissimilarities than what has been found in this thesis. Based on new and different external conditions, this could contribute with other approaches concerning technological solutions which possibly could be adopted. Also, the experiences made through this thesis could be useful in such a context.

7.3 Review of own Work

This thesis' scope has been large and possibly to extensive. Even though there was made concrete limitations concerning information security aspects, the studied information material has been comprehensive. In addition, the legal part became a challenge since this was a new field to the author.

Also, the data collection was challenging. Information concerning the two Swedish cases was obtained by means of live interviews, while in the Danish and Norwegian cases, mail correspondence was used. The first is definitely preferable, since written conversation turned out to be both limiting and imprecise. Some of the questions in the interview guide were inadequate, which resulted in insufficient answers. In addition, a few of the projects had limited possibilities to contribute with information due to heavy workload.

All things considered, working with this thesis has been very interesting and informative, and has emphasised the need for the involvement of factors like law, organisation structures and standards when implementing information security solutions.

References

[Alberts and Dorofee 2002] Alberts, C. and A. Dorofee (2002). *Managing Information Security Risks: The OCTAVE Approach* (1. ed.). Addison Wesley.

[Bishop 2003] Bishop, M. (2003). *Computer Security: Art and Science* (1. ed.). Addison Wesley.

[Buen 2005] Buen, L. E. (2005). Sikkerhetsarkitektur - klinisk portal. *ITA Datasenter*.

[Carelink 2005a] Carelink (2005a). Exekutiv rapport. *Nationell patientöversikt*. http://www.carelink.se/files/doc_2006111151435.pdf (Internet 2006-05-02), in Swedish.

[Carelink 2005b] Carelink (2005b). Kravspecifikation för pilotversion - version 1.11. *Nationell patientöversikt*.

[Carelink 2005c] Carelink (2005c). NPÖ - långsiktig innehåll. *Nationell patientöversikt*. http://www.carelink.se/files/doc_20051018085507.pdf (Internet 2006-06-17), in Swedish.

[Carelink 2005d] Carelink (2005d). Slutrapport steg 2, Regelverksgruppen. *Nationell patientöversikt*. http://www.carelink.se/files/doc_2005928091802.pdf (Internet 2006-06-04), in Swedish.

[Danish Data Protection Agency 2000] Danish Data Protection Agency (2000). Act on Processing of Personal Data. *LOV nr. 429 af 31/05/2000*. http://www.datatilsynet.dk/eng/index.html (Internet 2006-02-20).

[Danish Data Protection Agency 2006] Danish Data Protection Agency (2006). Privatpraktiserende lægers adgang til e-journal. http://www.datatilsynet.dk (Internet 2006-06-12, in Danish).

[Danish EHR Observatory 2005] Danish EHR Observatory (2005). Statusrapport 2005, EPJ-Observatoriet. http://www.epj-observatoriet.dk/ (Internet 2006-04-21), in Danish.

[Danish Regions 2006] Danish Regions (2006). Patienterne betaler prisen. http://www.arf.dk/Nyhedscenter/Pressemeddelelser/2006/PatienterneBetalerPrisen.htm (Internet 2006-06-08, in Danish).

[European Parliament 1995] European Parliament (1995). Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *L 281 , 23/11/1995 P. 0031 - 0050*.

[The Folketing 2002] The Folketing (2002). The register act (arkivlov). *LOV nr 1050 af 17/12/2002*. http://www.retsinfo.dk/DELFIN/HTML/A2002/0105030.htm (Internet 2006-05-25, in Danish).

[Galliers and Land 1987] Galliers, R. D. and F. F. Land (1987). Choosing Appropriate Information Systems Research Methodologies. *Communications of the ACM, Issue 11, 30*, 900–902.

[Grimson, Grimson, and Hasselbring 2000] Grimson, J., W. Grimson, and W. Hasselbring (2000). The SI challenge in health care. *Communications of the ACM, Issue 6, 43*, 48–55.

[Hancock 1998] Hancock, B. (1998). An Introduction to the Research Prcess. *Trent Focus for Research and Development in Primary Health Care, United Kingdom*. http://www.trentfocus.org.uk/Resources/using_interviews_research_project.htm (Internet 2006-04-11).

[Hulbæk 2005] Hulbæk, L. (2005). MedCom IV sådan gik det. *MedCom det danske sundhedsdatanet / December 2005 / MC-S203*.

[ISO 2005] ISO (2005). ISO/DTR 20514 Electronic Health Record Definition, Scope and Context. http://www.openehr.org/standards/t_iso.htm (Internet 2006-04-20).

[KITH 2006] KITH (2006). Kompetansesenter for IT i helse- og sosialsektoren AS. http://www.kith.no/ (Internet 2006-04-20, in Norwegian).

[Madsen 2004] Madsen, H. B. (2004). Tavshedspligt og videregivelse af helbredsoplysninger mv. i sundhedsvæsenet. *Juristen nr. 1, 2003*. http://www.djoef.dk/online (Internet 2006-05-31, in Danish).

[Mathers, Fox, and Hunn 1998] Mathers, N., N. Fox, and A. Hunn (1998). Using Interviews in a Research Project. *Trent Focus for Research and Development in Primary Health Care, United Kingdom*. http://www.trentfocus.org.uk/Resources/using_interviews_research_project.htm (Internet 2005-11-03).

[MedCom 2003] MedCom (2003). Projektbeskrivelse for MedComs SUP Projekt. http://www.medcom1-4.dk/mc4/sup/SUPProjekbeskrivelse.pdf (Internet 2006-06-08, in Danish).

[MedCom 2004] MedCom (2004). SUP-Specifikationen - Version 2.0. http://www.medcom1-4.dk/mc4/sup/standarder/sup_spec20.asp (Internet 2006-06-12, in Danish).

[MedCom 2005] MedCom (2005). Elektronisk kommunikation mellem sygehusafdelinger. http://www.medcom1-4.dk/publikationer/publikationer/Mini-IRSK.pdf (Internet 2006-06-11, in Danish).

[Ministry of Health and Care Services 1999a] Ministry of Health and Care Services (1999a). The Act relating to Patients' Rights (the Patients' Rights Act). *LOV-1999-07-02-63*. http://odin.dep.no/hod/english/doc/legislation/acts/048051-990011/dok-bn.html (Internet 2006-04-05).

[Ministry of Health and Care Services 1999b] Ministry of Health and Care Services (1999b). The Health Personnel Act. *LOV-1999-07-02-64*. http://odin.dep.no/hod/engelsk/regelverk/p20042245/042051-200005/index-dok000-b-n-a.html (Internet 2006-04-04).

[Ministry of Health and Care Services 2001] Ministry of Health and Care Services (2001). Act on Personal Health Data Filing Systems and the Processing of Personal Health Data (Personal Health Data Filing System Act). *LOV-2001-05-18-24*. http://odin.dep.no/hod/engelsk/regelverk/p20042245/042041-990016/dok-bn.html (Internet 2006-03-28).

[Ministry of Health and Care Services 2004] Ministry of Health and Care Services (2004). Forskrift om individuell plan etter helselovgivningen og sosialtjenesteloven. http://www.lovdata.no/ (Internet 2006-05-15, in Norwegian).

[Ministry of Justice 1998] Ministry of Justice (1998). Information on the Personal Data Act. *Factsheet Article no. Ju 98.05*. http://www.datainspektionen.se/pdf/faktablad/ju-fakta-eng.pdf (Internet 2006-03-23).

[Ministry of Justice and the Police 2000] Ministry of Justice and the Police (2000). Act relating to the Processing of Personal Data (Personal Data Act). *LOV-2000-04-14-31*.

http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf (Internet 2006-02-20).

[Ministry of the Interior and Health 1999] Ministry of the Interior and Health (1999). National strategi for IT i sygehusvæsenet 2000-2002. http://www.im.dk/publikationer/sum-it/sum-it.pdf (Internet 2006-04-20).

[Ministry of the Interior and Health 2000] Ministry of the Interior and Health (2000). Bekendtgørelse om sikkerheds-foranstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning. *BEK nr 528 af 15/06/2000*. http://www.retsinfo.dk/DELFIN/HTML/B2000/0052805.htm (Internet 2006-05-25, in Danish).

[Ministry of the Interior and Health 2002] Ministry of the Interior and Health (2002). Health care in Denmark. http://www.im.dk/publikationer/healthcare_in_dk/healthcare.pdf (Internet 2006-05-26).

[Ministry of the Interior and Health 2003] Ministry of the Interior and Health (2003). Bekendtgørelse om lægers pligt til at føre ordnede optegnelser (journalføring). *BEK nr 846 af 13/10/2003*. http://www.retsinfo.dk/DELFIN/HTML/B2003/0084605.htm (Internet 2006-05-25, in Danish).

[Ministry of the Interior and Health 2005] Ministry of the Interior and Health (2005). The health act (sundhedsloven). *LOV nr 546 af 24/06/2005*. http://www.retsinfo.dk/DELFIN/HTML/A2005/0054630.htm (Internet 2006-05-25, in Danish).

[National Board of Health and Welfare 2006] National Board of Health and Welfare (2006). Socialstyrelsens termbank. http://app.socialstyrelsen.se/termbank/ (Internet 2006-04-20, in Swedish).

[National IT and Telecom Agency 2006] National IT and Telecom Agency (2006). Digital signatur. http://www.digitalsignatur.dk (Internet 2006-06-10, in Danish).

[Nohlberg and Åhlfeldt 2005] Nohlberg, M. and R.-M. Åhlfeldt (2005). System and Network Security in a Heterogenous Healthcare Domain: A Case Study. *In Proceedings of the 2005 Security Conference, Las Vegas, USA*.

[NOMESCO 2005] NOMESCO (2005). Health Statistics in the Nordic Countries 2003. http://www.nom-nos.dk/ (Internet 2006-05-01).

[Ohnstad 2003] Ohnstad, B. (2003). *Taushetsplikt, personvern og informasjonssikkerhet i helse- og sosialsektoren* (3. ed.). Gyldendal Akademisk.

[Rikshospitalet 2006] Rikshospitalet (2006). Opererer for fremtiden nå. http://www.rikshospitalet.no (Internet 2006-06-08, in Norwegian).

[Roberts 1997] Roberts, A. (1997). Social Science History for Budding Theorists [web edition]. *Empiricism, Theory and the Imagination*. http://www.mdx.ac.uk/www/study/glothi.htm#Induction (Internet 2005-11-03).

[Røstad 2004] Røstad, L. (2004). Juridiske betraktninger rundt elektronisk samhandling om individuelle planer etter helselovgivningen. *SINTEF Tele og Data*.

[Røstad, Øystein Nytrø, Moe, Stav, and Skylstad 2004] Røstad, L., Øystein Nytrø, N. B. Moe, E. Stav, and G. Skylstad (2004). Sikkerhetsarkitektur for PlanBasert Samarbeidsjournal v.2.0. *SINTEF Tele og Data*.

[SFS 1949] SFS (1949). The Freedom of the Press Act. *(1949:105)*. http://www.riksdagen.se/templates/R_Page____6313.aspx (Internet 2006-03-22).

[SFS 1980] SFS (1980). The Secrecy Act. *(1980:100)*. http://www.notisum.se/rnp/sls/lag/19800100.HTM (Internet 2006-03-22, in Swedish).

[SFS 1982] SFS (1982). The Health and Medical Service Act. *(1982:763)*. http://www.sweden.gov.se/content/1/c6/02/31/72/5ef21912.pdf (Internet 2006-03-22).

[SFS 1998a] SFS (1998a). The Act on Healthcare Records. *(1998:544)*. http://www.notisum.se/rnp/sls/lag/19980544.HTM (Internet 2006-03-23, in Swedish).

[SFS 1998b] SFS (1998b). Personal Data Act. *(1998:204)*. http://www.datainspektionen.se/pdf/ovrigt/pul-eng.pdf (Internet 2006-02-20).

[SLL 2004a] SLL (2004a). Bat & portal - förfrågningsunderlag, version 1.0. *Stockholms Läns Landsting*.

[SLL 2004b] SLL (2004b). Beskrivning av stödtjänster - bat&portal. *Stockholms Läns Landsting*.

[SLL 2006] SLL (2006). Gemensam Vårddokumentation. *Stockholms Läns Landsting*. http://www.sll.se/w_GVD/155592.cs?dirid=155823 (Internet 2006-03-10).

[SOSFS 1993] SOSFS (1993). Patient register act (patientjournallagen). *Socialstyrelsens föreskrifter och allmänna råd 20*.

http://www.sos.se/sosfs/1993_20/1993_20.htm (Internet 2006-03-23, in Swedish).

[SOU 2006] SOU (2006). Patientdatautredningen. *Statens offentliga utredningar*. http://www.sou.gov.se/patientdata/ (Internet 2006-06-12, in Swedish).

[Stake 2005] Stake, R. E. (2005). *The Sage Handbook of Qualitative Research* (3. ed.)., Chapter Qualitative Case Studies. Sage Publications, Inc. 443-481.

[Ståhl and Andersson 2005] Ståhl, I. and T. Andersson (2005). Slutrapport. *Nationell patientöversikt*. http://www.carelink.se/files/doc_2005127133953.pdf (Internet 2006-06-05), in Swedish.

[Swedish Data Inspection Board 2000] Swedish Data Inspection Board (2000). Information om vårdregisterlagen. *Datainspektionen informerar 5*. http://www.datainspektionen.se/pdf/skrifter/nr5.pdf (Internet 2006-03-23, in Swedish).

[Visma Unique 2006] Visma Unique (2006). Unique sampro oppfyller kravene til individuell plan. http://www.sampro.no/ (Internet 2006-05-15, in Norwegian).

[Utbult, Holmgren, Larsson, and Lindwall 2004] Utbult, M., A. Holmgren, R. Larsson, and C. L. Lindwall (2004). Patientdata - brist och overflöd i vården. *Teldok Rapport 154*, 33–43.

❖ A

Appendix A: Interview Guide

Stakeholders

1. Which stakeholders have been involved in the project?
2. Who has made the requirements?
3. Is it possible to get access to the requirements specification?

Legislation

1. Which laws and regulations has it been necessary to make allowance for under the development?
2. Have any parts in the legislation been a hindrance? If so, which parts?
3. If yes to question 2), which 'workarounds' did you chose?

Technical infrastructure - Information Security

1. **Access Control in general**
   a) Which type of access control is used:
      [ ] Built-in
      [ ] External
      [ ] Others, describe:
   b) Is the access control dependent on other systems:
      [ ] None
      [ ] Database
      [ ] Ldap
      [ ] Service
      [ ] Others, describe:
   c) Allocation/revocation of access:
      i. How (technically)
      ii. By whom (who decides)

   d) Emergency access:
      i. How (technically)
      ii. By whom (who decides)
      iii. Time span
2. **Identification**
   a) Which types are used in the system:
      [ ] Users
      [ ] Groups
      [ ] Roles
      [ ] Combinations/others, describe:
   b) How are these types (users, groups, roles, others):
      i. defined
      ii. allocated
      iii. revoked
3. **Authentication**
   a) Which authentication mechanisms are used:
      [ ] Passwords
      [ ] Challenge-response
      [ ] Biometrics
      [ ] Multiple methods or others
      i. Describe the mechanism:
   b) Administration of authentication:
      i. How is distribution done, e.g. password
      ii. Maintenance, e.g. frequent password changes etc.
   c) Is Single Sign-On implemented? If yes, how:
4. **Logging**
   a) What is the content of the log report (e.g source, timestamp, type, level of priority):
   b) What is being logged (e.g accessing, changes, error corrections, others):
   c) Auditing
      i. How is the log analysed
      ii. Notification of abnormalities
   d) Routines for notification of abnormalitites:
   e) How is archiving of the log done:
   f) Who has the responsibility and who administrates the log:
   g) Has the patient right to get access to the log:
5. **Distribution/exchange of Information**
   a) How is distribution of sensitive health information done:
      i. within an organisation

   ii. between several organisations
   iii. is the distribution dependent on patient's consent
b) How is exchange of sensitive health information done:
   i. within an organisation
   ii. between several organisations
   iii. is the distribution dependent on patient's consent
c) How is the patient's consent given:
   i. How is registration done
   ii. When and how is status updated/maintained

❖ **B**

Appendix B: Terms

DANISH TERMS

Act on Processing of Personal Data	Lov om behandling af personoplysninger
The Danish Data Protection Agency	Datatilsynet
Danish Regions	Amtsrådsforeningen
The Folketing	Folketinget
The Health Act (unofficial name)	Sundhedsloven
MedCom	Samarbejdsorganisation mellem myndigheder, organisationer og private firmaer med tilknytning til den danske sundhedssektor
Ministry of the Interior and Health	Indenrigs- og Sundhedsministeriet
National Board of Health	Sundhedsstyrelsen
National IT and Telecom Agency	IT- og Telestyrelsen
Statutory order concerning doctors' duty of keeping orderly notes (keep records) (unofficial name)	Bekendtgørelse om lægers pligt til at føre ordnede optegnelser (journalføring)
Statutory order concerning security measures for protection of personal data which is processed for the public administration (unofficial name)	Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning
The Patients' Rights Act	Lov om patienters retsstilling
The Register Act (unofficial name)	Arkivlov

Norwegian Terms

Act relating to Patients' Rights	Lov om pasientrettigheter
Central Norway Regional Health Authority	Helse Midt-Norge
The Data Inspectorate	Datatilsynet
The Directorate for Health and Social Affairs	Sosial- og helsedirektoratet
The Health Personnel Act	Lov om helsepersonell m.v.
KITH - Norwegian Centre for Informatics in Health and Social Care	Kompetansesenter for IT i helse- og sosialsektoren
Ministry of Government Administration and Reform	Fornyings- og administrasjonsdepartementet
Ministry of Health and Care Services	Helse- og omsorgsdepartementet
Ministry of Justice and the Police	Justis- og politidepartementet
Ministry of Labour and Social Affairs	Arbeids- og inkluderingsdepartementet
Act relating to the Processing of Personal Data	Lov om behandling av personopplysninger
Personal Health Data Filing System Act	Lov om helseregistre og behandling av helseopplysninger
The Act relating to Public Supervision of the Health Service (unofficial name)	Lov om statlig tilsyn med helsetjenesten
Regulations on the Processing of Personal Data	Forskrift til personopplysningsloven
Regulations relating to Patients' Medical Records	Forskrift om pasientjournal
The Research Council of Norway	Norges forskningsråd
Regulations relating to Individual Plans according to the Health Legislation (unofficial name)	Forskrift om individuelle planer etter helselovgivningen
Regulations relating to the Processing of Personal Data (unofficial name)	Forskrift om behandling av personopplysninger

SWEDISH TERMS

The Association of Private Care Providers	Vårdföretagarna
Carelink	National cooperation to develop the use of IT in Swedish healthcare
Citizen Certificate (unofficial name)	Medborgarcertificat
County council	Landsting
County council district	Landstingskommun
County director	Landstingsdirektör
The Freedom of the Press Act	Tryckfrihetsförordningen
Health care principals	Vårdhuvudman
The Act on Healthcare Records	Vårdregisterlagen
The Health and Medical Service Act	Hälso- och sjukvårdslagen
Health and Medical Services (Professional Activity) Act	Lag om yrkesverksamhet på hälso- och sjukvårdens område
Ministry of Health and Social Affairs	Socialdepartementet
The National Board of Health and Welfare	Socialstyrelsen
SITHS	Säker IT i Hälso- och Sjukvård
The Secrecy Act	Sekretesslagen
The Patient Register Act	Patientjournallagen
The Personal Data Act	Personuppgiftslagen
The Swedish Association of Local Authorities and Regions	Sveriges Kommuner och Landsting
The Swedish Data Inspection Board	Datainspektionen
The Swedish Pharmacy Chain	Apoteket AB

❖ C

Appendix C: Definitions

In this appendix, first, the term *Electronic Health Records* will be described. Then, key terms in Scandinavian health legislation will be defined.

C.1 Electronic Health Records

In the ISO standard 'Electronic Health Record Definition, Scope and Context', the basic-generic definition for the EHR is

> *a repository of information regarding the health status of a subject of care, in computer processable form*

This definition makes no assumptions about the health system of any country or region, or the type or granularity of information in the record. The definition is thought to be broadly applicable to all health sectors, health disciplines, and methods of health delivery [ISO 2005].

Denmark

In the national IT strategy for health care in Denmark, an electronic health record is defined as follows:

> *a clinical information system which directly supports daily process oriented examination, treatment and care of each individual patient*

[Ministry of the Interior and Health 1999, definition translated from Danish].

Norway

According to KITH, based on The Health Personnel Act and Regulations relating to Patients' Medical Records, an electronic health record can be defined as:

> *an electronically kept collection or collocation of recorded/registered information concerning a patient in connection with health care*

[KITH 2006, definition translated from Norwegian].

Sweden

The National Board of Health and Welfare has defined a health record as the following:

> *notes which are done and documents which are created or received in connection with care, and include information concerning a patient's state of health or other personal circumstances*

[National Board of Health and Welfare 2006, definition translated from Swedish]. The Patient Register Act is supposed to be technology neutral, and all legislation concerning health records in general are therefore understood to be prevailing also for electronic versions.

Electronic Health Records in this Context

As seen above, the three countries use slightly different definitions. The main difference is that the Norwegian and Swedish terms chiefly follows the ISO standard by describing a collection of information about a patient, while the Danish term defines an EHR to be a clinical information system. Based on these dissimilarities, it is in this context appropriate to distinguish between an electronic health record and an electronic health record system:

> Electronic Health Record (EHR): *a collection of digitally saved information about a person with the objective to support and contribute to a continuous patient course*

> Electronic Health Record System (EHR System): *an electronic data processing system, which can update and maintain electronic health records. The system has functions which makes it possible for qualified personnel to share information in a secure and user-friendly way.*

(Definitions inspired by The Danish EHR Observatory 2005).

The term *EHR* is not universally defined in literature. It has siblings as 'Electronic Medical Records' (EMR), 'Computerized Patient Record' (CPR) and 'Medical Records Systems, Computerized' (MeSH), amongst others. According to the ISO standard previously mentioned, EHR is now well established internationally, and this definition will therefore be used in this thesis [ISO 2005].

C.2 Key Terms in Scandinavian Health Legislation

In table C.2, relevant key terms in Scandinavian Health Legislation are defined. The table below shows abbreviations for sources referred to in the definitions in table C.2.

Table C.1. Abbreviations used in table C.2 with descriptions

ABBREVIATION	DESCRIPTION
Danish	
D-HA	Health Act
D-HC	Health care in Denmark [Ministry of the Interior and Health 2002]
D-PD	Act on Processing of Personal Data
D-PS	Act on Patient Safety in the Danish Health Care System
Norwegian	
N-HP	The Health Personnel Act
N-DF	Personal Health Data Filing System Act
N-PD	Personal Data Act
N-PR	Act relating to Patients' Rights
Swedish	
S-PD	Personal Data Act
S-HM	The Health and Medical Services Act
S-PR	The Patient Register Act
S-HMP	The Health and Medical Services (Professional Activity) Act
S-ST	Socialstyrelsens termbank [National Board of Health and Welfare 2006]

Table C.2. Legal terms in Scandinavian health legislation

TERM	DENMARK	NORWAY	SWEDEN
Consent	Any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed [D-PD]	Any freely given, specific and informed declaration by the data subject to the effect that he or she agrees to the processing of personal health data relating to him or her [N-DF]	Every kind of voluntary, specific and unambiguous expression of will by which the registered person, after having received information, accepts processing of personal data concerning him or her [S-PD]
Data Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data [D-PD]	The person who determines the purpose of the processing of personal health data and which means are to be used, unless responsibility for such data control is specially prescribed in the Act or in Regulations laid down pursuant to the Act [N-DF]	A person who alone or together with others decides the purpose and means of processing personal data [S-PD]
Data Subject (D,N) / Registered Person (S)	Identified or identifiable natural person [D-PD]	The person to whom personal health data may be linked [N-DF]	A person to whom the personal data relates [S-PD]
Data Processor (D,N) / Personal Data Assistant (S)	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller [D-PD]	The person who processes personal health data on behalf of the data controller [N-DF]	A person who processes personal data on behalf of the controller of personal data [S-PD]
Health Care (N,S) / Treatment (D)	Examination, diagnosis, clinical treatment, rehabilitation, specialist health care and prophylactic health care measures in relation to the individual patient [D-PS]	Acts which have a preventive, diagnostic, therapeutic, health-preserving or rehabilitating effect and are carried out by health personnel for the purposes of nursing and care [N-PR]	Measures which includes examination, treatment, consultation or nursing (translated from Swedish; 'vård') [S-ST]

Continued on next page

TERM	DENMARK	NORWAY	SWEDEN
Health Personnel	Persons who are authorised according to specific legislation concerning performance of health care related duties, and persons, who act on their responsibility (translated from Danish; 'sundhedspersoner') [D-HA]	1) Personnel with an authorisation pursuant to section §48 or a licence pursuant to section §49 in [N-HP] 2) Personnel in the health services or in pharmacies who perform acts as mentioned in the third paragraph 3) Pupils and students who in training as health personnel perform acts as mentioned in the third paragraph [N-HP]	1) Persons who are licensed to a profession within the health care sector 2) Personnel who are working at hospitals or other health establishments and participate in care of patients 3) Persons who otherwise assist licensed personnel in providing care 4) Personnel who are associated with 'Apoteket Aktiebolag' 5) Personnel at emergency service centres 6) Persons who otherwise according to regulations provides services in their profession under a temporary visit in Sweden without having a Swedish license for this profession (translated from Swedish) [S-HMP]
The Health (and Medical) Service(s)	Can be divided into 2 sectors; primary health care and the hospital sector. The primary sector deals with general health problems and its services are available to all. The hospital sector deals with medical conditions which require more specialised treatment, equipment and intensive care. [D-HC]	The primary health service, the specialist health service and the dental health service [N-PR]	Measures for the medical prevention, investigation and treatment of disease and injury. Health and medical services also include ambulance services and the care of deceased persons. Special provisions apply concerning dental care [S-HM]
Patient	[not explicitly defined in the documentation studied in this context]	A person who contacts the health service requesting health care, or to whom the health service provides or offers health care as the case may be [N-PR]	A person who receives or is registered for receiving health care (translated from Swedish; 'patient') [S-ST]

Continued on next page

TERM	DENMARK	NORWAY	SWEDEN
Personal Data	Any information relating to an identified or identifiable natural person ('data subject') [D-PD]	Any information and assessments that may be linked to a natural person [N-PO]	All kinds of information that directly or indirectly may be referable to a natural person who is alive [S-PD]
Personal Data Filing System	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis [D-PD]	Filing systems, records, etc. where personal data is systematically stored so that information concerning a natural person may be retrieved [N-PO]	[not explicitly defined in the documentation studied in this context]
Processing (of personal data)	Any operation or set of operations which is performed upon personal data, whether or not by automatic means [D-PD]	Any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses [N-PO]	Any operation or set of operations which is taken as regards personal data, whether or not it occurs by automatic means, for example collection, recording, organisation, storage, adaptation or alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction [S-PD]
Sensitive Personal Data	Personal data revealing a) racial or ethnic origin, b) political opinions, c) religious or philosophical beliefs, d) trade union membership, e) data concerning health or sex life [D-PD]	Information relating to a) racial or ethnic origin, or political opinions, philosophical or religious beliefs, b) the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act, c) health, d) sex life, e) trade-union membership [N-PO]	Personal data that reveals a) race or ethnic origin, b) political opinions, c) religious or philosophical beliefs, d) membership of a trade union, e) health or sex life [S-PU]

Continued on next page

TERM	DENMARK	NORWAY	SWEDEN
Third country	Any state which is not a member of the European Community and which has not implemented agreements entered into with the European Community which contain rules corresponding to those laid down in Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [D-PD]	Not explicitly defined, but understood as a country which is not a member of the European Union and which has not implemented Directive 95/46/EC [N-PO]	A state that is not included in the European Union or part of the European Economic Area [S-PD]

❖ D

Appendix D: Swedish Legislation - Relations, Problems and Amendments

Swedish health care is regulated by various acts, regulations and statues. The Health and Medical Service Act(1982:763) concerns health care in general. It's goal is to assure the entire population of good health and care on equal terms, by providing health and medical services [SFS 1982]. In addition, there are five specific acts which effects electronic health records in particular; The Freedom of the Press Act, The Secrecy Act, The Patient Register Act, The Act on Healthcare Records and The Personal Data Act [Utbult, Holmgren, Larsson, and Lindwall 2004].

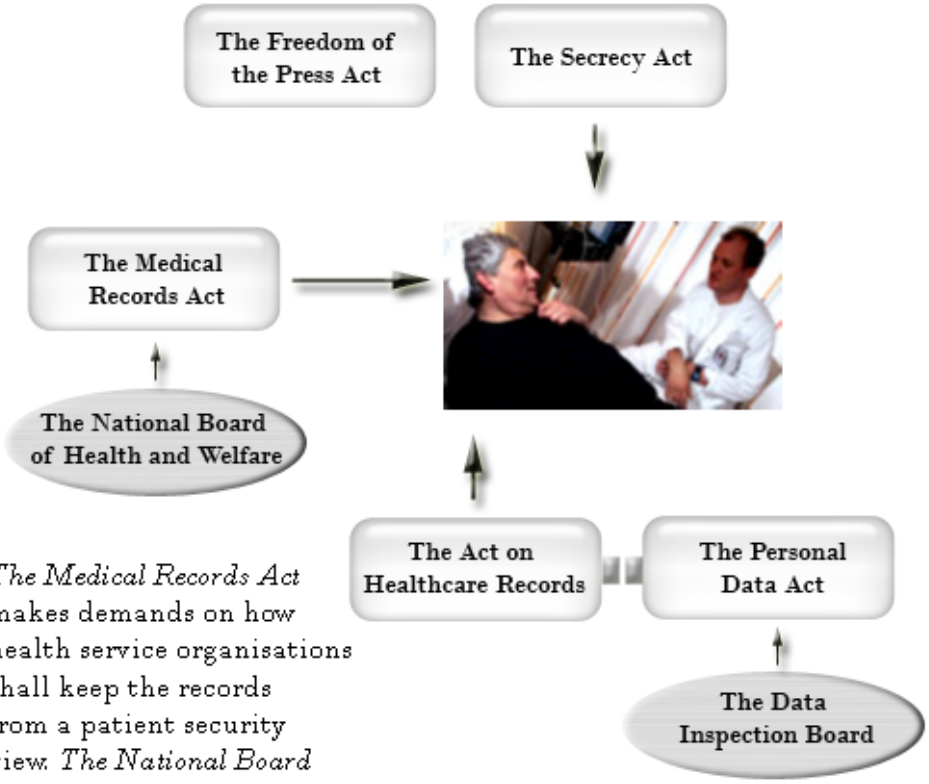
The Swedish legislation concerning the health sector shows signs of being outdated and not well coordinated, and in the light of this, being to hindrance when it comes to introduction of new technology. At the present moment, the development of a more coherent legislation is commenced. Figure D.1 describes how the Acts relate to each other (rewritten from [Utbult et al. 2004]).

D.1 Freedom of the Press, Secrecy and Health Records

The fact that health records in Sweden are public documents according to the Freedom of the Press Act, is unusual compared to other countries' legislation. But, in practice, the health records are everything else than public. How this is possible to accomplish, is stated in the Secrecy Act, which says that information in health records is to be considered secret.

The question is how the health records ended in such a legal vacuum. Most likely, there has not been a well thought-through evaluation before these Acts have been passed. In addition, it takes two Riksdag resolutions to make changes in a constitutional law, and it has probably been a more smooth solution to fix the problems by means of the Secrecy Act [Utbult et al. 2004].

The Freedom of the Press Act states that all health records are public, and thereby exchangeable across organisational boarders, e. g. between county councils. Then, *the Secrecy Act* complements this by saying that sensitive information cannot be distributed to other health service organisations without having the patient's consent.



The Medical Records Act makes demands on how health service organisations shall keep the records from a patient security view. *The National Board of Health and Welfare* is supervisory authority.

The Act on Healtcare Records includes rules concerning processing of information in electronic records and other health information systems and how the patient's integrity shall be protected The Act is connected to *The Personal Data Act* which concerns how personal data shall be processed electronically in a general perspective.
The Data Inspection Board assures that these acts are comformed to.

Fig. D.1. Relevant Swedish Acts and how they relate to each other

The Secrecy Act in today's applicable form, came into force in 1980. Dependent on how it is interpreted, it can complicate and even hinder information from being exchanged between different chains of care. If the vision of 'one patient - one record - through the whole life' shall be met, there has to be rules saying more clearly when and how secrecy can be broken out of necessity. This would be easier to fulfil if the information was not comprised by the Freedom of the Press Act [Utbult et al. 2004].

D.2 The Personal Data Act, the Patient Register Act and the Act on Health Records

The Swedish Data Inspection Board is the supervisory authority as regards the Personal Data Act, while the Ministry of Health and Social Affairs has the responsibility for the Act of Medical Records. These two authorities' roles differ quite a lot from each other. While the Data Inspection Board focuses on personal integrity, the Ministry are more concerned with good quality care and patient security [Utbult et al. 2004]. Based on these two different points of view, the acts are often interpreted in a dissimilar way, creating counterproductive situations.

The Patient Register Act came into force in 1985. At this time, IT was not in extensive use, and the Act shows signs of this. Some of the obstacles it creates, is that it makes it troublesome to correct mistakes in a record, and the rules for digital signing are diffuse. The Act on Health Records is also a problem when it comes to the vision of one record for each patient. Among other factors, the Act does not say anything about sharing of records between several care services.

D.3 The Patient Data Investigation

The Patient Data Investigation, or 'Patientdatautredningen' which is it's original name, is a governmental investigation initiated by the Ministry of Health and Social Affairs. The purpose is to examine all Acts and regulations affecting patient information. The investigation shall produce a proposal to a coherent and well functioning legislation on how personal information shall be handled within health care. Focus will be on increasing the patient security and the patient's possibility to participate when it comes to information concerning own state of health, in addition to improve the medical and economic follow-up. Also, protecting the patient's integrity is of great importance.

The investigation will analyse premises for and the usefulness of creating an united record for each patient, used by all involved care services, either on a national or county council level. The possibility for patients to access their own record via Internet, will also be explored [SOU 2006].

The Patient Data Investigation shall be completed by 31. December 2006.

❖ E

Appendix E: Requirements Specifications

This appendix includes the various projects' requirements specifications. Unfortunately, in two of the six cases, the specification was not available.

The requirements have been translated into English, but references to the original versions are given.

E.1 Case 1: InterRegionale SygehusKommunikationsprojekt - mini-IRSK

[Requirements specification not available from developer]

E.2 Case 2: Standardiseret Udtræk af Patientdata - SUP

The requirements concerning SUP are translated from [MedCom 2004].

CASE 2: SECURITY AND CONSENT

ID	DESCRIPTION
2.1	**Authentification**
2.1.1	There shall be established a county-specific security solution for logon of users and other systems, e.g. Sundhedsportalen (Sundhed.dk - SP).
2.1.2	Access to the SUP-solution shall happen via SP and its security solution.
2.1.3	Access to the SUP-solution ought to be able to be done from own county net, where the user in the county's SUP-web application authenticates himself either with user identity and passord (at a minimum) or via the public OCES-certificate.
2.1.4	The SUP-database can be called via webservices from other applications. Because of this, it is necessary that the SUP-database can reject calls which come from unsecured SUP-web applications.
2.1.5	The SUP project has chosen a solution, where the SUP-web application shall be authenticated by inquiries in the SUP-database. As a minimum, the SUP-database shall be able to identify a SUP-web application from a (system-) user's identity and password, or via a certificate.
2.1.6	The table containing SUP-web applications authorised (certified) to inquire data from the database, shall include the SUP web-application's user identity and password. The table shall be administrated by means of the SUP-database.
2.1.7	The security administrator of the SUP-database can only give access to applications, when the access to the application happens through an 'authorised' authentication.
2.1.8	Communication between the SUP-web application and the SUP-database shall happen on an adequately secured line, e.g. by means of SSL.
2.1.9	In order to handle the situation where the user already is authenticated in another system (e.g. Sundhedsportalen), and via a link calls a SUP-web application, the SUP-web application shall, in the same way as the SUP-database, be able to handle an authentication of anoter system. The SUP-web application shall be started with a parameter for indication of the system's user identity and password (or certificate), and also the user's user identity (or certificate).

CASE 2: SECURITY AND CONSENT

ID	DESCRIPTION
2.1	**Authentification**

2.1.10	In the situations where Sundhedsportalen (SP) calls a SUP-web applicationa via a parameterised link, the following steps are agreed upon:
	- SP are created as a system user in the SUP-web application's security system.
	- Via a parameterised link (URL) i SP are the following sent:
	  - SP's user identity and password (system-ID)
	  - The concrete user's User identity (or certificate number), who requests access
	  - The patient's national identity number, whose data is requested
	  - Choice of consent statement
	- An overview of national identity number in relevance are displayed (logon- and consent dialogues are not).
	- All attached parameters are hidden by the SUP-web application (they are logged).

2.1.11	To ease the administration of users, the user administration of the SUP-web application and the database ought to be based on a solution, which can be a part of MedCom's common user administraion (LDAP).
2.2	**Authorisation**
	In the four previously mentioned scenarios, the need for authorisation and administration is various. The first scenario concerns a traditional authorisation, where the county ca decide which rights the user shall have based on the person's conditions of employment. In the second scenario, the user is in principle external, and the county shall therefore either through a manual registration of the user allocate him rights, or via an inquiry to an external database obtain information, which can be used for allocation of rights.
2.3	**Security logging and usage statistics**
	Since a SUP-web application can call many different SUP-databases, and a SUP-database can be called from several SUP-web applications, which can physically be in different organisational contexts, in practice, it will not be possible to isolate security logs of one single component.
2.3.1	It is a requirement that both the SUP-web application and the SUP-database do security logging from the beginning.
2.3.2	Both the SUP-web application and the SUP-database shall provide the establishment of a usage statistics.
2.4	**Consent**
2.4.1	In the SUP-project, the statement of consents are based on Sundhedsportalen's 'temporary' consent model, i.e. consent in SUP shall be given after the same principles as in the Sundhedsportalen. This means that, before a user can get access to sensitive patient data, he shall state a consent via the SUP-web application.
2.4.2	The consent shall be stored by the SUP-web application, and it shall be possible for an administrator to control the stated consent at a later moment.

E.3 Case 3: Klinisk Portal

[Requirements specification not available from developer]

E.4 Case 4: PlanBasert Samarbeidsjournal - SamPro

The requirements concerning SamPro are translated from [Røstad et al. 2004].

CASE 4: REQUIREMENTS CONCERNING SECURITY

ID	DESCRIPTION
4.1	**Access control**
4.1.1	Access to the plan for users shall be role-based. A role defines basic rights to what one can view and do. Users can have additional rights beyond the rights included in their role.
4.1.2	Certain users of the system shall be able to have the right to delegate their own rights to other users.
4.1.3	The control of access to the system shall be divided into an own module, which shall be re-usable in other systems.
4.1.4	The registration of access rights shall be based on information in the consent statement. Valid rights to a plan shall always be within the consented time period. Note that on a maximum, the time period for the consent can be as long as the time period for the plan.
4.2	**In the future, the system shall be using PKI for authentication of users and digital signing of information**
4.3	**Authentication of users (until PKI is implemented)**
4.3.1	Users shall be identified by user name and password, plus an additional authentication (e.g. one-time code)
4.3.2	The system shall support integration towards existing user databases in the domain.
4.3.3	User name and password shall only be stored on the server.
4.3.4	Passwords shall never be stored or exchanged in plain text.
4.4	**After a period of inacitvity, the system shall carry out an automatic logoff**
4.5	**Traceability and log**
4.5.1	The system shall produce traceability for all usage. The log shall include time, user and all activities which have been done in the system.
4.5.2	Logged activity shall be deleted after three months.

E.5 Case 5: Gemensam Vårddokumentation - GVD

The requirements concerning GVD are translated from [SLL 2004a].

CASE 5: IDENTIFICATION & AUTHENTICATION - FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
5.1.1	**Architecture and Principles**
5.1.1.1	BAT&Portal **shall**, via support services, be able to identify users and authenticate their identities according to chosen method.
5.1.1.2	A user **shall** be able to be a person or system component (software, server etc.)
5.1.2	**Authentication Methods**
5.1.2.1	The following authentication methods **shall** be included with full usufruct: - PKI based logon with X.509 v3 certificate (Citizen Certificate and Health Care Certificates (HCC) according to the SITHS model) - User identity and password - One-time password - can be SMS based, password generators as downloadable software or corresponding technique.
5.1.2.2	It **ought to** be support for the user to chose authentication method. at logon.
5.1.2.3	By log on, it **ought to** be support for the possibility for the user to chose certificate from a certain authority for a particular logon.
5.1.2.4	It **ought to** be possibilities for direct access to the respective authentication method so that the user does not have to actively chose method on each logon.
5.1.3	**PKI related requirements**
5.1.3.1	It **shall** be possible to specify approved certificate authorities for the respective PKI application.
5.1.3.2	There **shall** be functions where it is possible to configure which attribute in X.509 that is used to identify the user (e.g. Subject Name, Serial Number etc.).
5.1.3.3	When certificates are used for authentication, the system **shall** control certificate status (account info). The methods LDAP/CRL and OCSP **shall** be supported.
5.1.3.4	When certificates are used for authentication, the system **ought to** be able to control the certificate status (account info) via 'Delta CRL' (X.509 CRLv2) or SCVP (Simple Certificate Verification Protocol).
5.1.3.5	It **shall** be possible to configure how often updates of account information shall be done (when CRL is used).

CASE 5: IDENTIFICATION & AUTHENTICATION - FUNCTIONAL REQ. *(Continued)*

ID	DESCRIPTION
5.1.3	**PKI related requirements**
5.1.3.6	By availability reasons, the system **ought to** not be dependent on getting access to CRL on each authentication. At interruptions, it ought to be backup methods.
5.1.3.7	By availability reasons, the system administrator **ought to** be able to close the account information control for certificates.
5.1.3.8	By availability reasons, the system **ought to** be able to occasional accept account information for certificates (typically CRL) where 'use-by date' has passed.
5.1.3.9	Updates of CRL or other valid CA certificates **shall** be done without shutdowns.

CASE 5: IDENTIFICATION & AUTHENTICATION - NON-FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
5.1.4	**Scalability**
5.1.4.1	It **shall** be possible to add or replace authentication methods with support from well-defined extension mechanisms or frameworks, without extra programming.
5.1.5	**Accountability**
5.1.5.1	It **shall** be possible to log relevant authentication information, including e.g. method, unique user identity, time stamp, result etc.
5.1.6	**Confidentiality**
5.1.6.1	It **shall** be a strong safeguard against unauthorised access to the authentication information which the services use, both under transportation and storage.
5.1.7	**Administration**
5.1.7.1	The users **ought to** be tied to authentication methods via profiles or equivalent. It should be defined in the profile which methods that are applied and the configuration of these. Users should later be tied to an adequate pre-defined profile.
5.1.8	**Integration**
5.1.8.1	The authentication services **shall** both be possible to use as independent services and as an integrated part of the portal's graphical user interface.
5.1.8.2	The authentication services **shall** by needs use basic functionality concerning the user identity from the identity handling services.
5.1.8.3	The authentication services **shall** be able to be integrated in the SSO service to be made use of in connection with the Single Sign-On.

CASE 5: ACCESS CONTROL

ID	DESCRIPTION
5.2.1	**General Access Control Requirements**
5.2.1.1	The result of an access control **shall** be a logical 'yes' or 'no'.
5.2.1.2	The system **ought to** support a language for rule description (e.g. XACML).
5.2.1.3	The access control **ought to** be able to be directly connected to EK (Electronic catalog in Stockholm county) and useful information therein.
5.2.2	**Care relation**
5.2.2.1	A control of care relation **shall** be possible to include in the set of rules for access control.
5.2.2.2	The access control **shall** be able to use/call the care relation service.
5.2.2.3	At access control of health information, in the set of rules it **shall** be possible to set conditions on when the access control service has to control the care relation.
5.2.3	**Consent**
5.2.3.1	A control of whether consent has been given or not **shall** be possible to include in the set of rules for access control.
5.2.3.2	The access control **shall** be able to use/call the consent service.
5.2.3.3	At access control of health information, in the set of rules it **shall** be possible to set the secrecy limit for when the access control service has to control if a consent has been given.
5.2.4	**Emergency Access**
5.2.4.1	A specified user, or a user connected to certain defined roles **shall** be able to use emergency access and by this pass by authorisation hindrances.

CASE 5: AUTHORISATION MODEL

ID	DESCRIPTION
5.3.1	**Comprehensive Authorisation Model Requirements**
5.3.1.1	It **ought to** be possible to define and use several different authorisation models, dependant on application.
5.3.1.2	It **shall** be possible to execute specific access controls for applications and systems.
5.3.1.3	The access control **shall** be able to be functional - or information orientated.
5.3.1.4	The access control **ought to** be able to contain conditions concerning the validity of rights (e.g. the right to read information concerning a certain patient with the limitation of information not marked 'sensitive', or information marked with the name of the organisation as origin).
5.3.2	**Authorisation Administrative Attributes**
	Authorisation Context
5.3.2.1	It **ought to** be possible to use authorisation contexts.
5.3.2.2	Requirements on different authentication methods **ought to** be able to be associated to type of system operation (e.g. read, write or sign). E.g. logon with HCC can be requested in order to write and delete data, while it is sufficient with user identity/password to read the same data. This requirement also holds for possible authentication methods which are added later.
5.3.2.3	It **ought to** be possible to control authorisation from a class or a group of authentication methods (e.g. PKI-based authentication with certificate from a number of specific certificate authorities).
5.3.2.4	Authentication context **shall** be possible to connect to access of resources (e.g. if log-on with HCC is done, this shall give a higher level of authorisation than authentication with user identity/ password).
	User Identity
5.3.2.5	There **shall** be support for individual authorisation.
5.3.2.6	User identity **ought to** be able to be grouped (e.g. in natural persons and mechanical users).
	Role
5.3.2.7	It **shall** be support for role based authorisation.
5.3.2.8	A user which is authenticated **ought to** not have to do another authentication in connection with change of role, as long as the new role is not requesting a higher level of authentication.
5.3.2.9	It **ought to** be possible to force a new authentication in connection with change of role.
5.3.2.10	A user with various allocated roles **ought to** be able to act in these separately or simultaneously.

CASE 5: AUTHORISATION MODEL *(Continued)*

ID	DESCRIPTION
	Organisational Belonging
5.3.2.11	It **shall** be possible to give a user access to different resources dependent on own organisational belonging.
5.3.2.12	Access to a information subject **shall** be given dependent on which organisational unit, field of activity or secrecy area the information belongs to.
5.3.2.13	It **shall** be possible to handle organisational hierarchies (e.g. hospital, clinic, section) or organisational terms (e.g. 'primary care').
	Resource
5.3.2.14	Individual functions in an application **shall** be possible to be access controlled.
5.3.2.15	Eligible resource characteristics **shall** be able to be authentication administrative (e.g. information - or secrecy class, etc.).
	Delegated Authorisation
5.3.2.16	Delegated authorisation **ought to** be supported.
	Time-limited Access
5.3.2.17	It **ought to** be possible to control access to resources by means of time intervals (e.g. time of day).
	Process Support
5.3.2.18	Status on resources included in a process flow **ought to** be possible to administrate authentication (e.g. to give right to execute certain steps in a matter of affairs process).

CASE 5: ADMINISTRATION OF AUTHORISATION MODEL AND ACCESS RULES

ID	DESCRIPTION
5.4.1	**Authorisation Administration Requirements**
5.4.1.1	It **shall** be possible to handle general and application specific authorisation rules (e.g. to create roles for a certain application ('AppA.role') or equivalent for activities ('AppA.Activity')).
5.4.1.2	All rules which concern a certain application (both general and application specific) **shall** be possible to be filtered out and presented.
5.4.1.3	It **ought to** be possible to decentralise administration of application specific authorisation rules.
5.4.1.5	It **shall** be possible to add, alter and remove roles dynamically.
5.4.1.6	It **shall** be possible to add, alter and remove resources dynamically. (Examples on resources are system, application, function and data object).
5.4.1.7	It **ought to** be support for templates (e.g. to use an existing role definition as a template for new definitions).
5.4.1.8	The administrator **ought to** have access to functions for verification and version handling of authorisation model, authorisation data etc., including the possibility for testing of changes before they are placed in production.
5.4.1.9	It **ought to** be possible to define conditions for connection of users to roles (e.g. a user must have occupational title 'doctor' in order to be allotted the role 'doctor', or a specific role can exclusively be allotted users who belong to a certain organisational unit).
5.4.1.10	It **ought to** be possible to connect users to roles based on specific criteria (e.g. all users with the occupational title 'doctor' are allotted the role 'doctor', or all users belonging to a certain organisational unit are allotted a certain role).
5.4.1.11	It **ought to** be support for role hierarchies.
5.4.1.12	SSD (Static Separation of Duty) **ought to** be supported. This means that a membership in a role excludes or in other ways limits the possibility for membership in one or several other roles. This includes inheritance of roles through the role hierarchy.
5.4.1.13	MCD (Mandatory Combination of Duty) **ought to** be supported. This means that membership in a role requests that membership in another role already is allotted.
5.4.1.14	Exclusive membership in roles **ought to** be supported. This means that e.g. a membership in a role exclusively can be held by an individual natural person.
5.4.1.15	The system **ought to** be able to return a list of resources which a specific role or individual have access to.
5.4.1.16	Authorisation administration **ought to** be able to be connected directly to EK and make use of information therein.

CASE 5: SINGLE SIGN-ON - FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
5.5.1	**Architecture and Principles**
5.5.1.1	The architecture **shall** include a SSO service with well defined service interfaces and documented dependencies on other components/services.
5.5.1.2	The SSO service **shall** be able to issue a logical certificate on the user. The certificate **shall** include the user's identity, properties (attributes) and information about current authentication method.
5.5.1.3	The certificate as above **shall** be possible to use to communicate secure user information to other components/services.
5.5.1.4	The certificate as above **ought to** contain allotted access rights.
5.5.2	**User Authentication**
5.5.2.1	The SSO service **shall** (via suitable authentication service / - method) require an approved authentication of the user before a certificate has been created.
5.5.2.2	A certificate concerning the user's identity which has been issued earlier by the SSO service, **shall** be possible to use under authentication of users.
5.5.2.3	When PKI-based authentication with certificate is used, verified certificates **ought to** be able to be conveyed together with certificates issued by the SSO service.
5.5.3	**Support for Application Architecture and Platforms**
5.5.3.1	SSO towards web application **shall** be handled.
5.5.3.2	SSO **shall** be handled in solutions based on fat clients (client/server applications).
5.5.3.3	SSO **shall** be handled in solutions based on thin clients.
5.5.3.4	SSO towards local networks, principally Windows networks including MS Active Directory, and also Novell eDirectory/NDS, **ought to** be handled.
5.5.3.5	SSO towards WAP applications **ought to** be handled.
5.5.4	**Session Handling**
5.5.4.1	An active session **shall** be uniquely connected to a user.
5.5.4.2	A user **shall** be able to be connected to one or several active sessions.
5.5.4.3	SSO functions **ought to** handle interruptions in network communication.
5.5.4.4	The SSO session **shall** be persistent across several DNS (Domain Name Services) domains, which means that it is not necessary to do another logon to access applications which are in other DNS domains.
5.5.5	**Logoff**
5.5.5.1	It **ought to** be possible to set an inactivity time-out for a user session.
5.5.5.2	There **ought to** be support for coordinated logout from all SSO connected appl.
5.5.5.3	There **ought to** be functions for administrator managed logout (forced logout).

CASE 5: SINGLE SIGN-ON - NON-FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
5.5.6	**Support for Standards**
5.5.6.1	The SSO service **ought to** make use of protocols and message format standards.
5.5.7	**Adaptivity**
5.5.7.1	It **shall** be possible to alter or add new authentication methods / services within the limits of existing SSO service, without changing the fundamental interface.
5.5.8	**Applicability**
5.5.8.1	The SSO functionality **ought to** be available for the applications/target systems via user-friendly functions in the most frequently used technical environments. It is an advantage if there are alternatives for applications connected to SSO. Functions/interfaces ought to mask complex security technique.
5.5.9	**Security**
	Confidentiality
5.5.9.1	All entities which the SSO service uses to issue/confirm the user's identity, **shall** be protected from unauthorised access and usage during both transport and storing. This includes protection of possible certificates.
5.5.9.2	The core in the service **shall** be able to communicate securely with other components over insecure networks.
5.5.9.3	Connections between SSO service and authentication services **shall** be secured.
5.5.9.4	A session **shall** be strongly protected against unauthorised take-over by other user.
	Authenticity
5.5.9.5	The authenticity on the certificates issued by the SSO service **shall**, independent of location, be possible to verify in a secure manner.
	Data Integrity
5.5.9.6	All entities used by the SSO service to issue/confirm a user's identity (and potentially with that can give access to resources), **ought to** have a strong protection against corruption, e.g. through the usage of digital signatures. This includes protection of possible security certificates used by the solution.
	Traceability
5.5.9.7	All logons and logouts to applications with support of SSO **shall** be logged.
5.5.9.8	All requests/issuing of certificates from the SSO service **shall** be logged.
5.5.9.9	In the log, it **shall** be included point of time, if approved/denied, user identity (when applicable), target system/application (when applicable).
5.5.9.10	In the log, the reason for failed logon, from where (ip address/number) the request came from, and also authentication method used, **ought to** appear.
	Monitoring
5.5.9.11	Administrator **ought to** have access to monitoring and statistical functions concerning active users, the SSO service's utilisation and status.

CASE 5: CONSENT - FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
5.6.1	**Architecture and Principles**
5.6.1.1	The consent architecture **shall** include a consent service with well defined service interfaces and dependencies to other components/services.
5.6.2	**Registration of Consent**
5.6.2.1	Registration of consent **shall**, for each patient, include at least information about user identity, user's organisational possession, patient's identity, information volume (described by properties covered by consent, e.g. information/security class), if consent are recommended or not, when it was registered and start-up and finishing time of validity.
5.6.2.2	The registration of consent **ought to**, for each patient, be extended with information about how identity has been confirmed, who has given the consent (e.g. patient, next of kin etc.), how it has been given and who can the information be distributed to.
5.6.2.3	Registered consent **shall** be possible to revoke, and include information about the identity, how the identity has been confirmed, which of the documented consents are revoked and who documents the revocation.
5.6.2.4	Registration of a consent **shall** be possible to implement in other systems via a API towards the consent service.
5.6.2.5	It **shall** exist a web interface for registration of consent.
5.6.2.6	Organisations **shall** be able to see registered consents if a care relation is established.
5.6.3	**Status on Consent**
5.6.3.1	The service **shall** answer if a consent exists or not based on who requests the information and also possible limitations of information volume.
5.6.3.2	It **shall** be possible to offer the result of the consent control in the form of a certificate/ assurance containing verified rights.
5.6.4	**Administration**
5.6.4.1	There **shall** be an administration interface towards the consent service.
5.6.5	**Configuration**
5.6.5.1	A care organisation **shall** be able to configure the organisation limit/ secrecy limit when consent is requested for distribution of care information.
5.6.5.2	The consent service **shall** be possible to configure for 'opt-in' and/or 'opt-out' for each care organisation respectively. When 'opt-in' is used, a consent has to be found for the service to approve an distribution. For 'opt-out', it is assumed that a presumed consent has been given and a consent does not need to be registered in order for the service to approve distribution of information.

CASE 5: CONSENT - NON-FUNCTIONAL REQUIREMENTS

5.6.6	**Interface**
5.6.6.1	The consent service's interface **ought to** be based on open, standardised interfaces.
5.6.7	**Traceability**
5.6.7.1	All status questions and registrations of consents **shall** be logged via the log service.

CASE 5: LOGGING - FUNCTIONAL REQUIREMENTS

ID	DESCRIPTION
5.7.1	**Log Agent with belonging Client-API**
	General Requirements
5.7.1.1	Changes in the configuration of message sources, message destinations, priority level etc. **shall** be able to happen without influencing the availability of the service (without interruptions).
5.7.1.2	The client-API **shall** exist in both a Java and a .NET version.
5.7.1.3	The client-API **ought to** have pre-defined operations for logging according to the most frequently used log types (Application, Security, Event).
5.7.1.4	The client-API **ought to** have pre-defined operations for logging according to the most frequently used priority levels (Fatal, Error, Warn, Info, Debug).
5.7.1.5	Logging of a message via the client-API **ought to** happen asynchronically. With asynchronically messages, a logging call does not have to wait for answers before continuing execution.
	Log Messages
5.7.1.6	Log messages **shall** (in the API) consist of the following separate parts; message source, log level, log type, message text and time stamp.
5.7.1.7	Log messages **shall** be able to have various priority levels (e.g. Fatal, Error, Warn, Info, Debug).
5.7.1.8	It **ought to** be possible to define own priority levels (e.g. Trace, which is more detailed than Debug).
5.7.1.9	For certain log types, it **ought to** be possible to chose a minimum limit for priority level (e.g. minimum priority level can be Error for a security/audit log).
	Message Sources
5.7.1.10	Message sources **ought to** be possible to define according to hierarchical naming.
	Message Destinations
5.7.1.11	As a minimum, the system **ought to** support the following message destinations; database and text files.
5.7.1.12	The system **ought to** support other types of message destinations than database and text file (e.g. Windows Eventlog, Unix syslog, electronic mail messages, Windows Messenger Service, JMS queues, MSMQ).
5.7.2	**Consolidation, Processing and Administration Client**
	General
5.7.2.1	Log information, which has been transferred to the central log service, **shall** be available for searching within configured time.
5.7.2.2	It **shall** be possible, in an user-friendly way, to define which information that are available for searching based on log type, log level and message source.

CASE 5: LOGGING - FUNCTIONAL REQUIREMENTS *(Continued)*

ID	DESCRIPTION
5.7.2.3	It **ought to** be possible to, at a later moment, to index previously unindexed information. This means that it shall be possible at a later moment to manually retrieve older logs and indexate these together with the already existing logs.
	Monitoring
5.7.2.13	It **shall** be possible, in an user-friendly way, to define specific behaviour and patterns which the system automatically does a search for in the logs.
5.7.2.14	It **shall** be possible to inform the operators or other responders about detected events and differing behaviour (e.g. via electronic mail, terminal, SNMP etc.).
	Administration
5.7.2.15	It **shall** be possible for an operator, in an user-friendly way, to search for specific behaviour and patterns which the system automatically searches for in the logs.
5.7.2.16	The result of a search **ought to** be presented in a clear way.
5.7.2.17	Additional searching **ought to** be possible to do based on a search result.
5.7.2.18	It **ought to** be possible to define via the administrator clients those search criteria which are the basis for the automatic monitoring of the logs.
5.7.2.19	It **ought to** be possible to define which indexated priority level that are to be the lowest (e.g. indexate all messages having priority level Info or higher).
5.7.2.20	It **shall** be possible to manually consolidate and indexate the information which earlier has not been consolidated and indexated.
5.7.2.21	It **shall** be possible to set rules for when and how the log information is thinned out. By thinning out, e.g. information that are out of date is removed.
5.7.2.22	It **ought to** be possible to set rules for when and how log information shall be archived.
5.7.2.23	It **ought to** be possible to manually export parts of the log information from the log service.
5.7.2.24	It **ought to** be possible to manually export parts of the log information from the archived log information.
5.7.2.25	It **ought to** be possible to analyse archived log information.
5.7.2.26	It **ought to** be possibilities for automatic generation of reports based on audit- and other information (e.g. patient record).
5.7.2.27	The information which is not indexated **ought to** be saved in another way.
5.7.3	**Archiving**
5.7.3.1	It **shall** be possible to archive logs on secondary media for long-time storage.
5.7.3.2	The archive **ought to** be able to import and export log information in XML format.

CASE 5: LOGGING - NON-FUNCTIONAL REQUIREMENTS *(Continued)*

ID	DESCRIPTION
5.7.4	**Availability**
5.7.4.1	Logging **ought to** always be done, even if the central log service is not available at the logging moment.
5.7.5	**Performance**
5.7.5.1	The period of time for an application to log a message which are correctly formatted at starting point (no joint strings, only operation call with incoming log message), **shall** not exceed 10 ms.
5.7.6	**Security**
	Overall
5.7.6.1	Reading and export of log information **shall** be logged.
5.7.6.2	The consolidated log information **ought to** not be able to be modified.
	Administration Client
5.7.6.3	Authorisation control of administrator **ought to** be done with the same mechanisms which are used by the users of the system.
	Modifiability
5.7.6.4	The client-API's interface **ought to** be stable enough that modifications and additions of e.g. message destinations and agents can be done without affecting the clients.

E.6 Case 6: Nationell Patientöversikt - NPÖ

The requirements concerning NPÖ are translated from [Carelink 2005b].

CASE 6: REQUIREMENTS CONCERNING TECHNICAL SECURITY

ID	DESCRIPTION
6.1	**Security Functions**
	Requirements concerning traceability
6.1.1	All events and accesses (requesting part, distributing part and relevant objects) shall be registered.
6.1.2	There shall be advanced functions for follow-up and inspections of logs.
6.1.3	The system ought to be able to protect logs and other critical information against inappropriate changes.
6.1.4	Log files in different systems shal be synchronished regarding time.
6.1.5	A standard log shall include the following information: - Message source - Log level - Log type - Message text - Time stamp
6.2	**Authentication / authorisation control**
	General requirements
6.2.1	There skall be functions for safeguarding of access in the solution. The safeguard ought to among other factors include protection for log data and other security sensitive data.
6.2.2	All users connected to the platform shall be unique.

CASE 6: REQUIREMENTS CONCERNING TECHNICAL SECURITY *(Continued)*

ID	DESCRIPTION
6.2	**Authentication / authorisation control**
	Authentication of health personnel
6.2.3	The model for authentication of health personnel users making use of the patient register service (PRS) assumes that the local logon transparently controls the access to PRS. Identification happens through the local authorisation control system which issues a ccertificate or ticket. This gives the user access to the health care portal (which is a part of PRS). Information which is to be attached are: - User identity (HSA-id is preferred, but local user name is also accepted) - Category of profession or title - System identity (name/certificate from the information system) - County, clinic, unit - Patient identity (national identity number)
	Authentication of patients
6.2.4	The model for authentication of patient users making use of the patient register service (PRS) assumes two different methods: a The first alternative is used by patient users holding citizen certificates in order to be authenticated towards the patient portal in PRS. The portal verifies the certificate against a Certificate Authority (Steria) and gives the patient access to PRS. The portal does a control towards an internal list of acceptable national identity numbers to assure that not anybody who holds a citizen certificate shall get access to PRS. b The second method is used by patient users with generated one-time passwords in order to be authenticated towards the patient portal, where authorised patients and their national identity numbers are already registered. If the user is authorised for PRS, he is granted access. Both methods assume that the patient portal controls the access to the patient register service.
6.2.5	The information which is to be sent to the patient register service (PRS) are: - User identity (national identity number) - Patient identity (national identity number)
	Authentication of IT components
6.2.5	The model for authentication of computers in the system is based on functionality certificates (server certificates). These shall be used for authentication between all incoming computer components in the PÖS platform.