Study of aspects in electronic patient journal relevant to the medical office agreement

By

Halvard Øysæd and Roy Otto Kleiv

Master Thesis in Information and Communication Technology

Agder University College

Grimstad, May 2003

Summary

Keeping track of the condition of a patient is and always will be important in order for a doctor to give the best diagnosis and keeping the patient as healthy as possible. Earlier the patient journals were stored at the local medical office, and were not possible to get your hands on if you were in another part of the country, or county for that matter. Electronic Patient Journal aims to change this for good. When, or if, the medical offices start using Electronic Patient Journal, viewing and getting the latest update on a journal will no longer be a problem for the doctors, making their job easier.

In Norway today Electronic Patient Journals are coming more and more into use. This is a study on how to develop the system a little further. In some counties in Norway, a roster has been set up for medical treatment after office hours. They often need to access journals from the other medical offices participating in the roster. This is not possible today, but we have specified a solution that should make it possible.

Electronic Patient Journal is a powerful tool for doctors, with it they can access journals from their work desks and the information inside the journals are categorized so it is easy to find the information that is needed. With the Electronic Patient Journal system it is possible to administrate the access to the journals down to the doctors using it or even down to a bed in a hospital. This way the system takes care of the professional secrecy.

The doctors' computer knowledge is in general good and they are ready to start using new technology. When developing systems for the health sector it is important that the doctors' advices are taken to consideration. If they are not, the systems might be very good and very handy, but might not be used because the doctors think it is has many functions or that they do not understand the system at all.

We will include explanations on what the different background material are and what they do, such as Public Key Infrastructure and how Electronic Patient Journal is built up.

To maintain the security, Public Key Infrastructure is often used in relation to Electronic Patient Journal. We have explained why this is a highly used solution in upholding the security and why it is so popular. In our suggestion we have decided to use Virtual Private Network for transferring the journals securely.

We have specified a solution that should make it possible too access journals after office time. This solution will help doctors make better diagnosis and give better health aid in general. We have not specified a total program just how to adapt a module into the existing systems. You must establish a register, ”Treatment register”, that can hold parts of the Electronic Patient Journal. This has to be done in conduction of the Norwegian Laws. This register will store information that is copied from the journals the doctors are writing on their own system. If the doctor means that some of the information he adds to a journal is important and should be stored for future notice, he checks off the information to be sent to the “Treatment register” and it is stored both in the local registry and in the “Treatment register”. To access the information in the “Treatment register”, you need permission to access the journals.

This thesis is a theoretical study and no testing or product development will be done. The idea is that we will study how EPJ works, see if this is secure enough and then make a recommendation on how an enterprise can implement this.

Preface

This thesis “Study of aspects in electronic patient journal relevant to the medical office agreement” is done to complete our study Master of Science degree in Information and Communication Technology at Agder University College, Faculty of Engineering and Science in Grimstad, Norway. The period this report was made was at the beginning of January to the end of May.

The thesis was done in cooperation with NC-Spectrum (NCS) in Kviteseid, who will later on implement EPJ in their current architecture. Rune Sandland, the manager of NCS, is also our “employer” regarding this thesis.

During the writing of this report we have gotten great help from our teacher supervisors Vladimir Oleshcuk (Professor at Agder University College) and Magne Arild Haglund (Professor at Agder University College). We would like to thank them for assisting us with the writing of the Master Thesis. Our thanks also go out to Rune Sandland and NCS for giving us this project.

______________________ ______________________

Halvard Øysæd Roy Otto Kleiv

Grimstad, May 2003

Contents

Summary....ii
Preface....iv
Contents....v
List of figures....viii
List of tables....viii
1 Introduction....1
1.1 Thesis introduction....1
1.2 Task description:....2
1.2.1 Thesis Title:....2
1.2.2 Background:....2
1.2.3 Thesis subject definition:....2
1.2.4 Limitations:....2
1.2.5 Activities:....2
1.3 Thesis resource review....3
1.3.1 Report outline....3
2 Electronic Patient Journal (EPJ)....5
2.1 What is an EPJ?....5
2.2 EPJ versus the paper based format....5
2.3 The Norwegian Electronic Patient Journal standard....6
2.3.1 Introduction....6
2.3.2 Architecture....6
2.3.3 Access controls in EPJ....8
2.3.4 Information exchange between different health sections....10
2.3.5 Journal filing....11
2.4 Overview of EPJ in use in Norway and other places....12
2.4.1 Norway....12
2.4.2 Denmark....13
2.4.3 Great Britain....14
3 The three systems currently in use by hospitals....16
3.1 DIPS....16
3.1.1 DIPS usage and support....16
3.1.2 Security....17
3.1.3 DIPS is made to be used....18
3.1.4 What platforms do DIPS run on?....18
3.1.5 Screen dumps of DIPS....18
3.2 INFOMEDIX....19
3.2.1 Development and managing....20
3.2.2 What does INFOMEDIX look like?....20
3.3 DocuLive....25
3.3.1 What does DocuLive look like?....27
4 Laws and rules....29
4.1 Health legislation....29
4.1.1 Rules concerning health personnel....29
4.2 Regulations managed by the Data Inspectorate....31

4.3 Government rules considering online health servers..32
4.3.1 The Health Register Law (Helseregisterloven)..32
4.3.2 The most relevant sections in Health Register Law.................................32
5 Transferring the information securely..35
5.1 The different standards...35
5.1.1 PKCS #1: RSA Cryptography Standard:...35
5.1.2 PKCS #3: Diffie-Hellman Key Agreement Standard:..............................35
5.1.3 PKCS #5: Password-Based Cryptography Standard:...............................35
5.1.4 PKCS #6: Extended-Certificate Syntax Standard:...................................36
5.1.5 PKCS #7: Cryptographic Message Syntax Standard:..............................36
5.1.6 PKCS #8: Private Key Information Syntax Standard:.............................36
5.1.7 PKCS #9: Selected Attribute Types:..36
5.1.8 PKCS #10: Certification Request Syntax Standard:................................36
5.1.9 PKCS #11: Cryptographic Token Interface Standard:.............................36
5.1.10 PKCS #12 Personal Information Exchange Standard:.............................37
5.1.11 PKCS #13: Elliptic Curve Cryptography Standard:.................................37
5.1.12 PKCS #14:..37
5.1.13 PKCS #15: Cryptographic Token Information Format Standard:............37
5.2 What are electronic signatures and encryption all about?................................37
5.2.1 Security services...38
5.2.2 Symmetric crypto:..40
5.2.3 Asymmetric crypto..40
5.2.4 Digital signatures...41
5.2.5 What is a Digital Certificate?..43
5.2.6 Hashing and Digital Signatures...43
5.3 PKI – Public Key Infrastructure...43
5.3.1 What is PKI?..43
5.3.2 How Public Key Encryption works...44
5.3.3 Validating Data Integrity...44
5.3.4 The role of the Certificate Authority...44
5.3.5 The four primary services PKI provide...45
5.4 VPN – Virtual Private Network...45
5.4.1 IPsec..46
6 What information do the doctors need...47
6.1 Survey done by Lærum, Ellingsen and Faxvaag...47
6.1.1 Facts about the survey...47
6.1.2 Results...47
6.1.3 What we can conclude from results:...48
6.2 Questionnaire...49
6.2.1 What we asked about...49
6.2.2 The results we got from these questions:..50
6.2.3 What we concluded from the results...51
7 Specification of the “Treatment register”..53
7.1 Starting conditions...53
7.1.1 System...53
7.1.2 Laws and regulations...53

7.1.3 Security 54
7.1.4 Other conditions 55
7.2 Overview of the ”Treatment register” solution 55
7.3 Architecture in the “Treatment register” 57
7.3.1 Basic architecture 57
7.3.2 The different components in the system 58
7.4 EPJ system 58
7.4.1 Components in the EPJ system 58
7.5 Securing the system 59
7.5.1 Security within the EPJ system 59
7.5.2 Security in open networks 60
7.6 Example 60
7.7 Possible additions to the “Treatment register” solution in the future 61
7.7.1 Using EPJ at an accident site 61
8 Conclusion 63
Appendix A – Abbreviations 64
Appendix B – References 65

List of figures

Figure 1: The basic architecture for the Norwegian EPJ standard. 7
Figure 2: The DIPS desktop 18
Figure 3: DIPS' journal explorer.. 19
Figure 4: Appointment diary. 19
Figure 5: The users can sort the available information by the use of filters which they set themselves; they can also decide what buttons are going to be available.. 20
Figure 6: This is an overview of who of the patients have a leave of absence. You can set the different dates when he/she will be back. 21
Figure 7: Registering of important information. 21
Figure 8: Requisitions and answers. 22
Figure 9: The nurses' documentation tool. 23
Figure 10: The INFOMEDIX treatment plan window. 24
Figure 11: The medication module... 25
Figure 12: The filing client in DocuLive. 27
Figure 13: The case client in DocuLive. 28
Figure 14: Encryption via the Internet.. 40
Figure 15: Using digital signatures... 42
Figure 16 Picture from BMJ showing results for the survey Lærum, Ellingsen and Faxvaag did. [37]... 48
Figure 17: The connection between the "Treatment register" and the local medical offices. 56
Figure 18: How the "Treatment register" works. 57

List of tables

Table 1: Which and whose keys are used when you encrypt and decrypt messages and signatures. 44

1 Introduction

1.1 Thesis introduction

The thesis was commenced January 2003 by getting an overview of the technologies and theories we were going to use during this thesis. The main issues were Electronic Patient Journal, secure transferring of information, different Electronic Patient Journal systems in use in Norway today and Government regulations.

We felt there was much theory studying to be done, so we did not make a preliminary report. We started off by retrieving and reading the different issues that had to be covered in order for us to get an understanding on how the Electronic Patient Journal works and is built up. We did make a project plan in which we set dates for when we wanted different activities to be finished.

Electronic Patient Journal is coming into the medical environment fast, therefore medical offices have to adapt to the new technology that is available in order to be more efficient. Most medical offices are using Electronic Patient Journal in their own system, but people are starting to move around a lot, and the patients journal might be needed at another medical office than the patient usually are visiting. This is the main reason why we want to take a look at how to transfer an Electronic Patient Journal between two or more medical offices.

Secure information flow between two medical offices is essential in this thesis. There is information in Electronic Patient Journals that are extremely confidential and personal; therefore it is important that no third part can get their hands on the Electronic Patient Journal. We will give an introduction to the different security techniques one can and should use in order to make the transfer as secure to conform regulations

There are many different government regulations that concerns Electronic Patient Journal and transferring of these between medical offices. There are different rules concerning who is supposed to have access to the patient journals and what kind of security the servers that the journals resides on need to have. These rules are extremely important; you do not want more than a limited amount of people to have access to your personal files. It would be a disaster if these servers were to be hacked and the journals made public for everyone to read. We have studied the different rules that apply to using electronic patient journal and extracted the main points from these.

1.2 Task description:

1.2.1 Thesis Title:

Study of security aspects in electronic patient journal in medical office agreement

1.2.2 Background:

Today most of patient's journals are paper based. If a journal is needed somewhere else than at your local medial office, it will have to be sent by mail or physically brought to you.

Because of the large geographical distances between the different medical offices in Norway, some of the local authorities have set up a roster for critical medical treatment of patient's outside normal office time. Some of the medical offices participate in this agreement.

We will to examine the possibilities to use an EPJ to solve the problems so that doctors can get their hands on a patient's journal wherever they are. The fact that the data transported are highly confidential means that security is one of the most critical aspects which is why we need a very secure solution.

1.2.3 Thesis subject definition:

We will look at a scenario of a patient coming to a medical office. From there we will look at strengths, weaknesses and problems in the secure information flow. We will look at the different solutions available today and in the near future. In the end we will make a proposal on how the most relevant solution can be implemented.

1.2.4 Limitations:

We will not do the actual implementation; just suggest possible solutions.

1.2.5 Activities:

Find material about Electronic Patient Journal and Norwegian rules about access to journals.

Study the different solutions, available today and in the near future, considering secure transferring of information.

Make a questionnaire to use for getting the information we need from the medical office.

We will have to get in touch with the Data Inspectorate and ask about rules concerning information on servers that is online 24/7.

Specify a possible solution.

1.3 Thesis resource review

In this section we will give a review of the resources we have used to obtain our information about the situation in the research and development in Electronic patient journal and Public Key Infrastructure. We have mainly used Internet as a resource of information basically because much of the information is changing month by month.

Our most commonly used base for information about electronic patient journal is the Norwegian government's health care Internet site. This site is where the Norwegian government keep the reports about status in the health sector. Here they have reports about the expectations in the development of Electronic patient journal and some progress reports on how far they have gotten. [1]

To get an understanding of what is and is not allowed regarding journals and having them on a machine that is online, we had to read through the different Norwegian laws concerning this. We mainly used the three different register for reference; "The Health Register Law" (Helseregisterloven), "The Health Personnel Law" (Helsepersonelloven) and "The Regulation of Patient's Journals"(Forskrift om pasientjournal). [23]

We have also used the Norwegian government's Internet database where they have published the Norwegian rules about health care registers and electronic treatment of health care information. [2]

We have used the Norwegian Standard for Electronic Patient Journals developed by KITH. [21] [22]

In order to get information and facts about the different systems in use by hospitals in Norway today we used the websites dedicated to the different systems. There are currently 3 systems that have gotten the most attention; these are DIPS, Software Innovation ASA's DocuLive and INFOMEDIX. [4] [5] [6]

PKI (Public Key Infrastructure) will be used to make sure that the journal is transmitted in a secure fashion from the server where the journal is located to the client who is requesting it. [15] [36]

1.3.1 Report outline

The target for this thesis is people with interest in modern healthcare and secure transfer of information in open networks, and other health personnel that can make use of this thesis. Readers that take general interest in secure transfer of information and health care may find this interesting reading.

Chapter 2 gives the reader a general understating of what EPJ is and how it is used, and to what extent it is used.

In chapter 3 we describe the three different EPJ systems in use by hospitals in Norway as of today.

Chapter 4 concerns the different rules and laws that must be followed when dealing with patient records. The laws mentioned cover who can legally have access to the journals and what kind of security that most be upheld. The rules do not specify how these security issues are to be followed, just that it is imperative that you do follow them.

Chapter 5 explains what the different security functions do and, to a certain extent, how they do it. This chapter mostly covers the functions needed to maintain the secure system that must be used when dealing with something as confidential as people’s health records. Some keywords here are, PKI and VPN.

Chapter 6 contains information gathered by us and found on the Internet concerning what kind of information the doctors need when they get a new patient. In order to get some information regarding EPJ we made a questionnaire which we asked some doctors to answer.

The 7 chapter is a solution specified by us.

In the reference section we have tried to give the readers an understanding of where we found all of the different information used in this thesis. By following the links listed under each of the references the readers can get more detailed information concerning the different subjects if he or she is interested. The references are listed by the use of numbers inside braces [X]. Throughout the report we have referenced to Appendix B by adding the [X] before or after the chapters we have gotten our information from. Some of our references are used many places in the thesis so we did not add the [X] where this applies. Some of these links may unfortunately be changed in the future, although we doubt they will.

2 Electronic Patient Journal (EPJ)

We will in this section look at what happens when a patient comes to a medical office after office time, and how the doctor gets access to the information about the patient. We will look on the Electronic Patient Journal and some examples of how some Electronic Patient Journals have been used in Norway and in other countries.

2.1 What is an EPJ?

An Electronic Patient Journal (EPJ) is a patient journal where the information is being stored electronically. EPJ must be able to store the same kind of information as in paper patient journals, which in practice means that all information that is necessary or have any relevance to the treatment and nursing of the patient.

An Electronic Patient Journal system may also be viewed as a specialized computer record system with functions for registration, updating, deleting and retrieving of information from the EPJ.

An Electronic Patient Journal should give good opportunities to make the patient journals easier to manage and be done so more efficiently. The Electronic Patient Journal should support quality assurance of the information, more efficient ways to get hold of the information, better ways to present the information and better and more efficient ways to communicate between other patient journals about the same patient. With clever use of the Electronic Patient Journal, health personnel should be able to use more time with the patient, instead of reading through paper records.

Electronic Patient Journals will also be an important information- and decision basis in consecutive diagnostic, treatment and follow-up of patients. The information on Electronic Patient Journals will also be important for health service research, quality assurance and education of students. An Electronic Patient Journal should be able to give quick and relevant information about a patient when and where the information is needed. Because of that the information in patient journals is very sensitive, it is important that only health personnel that have legitimate need for the information at the time can get access to it. [2]

2.2 EPJ versus the paper based format

Many might think that there are going to be a lot of problems converting to EPJ instead of using the good old paper format. The paper based is easier to bring home, it is easier to read on a paper versus reading it on a screen etc, but what many do not think about are the many disadvantages the paper based format actually has. Below is a list of different downsides to the paper based journal contra EPJ.

- It can be lost.
- Can only exist at one place at a time, for example in a locked office which you do not have the keys for.
- Doctors do not always have a “well-read” handwriting.
- You cannot, or at least it is not easy, to search for a specific thing in a paper based journal.

These things cannot happen to EPJ. Of course a disk can “crash”, but there will always be a back-up somewhere which can be recovered. And there may be a power failure from time to time, but most public institutions have power generator which kicks in when that happens. Besides, neither a “disk-crash” nor a power failure is something that happens often.

2.3 The Norwegian Electronic Patient Journal standard

The Norwegian Government have issued a standard that applies for health services in Norway. We will in this section take a look on the standard and how it is meant to be used in the health services. It will be an overview over the standard, not a thorough examination. [21] [22]

2.3.1 Introduction

In the standard there are different priorities on the requirements. This is because the standard is for many different health care services and therefore cannot be specified too much to one of the services. There are some obligatory requirements and some recommendations. The standard also specifies requirements that are obligatory for hospitals and other health care services, but are voluntary for other services. In the future there will be made supplement documents which specify concrete requirements for the different health services. One of the goals with the standard is to make it easy for the health care services to follow the regulations that the Norwegian laws put on the use of Electronic Patient Journals when this standard is used. There is hardly any upper limit on what kind of information that can be put into the Electronic Patient Journal, but there is some key information that has to be put in.

For the health care services that want to use the standard there is no technological guiding on how the Electronic Patient Journal system should be implemented, as long as it can make a specific exportation format and follows the other obligatory requirements. This is so the different services can choose their own supplier.

2.3.2 Architecture

The figure shows the central part of the architecture in this standard.

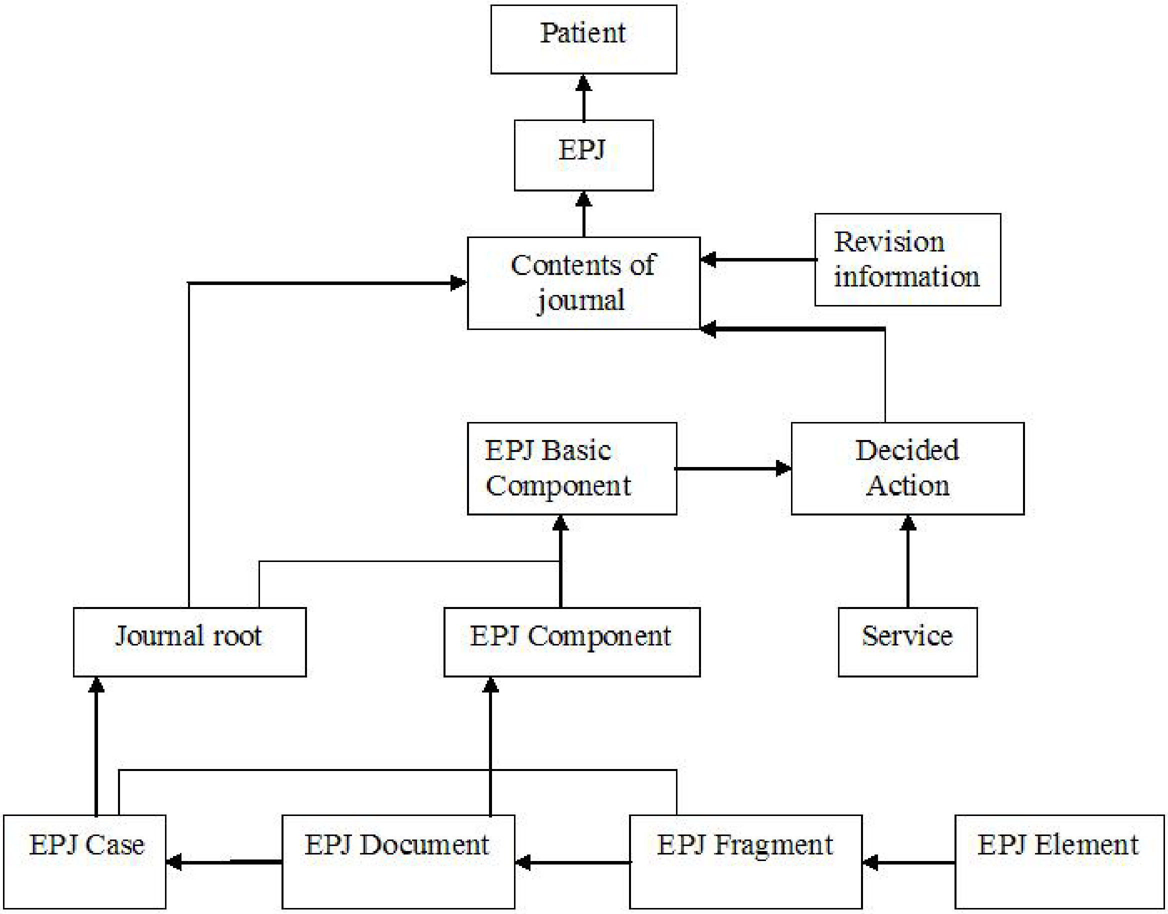


Figure 1: The basic architecture for the Norwegian EPJ standard.

The Electronic Patient Journal is always connected to a patient. In the journal health information about patients is viewed as components. The three main components “EPJ Case”, “EPJ Document” and “EPJ Fragment” are used in the journal. A fourth type, “Journal root”, is used to collect all components that are entered into the journal. “EPJ Fragment” holds the data elements. “EPJ Case” and “EPJ Document” are used to structure the journal contents in an adequate way. All components have some common properties that are used among other things for access control to health information. In addition to components the Journal contents is made of “Revision information”, “Decide Action” and “EPJ link”.

”Revision information” is where the information about when, who did and who had the responsibility of the changes that have been made in the components in the journal. This applies to all revision of the journal, for instance deleting, correction or adding. ”Revision information” also identifies all other changes that have been done in the journal, for instance registering of “Decided Action” or “Service”.

“Decided Action” is where it is stored that health worker has made a decision considering the medication for the patient that imply that the access to the journal has been changed. This decision has to be made of an authorized health worker. When it comes to reading and editing in the journals it has to happen on the basis of a “Decided Action”, because of that all “EPJ Components” can be backtracked to a “Decided Action”.

“Service” is where it is registered when the “Decided Action” has been executed. “Service” also serves as a log over who have had access to the patient’s journal.

“EPJ link” is used to register references between different parts of the journal.

The different components are used so it is possible to give health workers different access. Just because you have access to the journal does not mean that you should be able to read everything. Much of the information in the files is for doctors and the patient themselves. The patients also have absolute control over who should be able to view the information.

Some of the information is more important than other. Therefore it should be able to access it easily and it should be possible to emphasize it in the journal. This information might be for instance essential information concerning the patient’s health or who the patient’s closest relatives are. As far as it is possible X-rays, ultrasound, video and other picture material should be included in the journal, either directly or by references. From the journal it is possible to print out references, prescriptions, medical certificate, requisition and epicrisis.

In the journal you have to register some essential information. As a minimum you have to register the patients name, address, birthday and personal identification code or some other precise identification of the patient. There should be good possibilities to register name and address to relatives, especially when children are patients. In the journal there should also be information about health workers that are involved in the work with the patient. In addition to name and address it is important that the working position of the health worker is added.

2.3.3 Access controls in EPJ

The access controls in EPJ systems are there to make sure the laws are followed. This standard aims on doing that in such a way that it will not hinder the work of the health workers, as user-friendly and with as good performance as possible.

The requirements that come from the laws can be divided into two groups:

- General principles that will apply in most cases. That is for instance professional secrecy and that the patients give consent to the use of the journal.
- Exceptions, for instance that a patient or someone else with the authority have set some restrictions in the use of the journal. This group also applies for paramedic and other demands that make you depart from the law that says that the patients have to consent to the use of the journal.

One of the most important subjects regarding health information is the professional secrecy. This is written in § 21 in the health personnel law. It is also illegal to give access to information about a patient to other health personnel that should not have access to the information. The access controls in the EPJ system is made so that the health personnel that should have access to information get it, and those that should not do not. It is the health personnel's own responsibility that they do not tell the information to someone that should not know about it, this does not differ from the way it is without EPJ. It is also the health personnel's responsibility to make sure that nobody else can use their account or password to access the information.

The requirements in the standard shows that the information the health worker should be able to access are dependent of the situation. No one should be given access to health information in a journal as a particular person except the patient himself. It is the work the health workers are doing that should control what information they should have available.

There should be a person responsible for each journal and this person should keep accounts of who uses to the journal. It is not practical that the person responsible for the journal explicit authorise each health worker each time they should have access to the journal. The risk for medical malpractice would also be high. Because of the protection of personal privacy it is not acceptable to give all health workers access to all information in the journal. The answer will be to make procedures so the access to journals can be mostly automatic.

There have to be a "Decided Action" before there is given access to the patient journal. "Decided Action" is not carried out, unless the information that should be accessed are necessary. Access regarding patient management, internal control, quality assurance etc. should also be based on a "Decided Action". Also if a patient wants access to the journal it is called a special case of "Decided Action". It has to be possible to split up the "Decided Action". This is because in hospitals there might be involved different wards and therefore it is necessary to have different access to the information in the journal.

2.3.4 Information exchange between different health sections

The exchange of patient information can be statutory or they can be optional. In many cases the one that keeps the patient journal is obliged to report the information to people outside the health service or in another department. In other cases it is information exchange between departments inside the health sector he is working in. The most important thing is that the information content is the same both for the receiver and the sender.

The information that is going out to external departments is epicrises, laboratory reports, reports, messages, applications, statements, references and requisitions.

You can split the different participants in the information exchange in four enterprises

1. Public health service that have direct contact with the patients:
   - Here you will find hospitals, both somatic and psychiatric. In hospitals there are all kinds of health personnel and therefore the patient information accessible are very variable. The information flow in hospitals are between different hospitals, hospitals to other health care services and internal inside the hospital. Economic and administrative information will both go internal and external.
   - Primary health service in both private and public sector. Health personnel in primary health services send and receive medical certificate, requisition epicrises etc. Reports to government departments and registers are an important part of the information exchange.
2. Cooperative Health services:
   - Herein lays the educational psychology and the social services. They offer local government services according to the law about social care. Information flow is mostly about applications, references, statements, refund demands and end reports.
3. Health services with service and support functions:
   - Here are medical laboratory, physiotherapy, occupational therapy, ambulances, aid central agency and more. These services will have different need for information depending on what service and support functions they give. The information that is being exchanged is references, laboratory replies, epicrises, requisition, refund demands and applications.
4. Patient administrative service
   - It is the laws and regulations that regulate what information that should be collected to central health registers and government departments. The most central register that receive information from patient journals are: the Norwegian Patient Register (Norsk Pasient Register, NPR), the

Cancer Register (Kreftregisteret), the Cause of Death Register (Dødsårsaksregisteret), the Medical Childbirth Register (Medisinsk fødselsregister) and the Message system of Infective Disease Register (Meldingssystemet for smittsomme sykdommer, MSIS). There are also information flow to important central departments like the Norwegian Health Supervision (Statens helsetilsyn), the Norwegian Institute of Public Health (Statens institutt for folkehelse), the Central Bureau of Statistics (Statistisk sentralbyrå) and the National Insurance Department (Trygdeetaten). The National Insurance Department has a special role in the information flow in the patient administration services. The information flow goes from different health departments to the National Insurance Department and from there again to those institutions that shall help the patient. The exchange of information between patient journals and the different registers and departments is done by electronic messages.

The information flow in the departments should be done electronically; this applies for messages like prescriptions, references, medical certificate, form letters etc. The goal with this to reduce the paper amount that is in the service today. The need for messages will differ from department to department, but general practitioners have a large and acknowledged need. It is also a goal for the standard to make it possible to do administrative tasks more efficiently.

There are no obligatory requirements on how the messages should go in this standard. This is because it depends very much on what targeted group the EPJ system is aiming for. Some departments have not worked out how they want their standard to be and therefore the requirements are general instead of specific. It is expected that there will be obligatory demands in later standards and requirement specifications aimed at groups of the departments like somatic hospitals.

2.3.5 Journal filing

Many health services have to file the patient journals some years after there is no use for them. This applies for public health services and for some private health services. Therefore everything that has to do with filing is placed in a separate module. That module is mainly based on the Public Record Office's standard Noark-4 (Noark-4 is a specification for electronic filing systems in the public sector, which have certain demands regarding contents, structure and functionality).

Some information in Electronic Patient Journals will be in such a format that it will not be accepted for long-term storage. These documents should as soon as possible be converted to a format that is approved as filing format. Some documents that include electronic signatures have to be kept unchanged so the signatures still can be verified. There can be a centralized filing system or it could be a decentralized filing system. When electronic patient journals are being used it is natural to have a centralized filing system.

2.4 Overview of EPJ in use in Norway and other places

In this section we will look how far the work with EPJ has come in Norway, Denmark and Great Britain. It is most natural to compare Norway to Denmark since both countries has come pretty far in the work with EPJ.

2.4.1 Norway

In the summer 2001 KITH completed and published the standard for EPJ. This standard includes basic requirements to EPJ systems in the health care service. The standard is a guide to how the EPJ systems can be built. It is not required to use the standard when you build an EPJ system because some requirements are not needed for all health care institutions. On a later stage in the work with EPJ it might be required to use parts of the standard. The standards are adjusting to the existing government regulations.

The Norwegian Government has made a long-term plan for information technology co-operation in health care industry. The name of the plan is ”Si @” and is for the years 2001-2003. This plan is an important part of the Norwegian Governments “eNorge-plan”, that is the plan for Norwegian development in information technology as a whole. The purpose with this plan is to stimulate co-operation between different health care sectors, better contact with patients and better quality in the services trough information technology. There are 4 priority areas in this plan; National Health Network (Nasjonalt helsenett), Electronic co-operation in the Health- and Social Sector (Elektronisk samhandling i helse- og sosialsektoren), Telemedicine (Telemedisin) and General Public Services (Publikumstjenester).

Today many of the different participants in the Norwegian health service are not co-ordinated. The Norwegian Government have set the standards but it has been voluntarily for the different health service participants if they wanted to use them or not.

If the Government wants to get better co-operation between different health services they have to make sure that there are standards available and that these are followed. Today you can see this is being done with the EPJ standard. There are many reasons why there are not good co-operation between the different health service participants. For instance, most of the medical offices have IT-equipment, but they have not installed equipment for communication to other medical offices. In addition it is expensive and difficult to determine what security level is high enough. There are also compatibility problems with different equipment and standards and this will lead to high adaptations costs.

Some key development projects will be organised as national projects with Government management. This applies to the development of standards, organise and arrangement of Government information and development of national infrastructure in co-operation with the central health services. [1] [20]

2.4.2 Denmark

In Denmark they have a report dating back to July 2000, where they made a status report on the standardization of Electronic Patient Journal. Central in the strategy was development and introduction of EPJ in hospitals.

The standardization of EPJ in Denmark is based on the principles in the international EPJ standardization work within the CEN-co-operation (Comitè Europèen de Normalisation). The status report has been replaced with a new report in 2002 with a national information technology strategy for the Danish National Health Service 2003-2007. The new strategy shall strengthen the coordination of the central achievement in information technology, but the main goal is to make good conditions for an effective use of information technology in the health service as a whole. The vision for information technology in National Health Service is that health care personnel has access to send and receive relevant and time right information. Information technology, and specially EPJ, is in this relation a medium to make the information access and communication more efficient. The three main groups are the patients, the health care personnel and the community as a whole.

Most of the workers in health care use information technology in their work today. Denmark is also one of the countries that use most information technology in the communication between the different health care institutes. For instance 85% is using EPJ (there are two EPJ's the ones that doctors use to write patient journals that cannot communicate with others, and EPJ that is standardized so it can be used together with other EPJ. This percentage is for EPJ that are not standardized) to write the journal for patients among general practicing doctors. Still most of the communication between different institutes is still paper based. The large challenge is to make sure that information can be transferred securely and with meaningful information. It is here the standardization of EPJ is important. In a status report from "EPJ Observatoriet" in 2001 they say that the percentage of the EPJ usage in the health service is 5-10% depending on what definition of EPJ you choose. EPJ will make large gain in efficiency in the health care and therefore it is made large efforts to speed up the process introduction of EPJ.

There are four participants in the development of EPJ in Denmark: “Sundhedsministeriet”, “Sundhedsstyrelsen”, “Amtsrådsforeningen” and “H:S”. They sent out a mutual statement about the superior principles for the standardisation and propagation of EPJ in February 2001. The principles for EPJ concerns mutual standard specification, mutual responsibility for the development and mutual goals for the functionality. The government will draw up the standards together with the hospitals, and the hospitals commits to making sure the EPJ builds on mutual professional and technical standards that make sure that the information can be exchanged between the different systems. The main goal is that the hospitals have converted to EPJ within 1 January 2006. [14]

2.4.3 Great Britain

In Great Britain they have had a National Health Service (NHS) since 1948. The idea of the NHS is that people in Great Britain should get help on basis of illness not money. The NHS has had trouble following the developments since 1948 and up to today. The help patients receive is based too much on where they live, there are to long waiting lists to get help and there are unacceptable variations in the different standards across the country. They have failed to achieve what they set as a goal because there has been a lack of funding. You could say that the system is a 1940s system operation in the 21st century.

The Government has made a plan how to overcome these problems with the NHS. The vision and purpose of the plan is to give the people of Britain a health service that is fit the 21st century. The plan is that the health service should centre on the patients. The plan also says that the Department of Health will set national standards, but the different local health services will have to follow it up. Social services will work together so there will not be done too much double work and no one will fall in between those two services. The plan will not be achieved just on its own, so there is an increase in the funding of the NHS. Today they are investing £200 000 000 a year, but as a result of this plan there will be an extra £250 000 000 invested in information technologies in 2003/2004.

Within the NHS plan there is also a national program for information technology. According to this plan the first generation of electronic health records will be available in 2005. The meaning is that the full array of clinical applications and functionality in electronic health records should be available nationwide in 2008. The main goals in the plan are to get more central control over specification, procurement, resource management, performance management and implementation of the information technology strategy. They are also planning to get 24 hour access to health records and information, a National Electronic Library for Health and public access to on-line information.

In Great Britain there has been a pilot project with electronic health records. The electronic record development and implementation program was established as a pilot project to look on electronic health records in April 2000. First it was only 4 communities participating, but in June they added 13 more. These communities were used to research how electronic health records could be used to share patient information across health and social service communities. This pilot project has been finished and the experience and information that was gained from this project are available to the NHS and other health services. This is so they can use the experience to form the standards that they are making. [7] [8] [9]

3 The three systems currently in use by hospitals

There is mainly three different patient journal systems in use in Norway today; Software Innovation ASA's DocuLive, INFOMEDIX from EMS TietoEnator HealthCare and DIPS from DIPS ASA. We will give a description of the three and give examples of pros and cons with the systems. The following information is gathered from the respective systems' web page and must therefore be looked upon at an objective point of view. Companies have a tendency to favourite themselves, logically enough.

3.1 DIPS

The development of DIPS commenced at Nordland District General Hospital in 1987. They felt the need of a system that could easily be managed and run on a regular desktop computer. The system became highly popular, and in 1989 an agreement was made that other hospitals in Norway could use the system. Ever since then the number of clients have increased as well as the users and the input subsystem. Today DIPS have 27 hospitals and 80 psychiatric institutions as their customers.

DIPS is the most integrated health information system in Norway. No other system has the same connectivity between the system modules as DIPS. This connectivity between the subsystems gives an excess value that no one else can offer as of today. Because of this connectivity the data can be registered and stored in different places, in addition the data can be reused and presented in different contexts. This leads to a higher quality of the data, which is essential when you document the institutions' work.

This integration also leads to that the different subsystems look very similar and the cost of the training needed to use the system will therefore be reduced compared to other systems.

The fact that DIPS is an open system is also very positive. This way other suppliers can develop modules integrated in DIPS.

3.1.1 DIPS usage and support

As mentioned, the development of DIPS started at a hospital. This development was very well connected to the future users of the system, namely the doctors and the nurses. Communication between the two parties was highly relevant in order to make the system as good as possible. In addition some of the developers had a background from working at a hospital, and thus knew how important the need of information is and knew what kind of problems one could run into.

The various hospitals that use DIPS have an annual user conference called "DIPS-forum", which is being held at a hospital that uses DIPS. During these forums a special group of experts is being formed, DIPS reference group. These groups consist of users from all around the country, and they guide and advice in the further development of DIPS.

3.1.2 Security

Securing health information systems is extremely important and cannot be stressed enough. DIPS has an extensive system for access control. This system is based on events and categorizing of data instead of the ordinary rules, which helps make the admission system secure and flexible so that it can be adapted to each hospitals needs.

DIPS have access control at both the function level and the data level. In DIPS access control is protected down to which bed the new patients are hospitalised and at section level at polyclinic treatments. It is also possible to give a restricted number of people access to a patients journal, thus making it even more secure.

One other thing concerning access control is that the users only need a limited number of passwords to relate to. If the users have more than one place they have to give or enter their password, the chance of someone getting that password is greater, and in doing so making the security worse. In DIPS the hospitals have the possibility to integrate the password control with the network in a number of different ways, by doing it this way the users can get away with giving the password only once instead of several times.

Data quality is another important issue related to health information systems. Since the DIPS data model is much normalized, the data in the system is extremely easy to control. In some systems you have to synchronize the data to make sure that you have the latest and most up-to-date version. Because of integrated systems and avoiding redundant data you do not have to do this with DIPS. The information in DIPS will always be up-to-date and correct compared to each other.

DIPS also offers comprehensive routines for automated logging of changes made to a journal.

Controlling and limiting the access to the journals is very important but in some cases, for example an emergency, you have to evade this security. DIPS's version of this is called "bluelightfunction" (blålysfunksjon), because the use of this function gives access to data the users normally would not have access to, and the use of this function has a high degree of logging.

3.1.3 DIPS is made to be used

DIPS is designed to be available 24/7 made possible by a solid Oracle database. There is also well written routines on how to shut the system down to make any necessary updates to the system, this also applies to the system maintenance.

It is highly important to be able to distribute applications to the users of the system in an efficient way. Several of the co-workers at DIPS ASA have a background in running DIPS. To reduce the need of administrating an application these experiences were considered when designing DIPS. This is why the system works just as well in a WAN environment as in the ordinary LAN environment.

3.1.4 What platforms do DIPS run on?

DIPS is developed for open technology and runs on a standard network, either WindowsNT or Novell Netware, and standard computers. On the client side 32-bits Windows machines are used and on the database side they have chosen to standardize on an Oracle 8 system. Through a comprehensive security system one can integrate functionality from 3rd party suppliers.

These points are the main reasons why DIPS feels they have the best solution. More information can be gathered at DIPS's website which can be found in Appendix B [4].

3.1.5 Screen dumps of DIPS

Here are some different screen dumps of the DIPS windows.

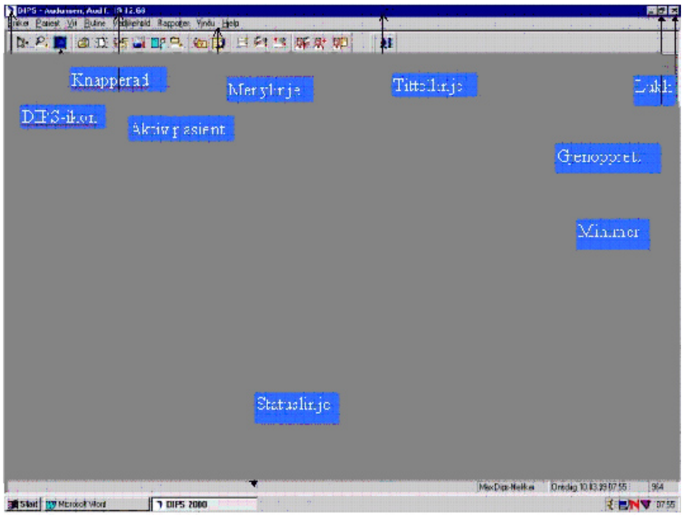


Figure 2: The DIPS desktop

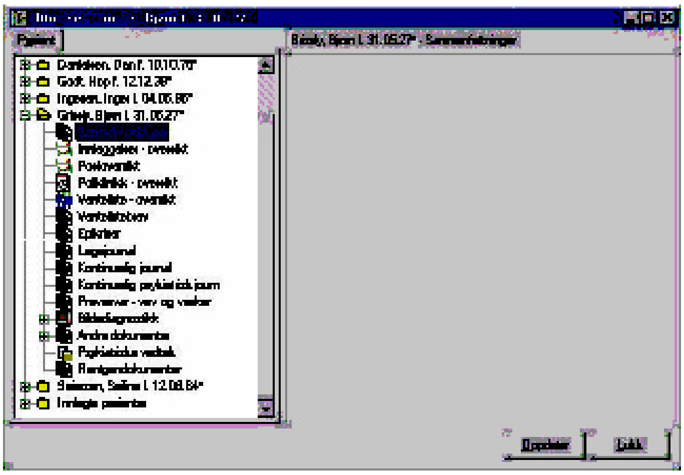
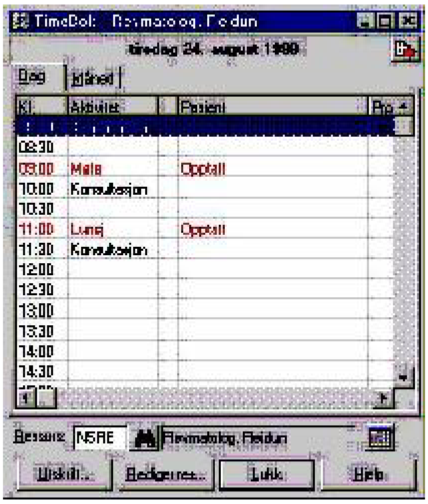


Figure 3: DIPS' journal explorer



Kl.	Aktivitet		Pasient	Pro
09:30				
09:00	Møte		Opptatt	
10:00	Konsultasjon			
10:30				
11:00	Lunsj		Opptatt	
11:30	Konsultasjon			
12:00				
12:30				
13:00				
13:30				
14:00				
14:30				

Figure 4: Appointment diary.

3.2 INFOMEDIX

As of today TietoEnator HealthCare has 33 health companies as their clients and amongst these are all but one of the university hospitals. And they are involved in deliverances and activities in Sweden and Denmark as well as Norway.

INFOMEDIX is totally installed for more than 15000 users in different hospitals, ranging from large ones like Uppsala Akademiske Sjukhus in Sweden with 7000 users to Sunaas hospital with just 10-20 users. In addition Oppland, Buskerud and Telemark have contract for a full upgrade from IMx Classic to INFOMEDIX. There is also an additional common module between INFOMEDIX and IMx Classic which are being used in a number of hospitals in both Norway and Sweden.

3.2.1 Development and managing

The INFOMEDIX database server is available on all system platforms certified for SYBASE's database system called Adaptove Server Enterprise. The most usual platforms are; Microsoft Windows NT and UNIX for HP, Sun and Intel.

INFOMEDIX is mainly developed in PowerBuilder from SYBASE. PowerBuilder has a good implementation under Microsoft Windows. This implies that you can use mechanisms such as DLL, DDE and OCX. PowerBuilder has an efficient way of handling result records from SYBASE databases, and one can do stored procedures/views directly from PowerBuilder. Microsoft Visual Basic and Microsoft Java are also used a little.

Some of the standard tools used are Microsoft Word and Accelio Capture, which would make it easy for most to use.

For customer support they use PVCS Tracker I-NET for Web-based communication with the customers. This is where all the reported messages from customers are followed up. This way the customers can check the status of the different messages directly in the system.

3.2.2 What does INFOMEDIX look like?

The desktop environment of INFOMEDIX can be customized to suit every user and ward.

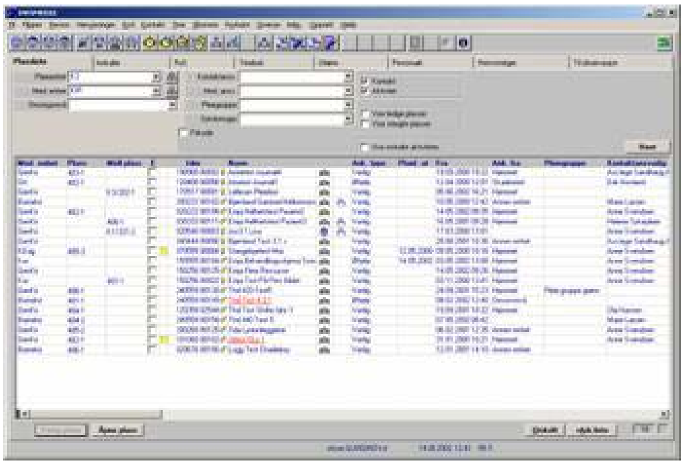
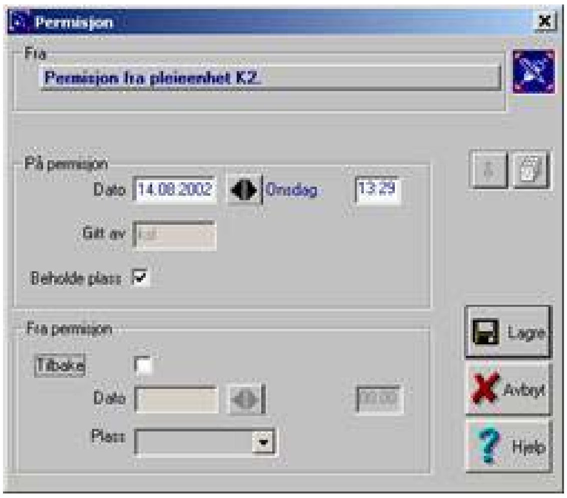


Figure 5: The users can sort the available information by the use of filters which they set themselves; they can also decide what buttons are going to be available.

It is also possible to register temporary and permanent locations of the patient, this way the nurses can keep track on where the patients are at all times.



Permisjon

Fra: Permisjon fra pleieenhet K2.

På permisjon

Dato 14.08.2002 Onsdag 13.29

Gitt av

Beholde plass ☑

Fra permisjon

Tilbake □

Dato 00.00

Plass

Figure 6: This is an overview of who of the patients have a leave of absence. You can set the different dates when he/she will be back.

Important medical information.

The registration of important medical information about a patient is done in another box; an example of this box is below.

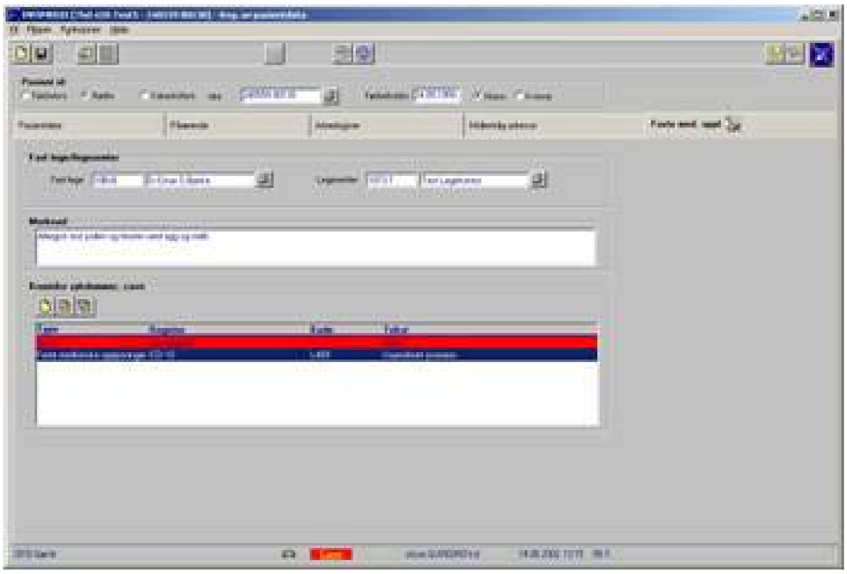
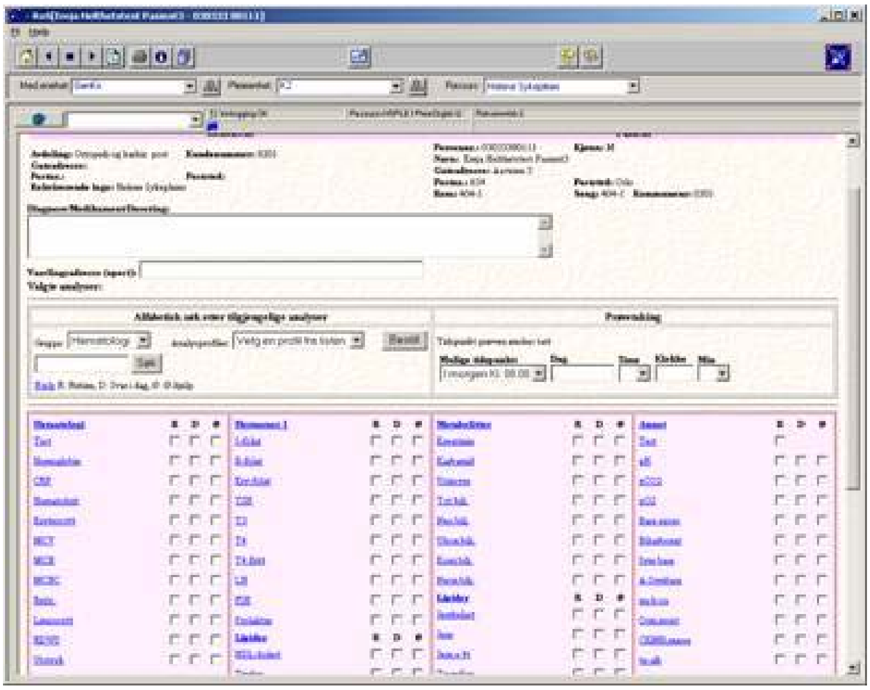


Figure 7: Registering of important information.

Requisitions and answers

Nurses sometimes need to send blood sample requisitions. This is easily done by simply clicking in the desktop. The hospitals blood sample requisitions lies here and you can just click for the tests you want taken.



Kjønn: M

Poststed: Oslo

Valgte analyser:

Prøvetaking

Gruppe: Hematologi

Analyseprofiler: Velg en profil fra listen

Søk

Mulige tidspunkt: I morgen Kl. 08.00

Dag

Time

Klokke

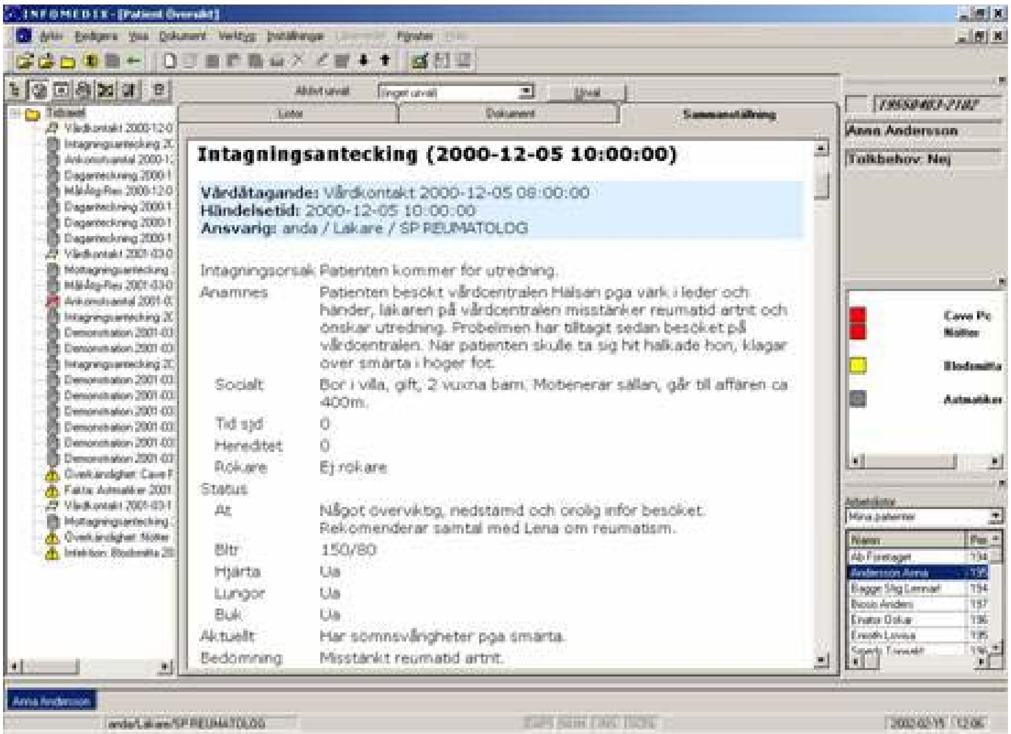
Min

Figure 8: Requisitions and answers.

Care study

The nurses' documentation tool is divided into two parts, the daily report and the care study. INFOMEDIX has a solution for both of them. You define a file for the nurses journal, in this journal you can freely add a certain number of document types.

The university hospitals in Norway have chosen VIPS (Norwegian abbreviations for Well-being, Integrity, Prevention and Security) as a model for the documentation of the nursing in the patient journal. This is also the system that is most used in Sweden. INFOMEDIX then thought it best to arrange this method of documenting first.



Intagningsanteckning (2000-12-05 10:00:00)

Vårdåtagande: Vårdkontakt 2000-12-05 08:00:00
Händelsetid: 2000-12-05 10:00:00
Ansvarig: anda / Läkare / SP REUMATOLOG

Intagningsorsak	Patienten kommer för utredning.
Anamnes	Patienten besökt vårdcentralen Hälsan pga värk i leder och händer, läkaren på vårdcentralen misstänker reumatid artrit och önskar utredning. Probelmen har tiltagit sedan besöket på vårdcentralen. När patienten skulle ta sig hit halkade hon, klagar över smärta i höger fot.
Socialt	Bor i villa, gift, 2 vuxna barn. Motionerar sällan, går till affären ca 400m.
Tid sjd	0
Hereditet	0
Rökare	Ej rökare
Status	
At	Något överviktig, nedstämd och orolig inför besöket. Rekomenderar samtal med Lena om reumatism.
Bltr	150/80
Hjärta	Ua
Lungor	Ua
Buk	Ua
Aktuellt	Har sömnsvårigheter pga smärta.
Bedömning	Misstänkt reumatid artrit.

Figure 9: The nurses' documentation tool.

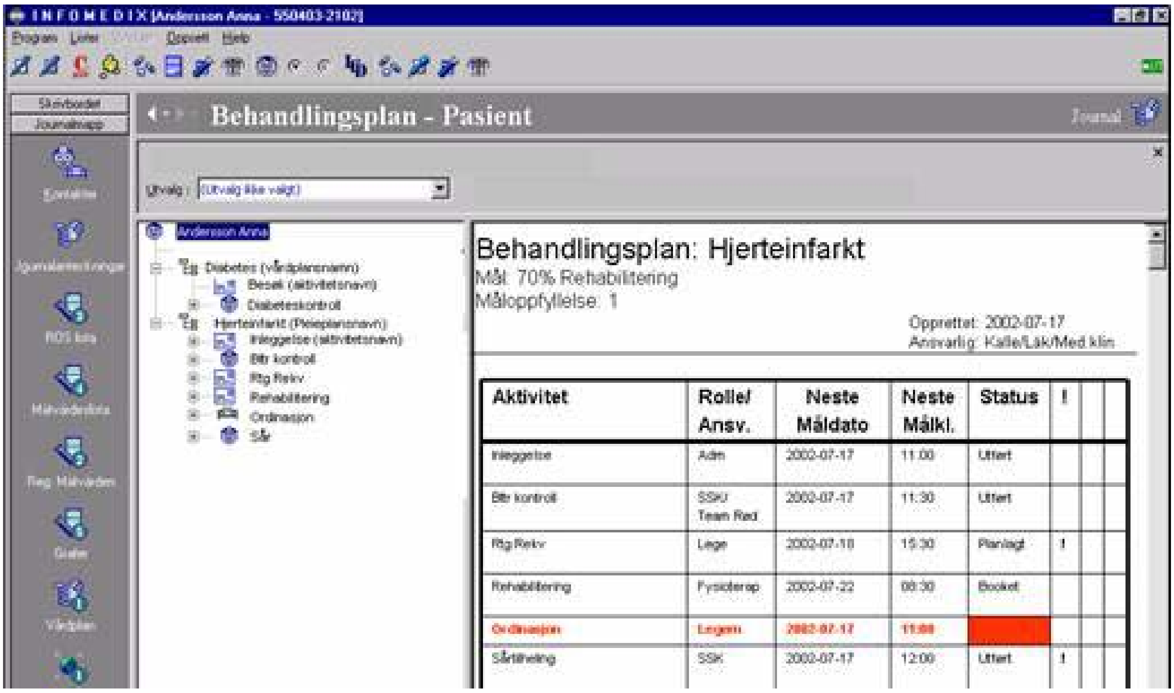
VIPS is divided into three parts;

1. The main word you want to search for.
2. The search word.
3. The sub search word.

Together these words are built up in a hierarchal way, and when you add the option to search for free text, this will be a clearly set out way to build up the journal. VIPS has been used in paper form in Sweden for many years, and now it is converted to a digital form, the necessary adjustments must be made. This will be done in co-operation with the nurses.

Treatment plan

There is a module for treatment plans in INFOMEDIX. This is a module that supports the processes around the patient and will work as a guidance system for the doctors.



Behandlingsplan - Pasient

Behandlingsplan: Hjerteinfarkt

Mål: 70% Rehabilitering

Måloppfyllelse: 1

Opprettet: 2002-07-17

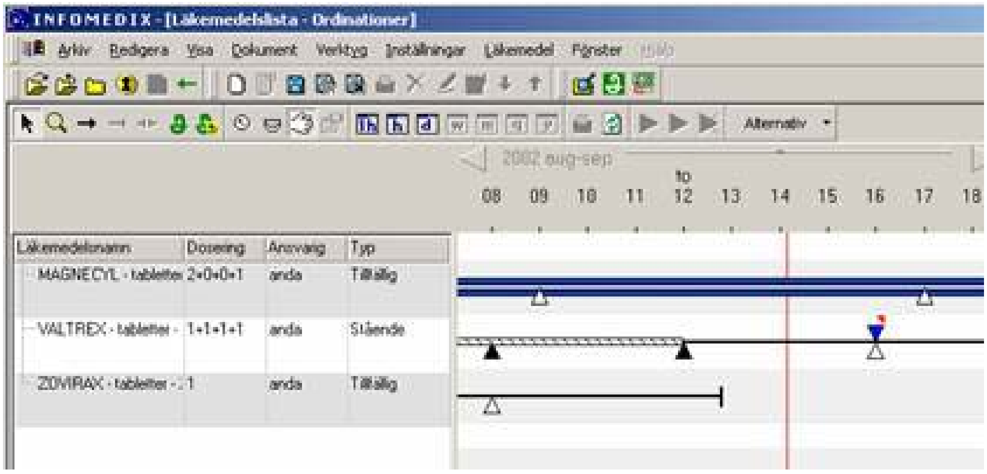
Ansvarlig: Kalle/Läk/Med klin

Aktivitet	Rolle/ Ansv.	Neste Måldato	Neste Målkl.	Status	!		
Inleggelse	Adm	2002-07-17	11:00	Utført			
Bltr kontroll	SSK/ Team Rød	2002-07-17	11:30	Utført			
Rtg Rekv	Lege	2002-07-18	15:30	Planlagt	!		
Rehabilitering	Fysioterap	2002-07-22	08:30	Booket			
Ordinasjon	Legem	2002-07-17	11:00	🟥			
Sårtilheling	SSK	2002-07-17	12:00	Utført	!		

Figure 10: The INFOMEDIX treatment plan window.

The registration of medication

The medication module in INFOMEDIX has an option that makes it possible for the doctors to register the patients' medicine. The nurses can also sign for what is being given to the patients. This way you get a complete list of what kind of medication the patient has been given.



Läkemedelsnamn	Dosering	Ansvarig	Typ
MAGNECYL - tabletter	2+0+0+1	anda	Tillfällig
VALTREX - tabletter -	1+1+1+1	anda	Stående
ZOVIRAX - tabletter -	1	anda	Tillfällig

Figure 11: The medication module.

For more detailed information please visit INFOMEDIX's website listed in Appendix B [6].

3.3 DocuLive

Software Innovation ASA's DocuLive is a complete and adaptive solution for handling of documents, and it is just as good for private as well as public enterprises. DocuLive is the market leader within government administration, but it is also used in many other organizations, it has more than 70 000 users in over 12 different countries. DocuLive is a tool for producing, managing, filing and reusing of the enterprises most important source of information, namely the documents.

DocuLive has a web-interface as an alternative to the traditional Windows-based client-server solutions and offers its users full DocuLive functionality through a regular webbrowser. This also adds other functionalities like remote administrating of the DocuLive system, easy access for mobile users etc.

The core of the DocuLive-concept is a general functionality for storing of electronic documents, filing and retrieving, in addition you get a support function for the workflow. With the basis of this platform Software Innovation offers general standard systems for both public and private enterprises, and tailored systems for those who want and need that, which makes it perfect for using in both big and small enterprises.

For the public sector DocuLive is approved as a Noark-4 system (Noark-4 is a specification for electronic filing systems in the public sector, which have certain demands regarding contents, structure and functionality) on an O2-level and include modules for filing, electronic journals, general executive work, plan etc.

For the private sector DocuLive's general filing-and case functions based on the Web and MS Outlook especially suitable for handling the documents.

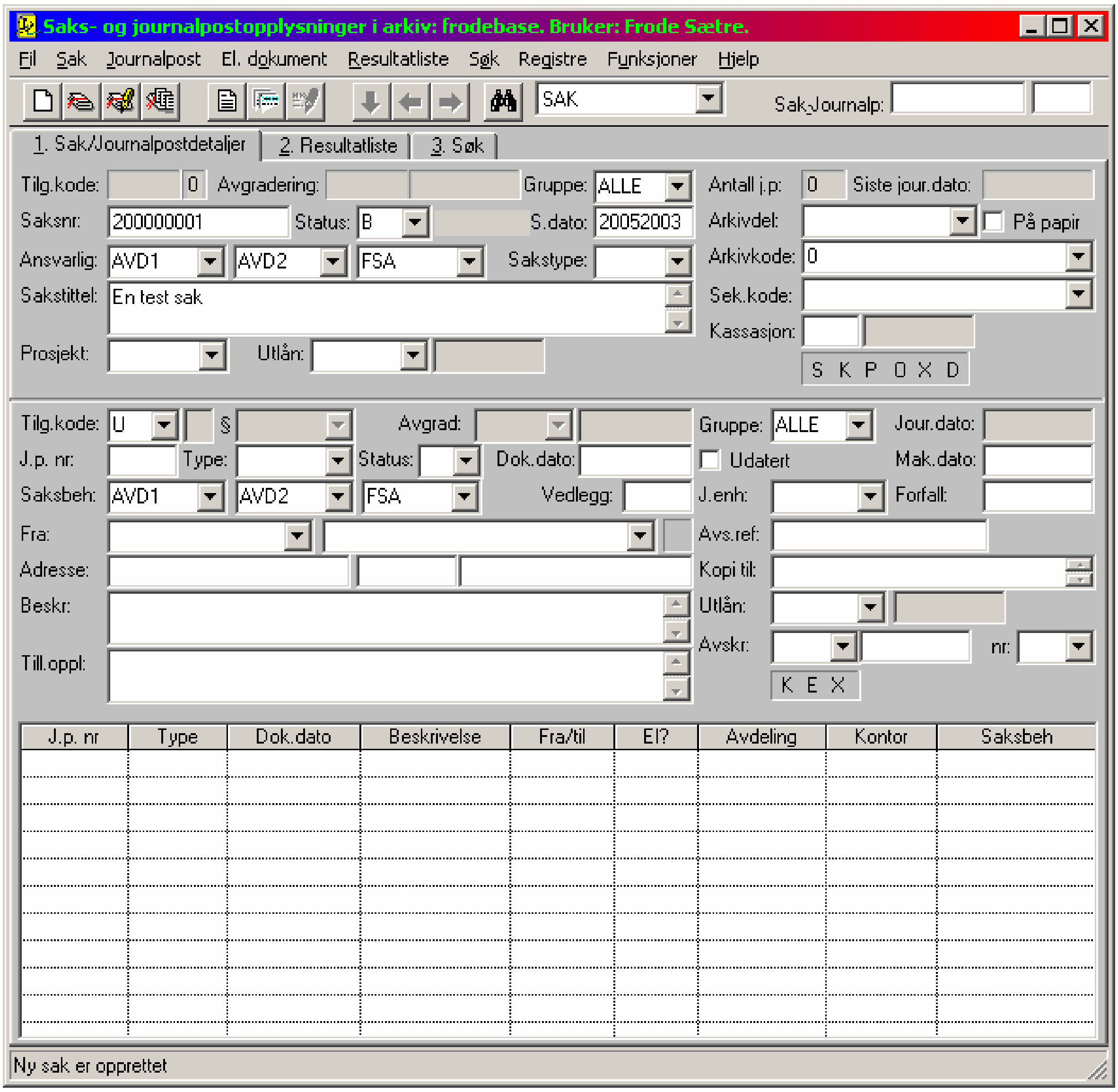
DocuLive has 10 different modules that are available and are meant for different kinds of work, these are:

1. Follow-up module (Oppfølgingsmodul)
2. Basic Document Archive (Basic Dok. arkiv)
3. Basic WWW (Basic WWW)
4. Microsoft Office (Microsoft Office)
5. Meetings and committees (Møte og utvalg)
6. NOARK Plus (NOARK Plus)
7. NOARK WWW Case (NOARKS WWW Sak)
8. Plan- and Build Case (Plan- og byggesak)
9. Case progress (Saksgang)
10. Administration, Council and Committees (Styre, Råd og Utvalg)

More information about DocuLive can be found by following the hyperlink in Appendix B [5].

3.3.1 What does DocuLive look like?

The pictures below give you some indication of what DocuLive looks like.


Saks- og journalpostopplysninger i arkiv: frodebase. Bruker: Frode Sætre.

SAK

Tilg.kode: 0

Gruppe: ALLE

Antall j.p: 0

Saksnr: 200000001

Status: B

S.dato: 20052003

Ansvarlig: AVD1 AVD2 FSA

Arkivkode: 0

Sakstittel: En test sak

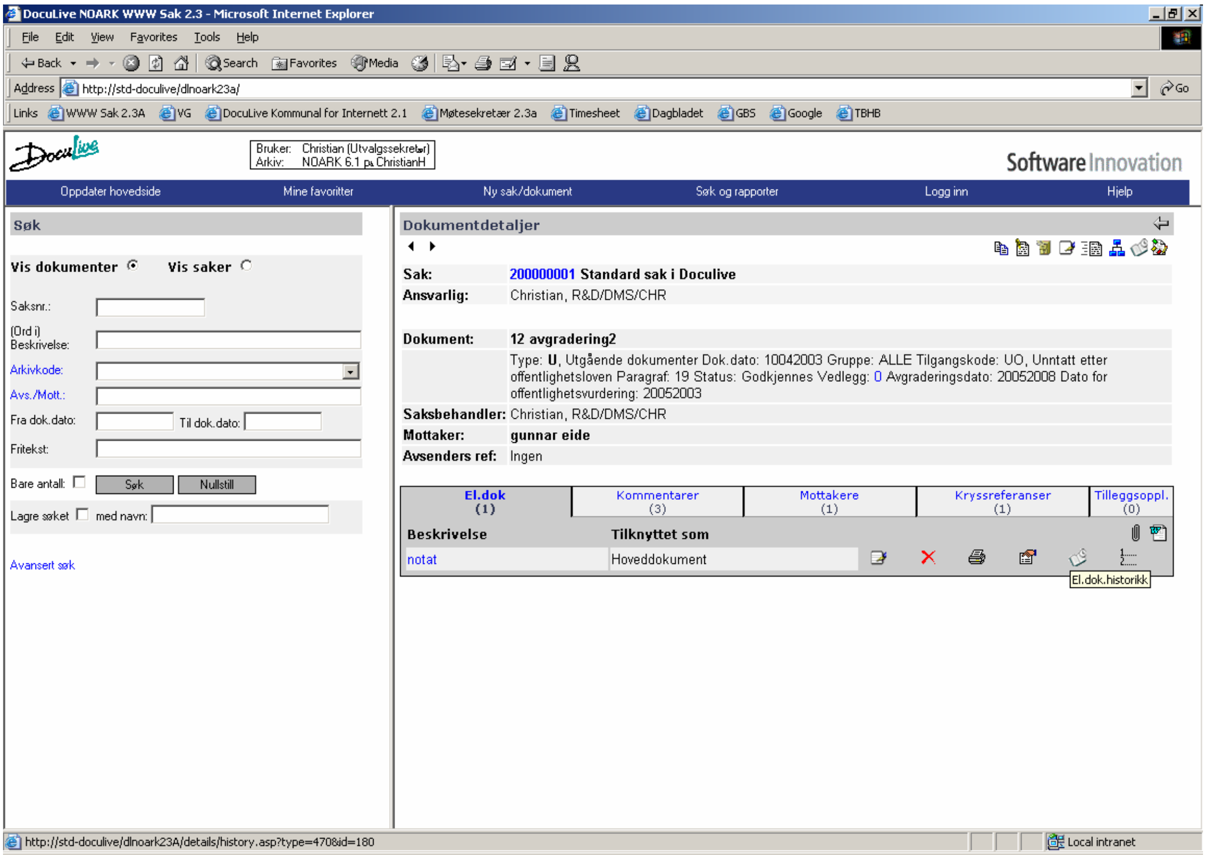
Tilg.kode: U

Gruppe: ALLE

Saksbeh: AVD1 AVD2 FSA

Ny sak er opprettet

Figure 12: The filing client in DocuLive.



Bruker: Christian (Utvalgssekretær)
Arkiv: NOARK 6.1 på ChristianH

Sak: 200000001 **Standard sak i Doculive**
Ansvarlig: Christian, R&D/DMS/CHR

Dokument: **12 avgradering2**
Type: **U**, Utgående dokumenter Dok.dato: 10042003 Gruppe: ALLE Tilgangskode: UO, Unntatt etter offentlighetsloven Paragraf: 19 Status: Godkjennes Vedlegg: 0 Avgraderingsdato: 20052008 Dato for offentlighetsvurdering: 20052003
Saksbehandler: Christian, R&D/DMS/CHR
Mottaker: **gunnar eide**
Avsenders ref: Ingen

Beskrivelse	Tilknyttet som
notat	Hoveddokument

Figure 13: The case client in DocuLive.

4 Laws and rules

The following chapter will point out the laws that have a specific relevance concerning patient journals and especially Electronic Patient Journals. This is not a detailed explanation of all the rules, but a brief description of the rules that apply to this standard, hence this cannot be looked upon as a complete collection of the laws. In addition to this description, we will include references to the legal framework. [23]

4.1 Health legislation

4.1.1 Rules concerning health personnel

The Health Personnel Law (Helsepersonelloven) contains regulations concerning the duties and responsibility of the personnel working within the health sector, which includes professional secrecy, disclosure requirements, the duty to report and information requirements.

Definitions
The law contains three definitions which are central for this standard:

Health personnel
Health personnel in this context means:

1. Personnel with authorization after § 48 or license after § 49.
2. Personnel in the health department or in a pharmacy who performs functions mentioned in the third section of the paragraphs.
3. Students who in relation to going through a medical training as mentioned in the third section.

Healthcare
The term Healthcare means any action which has a preventative, diagnostic, treating, health conserve and/or a rehabilitating goal which is performed by authorized health personnel.

The duty to perform documentation requirements
This law resides in § 39:

> He who performs healthcare, has a duty to record or register information mentioned in § 40 in a journal for every single patient. The duty to perform documentation requirements do not apply for health personnel who assists after instructions or guidance from other health personnel. In a health institution one person shall be appointed the responsibility for each journal, which includes taking decisions to what should be in the journal.

§ 40 say that the contents of the journal should be in accordance with good decency and just the relevant and necessary information about the patient and the healthcare. It is also a demand that the journal says who has written it.

When it comes to the patient's access rights to his own journal, the healthcare law refers to the patient right law § 5-1, where the patient, with the exception of special circumstances, has a right to view his/her own journal, included all supplements.

Electronic Patient Journal

In § 46 it is written that a patient journal can be written and kept electronically, and that purviews can be given in a regulation. The specialist healthcare law open up for the use of electronic journals at the enterprises which this rule applies to, and the law of health register opens up to that all forms of health registers can be stored electronically, included patient journals.

Professional secrecy, information requirements and the access to information.

§ 21 contain the main rule for professional secrecy:

> Health personnel shall prevent that other people get access to or knowledge about information concerning other people's health conditions or other personal conditions which they get access to as health personnel.

§§ 22 – 38 contain rules concerning who should have access to information concerning healthcare, included rules about the health personnel's duty to give information about certain conditions to the various public authorities.

The main rule is that health personnel have professional secrecy concerning all conditions in regards to the patient, and other people such as the patient's next of kin. The information can be given to others if and only if the person whose information we are talking about approves.

The main statutory concerning giving information to your co-workers can be found in § 25:

> Unless the patient says you cannot, the information can be given to co-workers when this is necessary so that you can provide the proper healthcare.

This rule has a parallel in § 45 which regard the patient information in the journal directly:

> Unless the patient says you cannot, the health personnel mentioned in § 39 can give the journal or information in the journal to other people who perform healthcare after this law, when it is necessary in order to provide

> the proper healthcare. It shall appear from the journal that other health personnel have been given access to the journal.

Information, such as the diagnosis, can be given to the head of the enterprise without the consent of the patient.

Correction and erasing of information in the journal
These rules are given in §§ 42-44

> Wrong, faulty or improper information or statements in a journal are to be corrected. When this is done the journal is to be rewritten, or one can also make a dated correction which is to be added in the journal. Information or statements are not to be deleted.

The law concerning health registers and electronic storing of information regarding health
As of January 1st 2002 a new Health Register law will come into force which will include a number of purviews that are relevant to Electronic Patient Journals. This applies for the use of the personal health information's general agreement concerning patient journals and other health registers, and the suggestions make up an important part of basic foundation for the demands regarding controlling who gets access to the sensitive data that the journals consists of.

The purpose of this law is to contribute to giving the health management and the health service information and knowledge so that health care can be given in a proper and efficient way. The law is present to ensure that health information is treated in accordance with the basic respect it should have, including the need for personal integrity etc.

4.2 Regulations managed by the Data Inspectorate

The Data Inspectorate is an independent administrative body subordinated the King and the Justice Department. Neither of them can give instructions nor reverse a decision made by the Data Inspectorate.

Some of the Data Inspectorate's duties are to control that rules and regulations regarding personal information is being followed, and that errors are corrected. They also have responsibility to control that the managing of personal information is done so in a secure matter.

All kinds of person registers and all electronic treatment of personal information are managed by the Data Inspectorate, which means that they have a central part concerning Electronic Patient Journals, meaning that everyone managing personal information must uphold these rules.

4.3 Government rules considering online health servers

We were in contact with the Data inspectorate and asked about rules concerning servers that were online all the time. Since this is health information, they pointed at the Health Register Law. This law applies for records information that contains health information. Therefore we will take a closer look on this law. [13] [23]

4.3.1 The Health Register Law (Helseregisterloven)

There has been an increased usage of information technologies in the health sector. It is now easier to register, store and exchange information. The information about patients themselves is increasing. This increasing use of information technology will make it harder to keep the information confidential and for the health workers to keep their professional secrecy. The Health Register Law was made to take care of the patient's security and at the same time make sure it is possible for the health sector to use the available information technologies.

One of the important questions for the health service is how to secure the information's confidentiality and reliability and at the same time that the necessary information is available to treat patients.

Three goals are essential here:

- To maintain good information security, in other words secure confidentiality, integrity and accessibility.
- To increase health personnel's skills in use of information technologies and work in good attitude towards information technologies.
- To improve the communication and co-operation between different links in the health service that is treating patients.

There are three interests that are in focus: *patients, society* and *protection of personal privacy*. These three interests are frequently identical, but not always. In critical situations considering life and death, protection of professional secrecy will have to step aside for the treatment the patient. In some other situations where protection of professional secrecy stands against health needs, it will have to be a balance between those two interests. In those situations were there are conflicts between the interest of research and the interests of protection of personal privacy, it is the interest for research that will have to give away.

4.3.2 The most relevant sections in Health Register Law

Electronic patient journals are allowed to be used in health registers

Electronic Patient Journals and other registers directed towards treating of patients are not obligated to get official permission from the Data Inspectorate, but those that want to create a register have to note the Data Inspectorate about it. Those businesses that use health registers are responsible for the registers and the use of it. Therefore the business needs to have a good security strategy.

Nationwide central registers suggest established by the King in Council
This is done so the registers will have more foundation in the laws. This will secure that:

- There will be more debate about the registers.
- Thoroughly study of what information is needed.
- That the decision-making authority is outside the health service.
- A flexible system that ensures that health information is treated after principles of relevance, impartiality and after the object of the Norwegian Government.

The King in Council gives regulations for regional and local health registers
This is done so the law can insure that county councils and local councils can fulfil their obligations to the laws about health services. The King in Council also gives external conditions for the management of the health information in regional and local health registers.

Patient's approval is the main rule by collection of information to local, regional and central registers
To collect information in health registers you need the patient's approval. This is done so the patients should have control of what information is stored in the registers. The King in Council can decide that health information should be transferred to central, regional or local registers without taking respect to the professional secrecy. This can be done without the patient's approval, but should only be given if it is necessary for the register to attend to purpose.

It is the responsible register manager duty to transfer health information to central, regional and local as provided in regulations
It is the register manager's duty to give the information to registers as said in the regulations. This also applies to information that has to get the patients approval.

Authorization to collect statistics from county and local councils
The Central Bureau of Statistics collects information to use for statistic purpose. This information is used in the government as a basis to make plans for economics in the health sector.

Authorization to make it a duty to use certain code and classification systems

To avoid too many differences in messages, certain codes and classification systems should be used. This will make it much easier to manage the messages.

Authorization to distribute of health information for linking and making of anonymous information

The health registers contains much valuable information that should be used as basis for decisions and planning in the administration. It should also be used for research to improve the health service. All delivery of information is on basis of a defined purpose. To use the information in more appropriate ways, without letting it compromise the protection of privacy, anonymous information should be used if possible.

Health service's professional secrecy

Everyone that manages health information has by the law, professional secrecy.

Securing of health information

The information that is stored in registers is sensitive information and therefore it has to be secured. These security rules should follow the Personal Record law (Personregisterloven) and should not depart from that one without good reason.

Right to get information by transferring or distributing of health information

The patient have a right to be informed when there is a transferral or distributing of information involving him/her, what kind of information and what purpose there is with the transfer or distribution.

Patient's right to access

The patient has the same right of inspection in local, regional or central health registers as he has in the patient journal. The patient can demand information about himself deleted. The basis for getting the information deleted is that it is incriminating for the patient. It might not be deleted if there are strong public reasons to store the information.

5 Transferring the information securely

When it comes to Electronic Patient Journal the most important thing is how to transfer a journal over the Internet without anybody having a chance to sneak a peak at it. We will in this section look at how one can make it possible to get information untouched from a point A to a point B.

The information below is gathered from the RSA Security website [10], this site goes much more into detail on how the different standards work and shows the mathematic algorithms and the different object classes used.

This can be achieved by the use of PKI (Public Key Infrastructure) which takes advantage of something called PKCS (Public Key Cryptography Standards). The PKC Standards consist of a number of components called PKCS #1, #3, #5, #6, #7, #8, #9, #10, #11, #12, #13 and #15. PKCS #2 and #4 have been incorporated into PKCS #1. Numbers 12, 13 and 15 are still drafts.

5.1 The different standards

5.1.1 PKCS #1: RSA Cryptography Standard:

This standard provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptography primitives, encryption schemes, signature schemes with appendix, ASN.1 syntax for representing keys and for identifying the schemes. [24]

5.1.2 PKCS #3: Diffie-Hellman Key Agreement Standard:

This standard describes a method for implementing Diffie-Hellman key agreement. The intended application of this standard is in protocols for establishing secure communications. [25]

5.1.3 PKCS #5: Password-Based Cryptography Standard:

PKCS #5 provides recommendations for the implementation of password-based cryptography, covering key derivation functions, encryption schemes, and message-authentication schemes. This standard is sometimes referred to in implementations as Password Based Encryption (PBE). [26]

In most applications of public-key cryptography, user security is ultimately dependent on one or more secret text values (passwords). A password in itself is not applicable as a key to any conventional cryptosystem, so some processing of the password is necessary to perform cryptographic operations on it.

A usual approach to password-based cryptography is to combine a password with a *salt* to produce a key. The salt can be viewed as an index into a large set of keys derived from the password, and need not be kept secret. Although it may be possible for an opponent to construct a table of possible passwords (called "dictionary attack"), but constructing a table of possible key will be extremely difficult because of the vast number of possible keys for each password. An opponent will therefore be limited to searching through passwords separately for each salt.

5.1.4 PKCS #6: Extended-Certificate Syntax Standard:

This standard is currently being phased out, and will be replaced by X509 v3. [27]

5.1.5 PKCS #7: Cryptographic Message Syntax Standard:

This standard describes general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. It is the basis for RFC 2630 Cryptographic Message Syntax (CMS) which updates PKCS #7 to support attribute certificates and key exchange algorithms. It is used to provide message security in S/MIME. [28]

5.1.6 PKCS #8: Private Key Information Syntax Standard:

PKCS #8 defines a standard for password protected private keys. This standard describes a syntax for private-key information. Private-key information includes a private key for some public algorithm and a set of attributes. The standard also describes a syntax for encrypted private keys. A password-based encryption algorithm (for example one of those in PKCS #5) could be used to encrypt the private-key information. [29]

5.1.7 PKCS #9: Selected Attribute Types:

Defines selected attribute types for use in other PKCS standards. [30]

5.1.8 PKCS #10: Certification Request Syntax Standard:

This standard defines a syntax for certification requests. It consists of a distinguished name, a public key and optionally a set of attributes, signed by the entity requesting certification. Certification requests are sent to a certificate authority, which transforms the request into an X.509 public key certificate. [31]

5.1.9 PKCS #11: Cryptographic Token Interface Standard:

PKCS #11 describes a programming interface named "Cryptoki" for doing cryptographic operations with hardware "tokens" (typically a "smartcard"). Popular applications like Netscape use PKCS #11 to provide smartcard support for their SSL and S/MIME capabilities.

PKCS #11 has now come into the next stage called PKCS #11 v2.11. This version introduced the concept of Personal Trusted Devices (PTDs) and a signature mechanism, CKM_CMS_SIG, aimed to allow users to benefit from such devices. A PTD that receives a message to sign through this mechanism may, depending on the messages content type, be able to securely present the message to the signer before asking for authorization.

When the message to sign is not a MIME message itself, the recipient will have to rely on the caller's stated content type when determining the presentation mechanism. Since the stated content type is not included in the signature, there is a possibility for an attack where the caller may take advantage of differences in presentation mechanisms for various content types in the PTD.

By defining an (authenticated) attribute intended to carry the alleged content type, this amendment presents one method to protect against such attacks. Note that for this method to succeed, a PTD must not allow the caller to assign the value of this attribute directly; the value must be the caller's stated content type, which was used by the PTD to decide on a particular presentation mechanism. [32]

5.1.10 PKCS #12 Personal Information Exchange Standard:

Specifies a portable format for storing or transporting a user's private keys, certificates, miscellaneous secrets, etc. [33]

5.1.11 PKCS #13: Elliptic Curve Cryptography Standard:

Describes mechanism to encrypt a sign data using elliptic curve cryptography. [34]

5.1.12 PKCS #14:

This standard covers Pseudo Random Numbers Generators (PRNG). This is currently under active development.

5.1.13 PKCS #15: Cryptographic Token Information Format Standard:

PKCS #15 is a standard that describes the format of cryptography credentials stored on cryptographic tokens. [35]

5.2 What are electronic signatures and encryption all about?

In today's society more and more of the information we exchange are transferred digitally, and the fact that broadband becomes more and more available in most homes contribute to the increased information stream. This development means that paper based products will have to be produced in new and digital forms. A good example of this is your signature. Its digital equivalent is called electronic signature and is more and more used to sign digital information.

This enormous technological development has also created a need to integrate secure solutions which contributes to keep the data out of harms way, not just for the industry but also for the common computer user at home. The new regulation concerning electronic communication is all about this development. We will look further at this below.

When talking about information security electronic signatures and encryption always seem to come up, but what do they really mean? These are very important subjects when it all boils down to securing information and keeping it secure. The different security routines we will discuss here are: *authentication, integrity, non-repudiation* and *confidentiality.*

By using these techniques we achieve that the sender of electronic messages can identify who he or she is and the recipient is able to confirm that the person (or computer) really are who they say they are. We will be able to find out if the information we send get to the receiver without being altered, in addition we can get proof that makes it hard, if not impossible, for both the sender and receiver to deny that they have sent or received the file. Sending and receiving of messages and "hide" them so that people who are not supposed to view them cannot. [11] [12]

5.2.1 Security services

This is a description of a quality that we want or need in a system, and does not explain what kind of means we use to realize this solution. A security service is realized or implemented with the help of specific security mechanisms and/or security techniques which we will try to explain below.

- **Authentication:** This is a security service that assures that information that identifies an entity (whether it is a person, machine, system etc) really is correct. Regarding the exchange of electronic messages, authentication will clarify that the sender of a message really is who they say they are and with that link the sender to the contents of the message. The authentication of users who logs on to an electronic system is extremely important and makes the basic building blocks of who we can trust in a security system. The need for authentication will depend on what kind of message we are about to send. In most transactions authentication is desirable or necessary to establish a common trust.
- **Integrity:** A security service which goal is to see to that the information cannot be altered while being stored or during the transport of the data

without it being discovered. If we were not sure whether or not the data can be altered there is a need for a integrity service. This type of integrity for data, information etc, must not be confused with information quality, which is whether or not the information is right. We can have information integrity even though the information is wrong. Here is a little example: Let us say Dr. Hansen wrote in Mr. Jensen's journal that he had broken his left arm, even though it was the right, and uploaded this to the EPJ server. Mr. Jensen's journal would still have the same information integrity as before, but it contains an error, which would be the lack of information quality.

- **Non-repudiation:** Non-repudiation is a service that provides the receiver a certainty that the alleged sender cannot later deny that he/she was the one who actually did send the document. This can also work the other way, i.e. the receiver cannot claim that he/she did not receive the document. The way this works is that the receiver sends a "receipt" that he/she got the message that was sent, this way there is no denying they got the message.
- **Confidentiality:** This service makes sure that the information will not be made available for unwanted people. To do this we use encryption to make sure nobody can view the document during the transport or storage, and even though somebody should get their hands on the document it would be unreadable without the proper key. The Civil Service Act does not say how one should obtain this, but it does say that professional secrecy is a must concerning all information regarding personal relations, and that this should be done in an ensuring way.
- **Traceability:** This is to ensure that important events in the system can be traced back to whoever is responsible. To ensure that you got trace ability, you would also need authentication services. Because without it you would not be able to tell who sent the information.
- **Availability:** We always need availability. This is to make sure that the person(s) who are supposed to have access to the information can get it when they need it. EPJ would not do much good if the doctors were not able to retrieve the patient's journals. Hence availability is one of the most important services, without it the other services would neither be a necessity. We will try to explain what we mean by that. If the server that all the journals were stored at was not online, then we would not need the other services. Simply because nobody would be able to get their hands on the journals without physically being in the same room as the server.

The services mentioned above are what together define security mechanisms. Cryptography is a very detailed field, but the basics are somewhat easier to under stand. To make it a bit easier to understand we will use some pictures and explain what really happens when information is sent over for example the Internet.

5.2.2 Symmetric crypto:

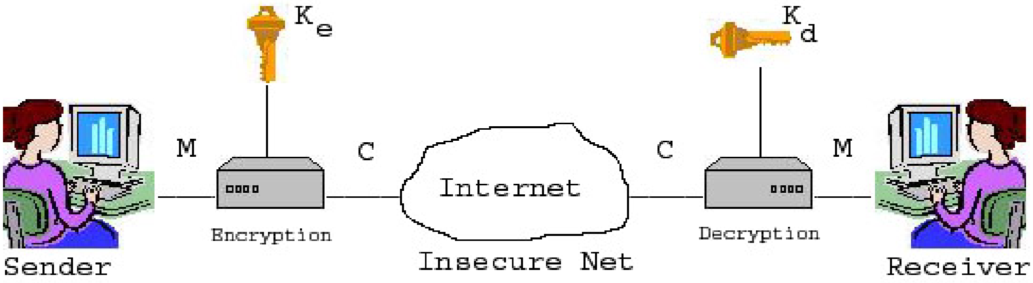


Figure 14: Encryption via the Internet

The sender has a message M in plain text which she wants to send. But before she sends it she wants to make sure that nobody can get the message on its way to the receiver and read it, so she encrypts it. When the message is being encrypted it is mixed with an encryption key K_e. The result of this is a message C which is not understandable unless you have the right key K_d to decipher it with. This key K_d must be used to decipher the encrypted message C back into its clear text form M. It is imperative that nobody else than the receiver has the key K_d.

In conventional or symmetric crypto systems the same key is used for both the encryption and the decryption, in other words $K_e = K_d$. Therefore this key must be distributed in a secure way, which will be expensive and demanding if many users are going to have this key.

The encryption function takes use of a crypto algorithm, which describes how the clear text and the key are to be mixed. There are lots of different algorithms that can be used, but there is not one common international standard. DES (Data Encryption Standard) is the American standard which is used a lot, but the problem, if one can call it a problem, is that it is over 25 years old. National Institute of Standards and Technology (NIST) have recently approved a new standard symmetric encryption algorithm called AES (Advanced Encryption Standard). NIST is an agency under The Ministry of Industry in the US.

5.2.3 Asymmetric crypto

In an asymmetric crypto or public key cryptosystem there is no longer a connection between the encryption- and the decryption-key. That means that there is no longer a need to keep the encryption key secret as it is with symmetric crypto. In these systems each user will get his/her own pair of keys (K_e, K_d). The public key K_e can now freely be distributed to everyone who wishes to send encrypted messages to the user. It is not called *public key* because it has something to do with the public, it just simply means that it is not necessary to keep the key secret. This means that the distribution of the key no longer is neither expensive nor demanding which is the case for symmetric crypto. But we still need to have the infrastructure to be able to distribute the key in a good fashion. The secret key K_d however must not be freely distributed.

There is however one big downside to asymmetric crypto and that is that it takes to long to encrypt large amounts of data. Therefore it is common to use a mixture of the two crypto systems.

The most used and well known asymmetric system is called after its originators Rives, Shamir and Adleman, this system is called RSA.

The technology behind asymmetric systems differ from that of the symmetric a great deal, amongst other things the requirements of the length of the keys are totally different. This is a good quality in asymmetric systems; the length of the key can easily be adjusted up to the desired security level.

5.2.4 Digital signatures

The above mentioned systems are used to obtain confidentiality, in other words to make the messages unreadable to the public. But so far nobody has been identified neither the sender nor the receiver. There is one way identification can be obtained by using an asymmetric system. If a person who has a secret key K_d encrypts a message with this key and sends it, the receivers who has the public key knows that it is the owner of the secret key who sent the message. This way at least the sender identifies oneself. But this is not the best way to sign messages electronically. A better way is to use *digital signatures.* This is in fact a form of asymmetric encryption. This technique’s main goal is to realise other security services such as authentication, integrity and non-repudiation, meaning that the contents which the signature is used on do not hide the text for uninvited people. But if the message can be opened or verified, the receiver will know who sent the message, and thus he/she has “signed” the message digitally and thereby confirmed that the message has its integrity intact.

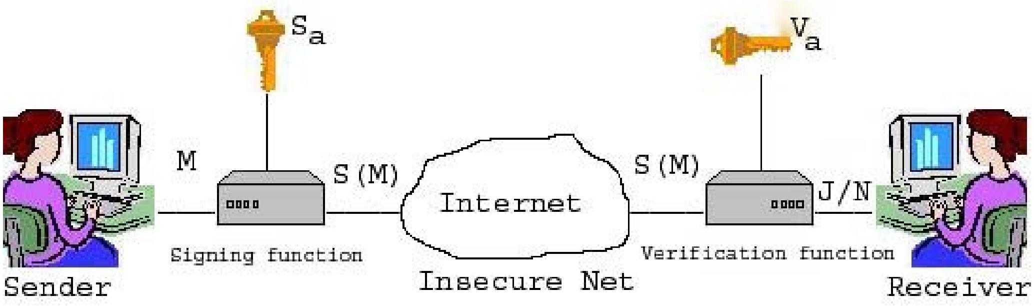


Figure 15: Using digital signatures.

The sender generates a pair of keys which contain of one secret key used for signing (S_a) and one public verification key (V_a). When the sender wants to sign an electronic document M, then M is sent together with the key used for signing the message in a sort of signing function. The result of this process is the signed message S (M). In most signing systems the signed message is the original message, untouched and in clear text, followed by a signature field where the signature is a complicated mixture of M and S_a.

When the recipient receives such a signed message he/she will have direct access to the message M. To verify that this message is the genuine message from the sender, he/she will send M together with the public verification key V_a, which belongs to the sender, into a verification function. This process will either give an approved or an unapproved result. All of this happens automatically so the receiver does not have to do anything special for this to happen. If the result is approved the receiver will know the following:

1. M probably comes from the right sender, since he/she is the only one who has the secret signature key which is needed in order to make the digital signature. The message is therefore authenticated.
2. The message or the signature field cannot deliberately be changed during the transfer, meaning that the integrity is intact.
3. In the future the sender cannot deny having sent the message. The recipient can prove to a third party that it was the sender’s secret key that was used to sign the message. Which means that the message is non-repudiate.
4. The signature also keeps the receiver from altering the original message. The recipient does not know the secret key Sa, which is needed in order to make a signature that is suitable for the modified message.

For this to work the way it is intended we need to establish an infrastructure that makes sure that all of the involved parties gain access to the different keys needed. It is especially important that everybody has access to the verification key.

To sum things up a bit you can say that in a signature system there is only one person that can sign by using the secret signing key, but several people can verify the signature by using the public verification key. In a crypto system many can encrypt messages by using a public encryption key, but only one can decrypt the text by using the secret decryption key.

5.2.5 What is a Digital Certificate?

A Digital Certificate contains for example information such as name of the owner, where he/she got it from, validity (expiration date), and other limitations if there are any. In addition a DC contains some information to prove that it is the real thing. In other words DC is resistance towards forgery and imitations.

A DC can sadly enough be misused. To keep this from happening with a DC that is no longer valid, the issuer will maintain a list called CRL (Certificate Revocation List). These lists are important to whoever that is going to use a DC to verify a transaction. The person who signs a transaction, an e-mail for example, normally sends his/her certificate with the signed message. The receiver, who has keys to check whether or not the certificate is real, will get the CRL directly from the certificate's issuer; with both the CRL and the certificate the recipient is able to accept a signed message.

5.2.6 Hashing and Digital Signatures

Tamper detection and related authentication techniques rely on a mathematical function called a hash (also called a message digest). A one-way hash is a number of fixed lengths with the following characteristics:

- The value of the hash is unique for the hashed data. Any change in the data, even deleting or altering a single character, results in a different value.
- The content of the hashed data cannot be deduced from the hash, which is why it is called "one-way".
- To create a digital signature, a one-way hash of the data is created and then encrypted with a private key.

5.3 PKI – Public Key Infrastructure

5.3.1 What is PKI?

Public Key Infrastructure combines software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions on the Internet. PKI's integrate digital certificates, public-key cryptography, and certificate authorities into a total enterprise-wide network security architecture. A typical enterprise's PKI encompasses the issuance of digital certificates to individual users and servers, end-user enrolment software, integration with corporate certificate directories, tools for managing, renewing, and revoking certificates, and related services and support.

5.3.2 How Public Key Encryption works

Public Key Encryption uses pairs of keys, one public key and one private key, associated with an entity that needs to authenticate its identity electronically to sign or encrypt data. Each public key is published, and the corresponding private key is kept secret by a Certificate Authority. Data encrypted with a public key can be decrypted only with the corresponding private key. In general, to send encrypted data to someone, you encrypt the data with that person's public key; the person receiving the encrypted data decrypts it with the corresponding private key. And vice versa; data encrypted with your private key can be decrypted only with your public key. Private Key encryption is an important feature because it allows you to sign with your digital signature. See Table 1 to see whose and which key is used when.

Table 1: Which and whose keys are used when you encrypt and decrypt messages and signatures.

What to do.	Whose key:	Which key:
Send an encrypted message	Receiver's key	Public key
Send an encrypted signature	Sender's key	Private key
Decrypt an encrypted message	Receiver's key	Private key
Decrypt an encrypted signature (and authenticate the sender)	Sender's key	Public key

5.3.3 Validating Data Integrity

During transaction within PKI, two items are transferred to the recipient of the signed data, the original data and the digital signature, which is basically a one-way hash of the original data that has been encrypted with the signer's private key. To validate the integrity of the data, the receiving software first uses the signer's public key to decrypt the hash. It then uses the same hashing algorithm that generated the original hash to generate a new one-way hash of the same data. Finally, the receiving software compares the new hash against the original hash. If the two hashes match, it was not changed since it was originally signed. If they do not match, the data may have been altered, or the signature may have been created with a private key that doesn't correspond to the public key presented by the signer.

5.3.4 The role of the Certificate Authority

After validating the data by matching the public and the private keys, they must then make sure that the public key used really belongs to the person that sent the data. The Certificate Authorities (CA) are entities that validate identities and issue certificates. Either third parties or organizations running their own certificate-issuing software can act as CA's. The methods used to validate identity vary depending on the CA, but is usually accomplished by a Registration Authority (RA). These methods involve a wide range, depending on the certificate level, including on-line registration, out-of-band notification, and even notary verification. The certificate issued by the CA binds a particular public key to the name of the entity the certificate identifies. In addition to a public key, a certificate always includes the name of the entity it identifies, the expiration date, the name of the CA that issued the certificate, a serial number and other information. [15]

5.3.5 The four primary services PKI provide

PKI offers four primary services, these are:

1. Authentication – Ensures that the person is who he/she claims to be.
2. Integrity – Makes sure that the data has not bee altered in any way between the sender and the recipient.
3. Confidentiality – The assurance to an entity that no one can read a particular piece of data except the receiver explicitly intended.
4. Signature services – A service that makes sure that the sender or the receiver cannot at a later point deny that he/she sent or received the data.. This service may also include time stamping.

These all support the concept of non-repudiation ensuring that transactions are legally valid and irrevocable.

5.4 VPN – Virtual Private Network

VPN is a way to provide secure access to an organization's network, for example the network at the medical office's, via a public telecommunication infrastructure, such as the Internet. A way to look at VPN is an enclosed network of leased lines that can only be used by that organization. This way of connecting networks together through for example the Internet is totally inexpensive and provides the same security as if the users were locally connected to remote networks and hosts.

The way VPN works is by using the shared public infrastructure while maintaining privacy through security procedures and tunnelling protocols. By using a tunnel you achieve a secure passage way for the data by encrypting it at the sending point and decrypting it at the receiving end, this "tunnel" cannot be "entered" by data that is not properly encrypted. It is also possible to gain even more security by encrypting the sending and receiving network addresses as well as the data.

The tunnelling protocol we will look further at is called Layer Two Tunnelling Protocol (L2TP) [19]. This protocol is an extension of the Point-to-Point Tunnelling Protocol (PPTP) used by Internet Service Providers (ISPs) to enable the operation of a VPN over the Internet. The reason why L2TP is so well used is that it uses the best features of two other tunnelling protocols, namely PPTP from Microsoft and L2F from Cisco Systems.

There are two main components that L2TP consists of;

1. The L2TP Access Concentrator (LAC), which is the device that physically terminates a call.
2. The L2TP Network Server (LNS), which is the device that terminates and possibly authenticates the PPP stream.

L2TP uses packet-switched network connections to make it possible for the endpoints to be located on different machines.

VPNs are implemented through encryption and authentication features within firewalls and routers.

5.4.1 IPsec

Most VPN uses Ipsec as cryptographic security service. IPsec allows for authentication, integrity, access control and confidentiality. You can use any IP protocol over IPsec and with IPsec you can create encrypted tunnels (VPNs), or just encryption between computers.

There are two protocols that provides for the different services. These are Authentication Header (AH) and Encapsulating Security Payload (ESP)

Authentication Header provides authentication, integrity and replay protection. It does not provide confidentiality. The Authentication Header authenticates portions of the IP header, for instance destination and source addresses.

Encapsulating Security Payload provide authentication, integrity, replay protection and confidentiality of the data. It secures everything in the packet that follows the header.

For most uses it is recommended to use Encapsulating Security Payload.

6 What information do the doctors need

In this part we will take a look on what doctors think about and how they use the Electronic Patient Journal. We have used information from a survey done by Hallvard Lærum, Gunnar Ellingsen and Arild Faxvaag. They published some results in a periodical “Tidskrift for Den norske lægeforening” [36], and also in the periodical British Medical Journal (BMJ) [37]. We also spoke to some doctors who agreed to answer some questions we had prepared.

6.1 Survey done by Lærum, Ellingsen and Faxvaag

We will here refer to the most important things they did find in the survey.

6.1.1 Facts about the survey

- The surveys objective is to compare the usefulness of three electronic medical records systems by Norwegian doctors in hospitals for general clinical tasks. The three systems are DIPS, DocuLive and INFOMEDIX.
- There were 227 participants equally divided on the three systems.
- The questions/clinical tasks were developed after 40 hours of study in five sections in two hospitals.
- The doctors where asked how often they used computers for the clinical tasks.
- The answers where divided into 5 categories, “Never or almost never” to “Always or almost always”.
- The selection was done randomly out of 32 hospitals units in 19 hospitals that has used electronic medical record systems more than 3 months. They excluded very small (below 4) and very large units (above 30).
- Trough interviews with representatives for the information sections in the hospitals they found out if the clinical tasks involved in the questionnaire was implemented in the system in that hospital.

6.1.2 Results

- There was no difference in use of computers considering age, sex and work position.
- The doctors scored high in computer usage.
- The doctors had access to computers, either in their office or in rooms used for clinical work. About 40% were weekly or daily prevented from using the computers because of others using it, and about 40% where monthly or weekly prevented from using the computers because of data errors or password trouble.

- There where limited use of the different systems, though in general 15 out of 23 tasks where supported. Mainly the tasks that where used most was those that involved reading patient data.
- There where moderate user satisfaction with the systems.

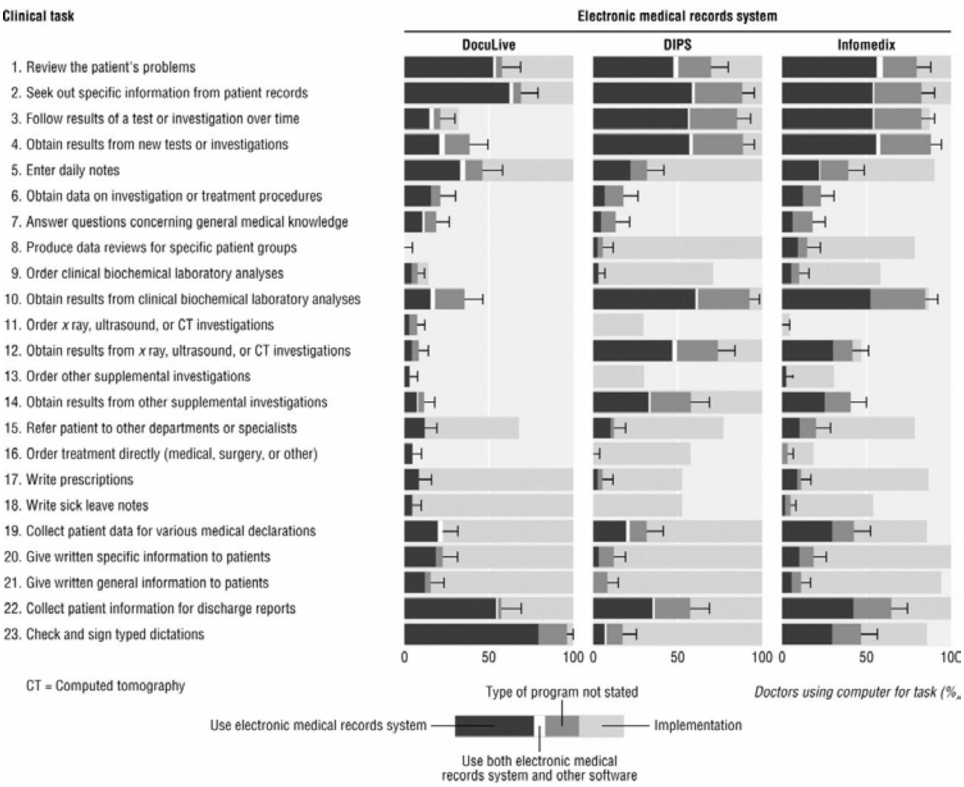


Figure 16 Picture from BMJ showing results for the survey Lærum, Ellingsen and Faxvaag did. [37]

6.1.3 What we can conclude from results:

These results are based on a survey done in hospitals. We are going to try to conclude for doctors that are working in medical offices.

- The doctors' computer usage is in general good. There is no difference on basis of sex, age or work position. The doctors working at medical offices have in general used computers longer than doctors working in hospitals, and therefore we assume that they are better in computer usage.
- The doctors working at medical offices have probably better access to computers as well. In hospitals some were prevented from using computers because other used it. In medical offices doctors have their own computer and therefore they should not be hindered from using computers. There might be some trouble with computer problems, like data errors and

password trouble. We would expect the trouble that occurs to be less for medical offices than for hospitals. So they should be well suited for using Electronic Patient Journal.

- The use of Electronic Patient Journal. The doctors used it mostly for reading information about patients. They use it less for writing reports and order different tasks. In the survey you can see that doctors use Electronic Patient Journal for less than half of the tasks overall. This means that they do not use the Electronic Patient Journal for many tasks that the systems support. This might be because the tasks is not obvious enough in the system, that they are to difficult to understand or that the doctors in general have not gotten a good enough introduction to the program.
- There where moderate user satisfaction with the system. This shows that the system may not have been made for the doctors needs or that the doctors have not gotten a good enough introduction to the system. It is also a possibility that the infrastructure inside a hospital should be changed a little with the introduction of Electronic Patient Journal. Normally if you introduce a new system without trying to introduce a new infrastructure people will only try to use the system in their old ways and not try to use it in new ways as might be done if there had been introduced a new infrastructure or new tasks division. With a new system there might be other personnel that can do the tasks the doctors now are doing.

6.2 Questionnaire

We made some questions that we sent to a couple of doctors in medical offices. We did this as a supplement to the survey done by Hallvard Lærum, Gunnar Ellingsen and Arild Faxvaag. We will here summon up what we learned from those questions.

6.2.1 What we asked about

We had 14 questions divided into 5 main themes. The 5 main themes are:

1. What routines are used when a doctor receives a patient and what information is needed about the patient?
2. What the doctor’s expectations to the Electronic Patient Journal are and what they thought the electronic patient journal could help them with?
3. If the doctors thought the introduction of Electronic Patient Journal would change their routines, organization and if it would be a strain to go over to use Electronic Patient Journal?
4. What the general knowledge about computers and computer usage is and if there is need for education together with the introduction of Electronic Patient Journals?

5. See what the doctors think would be the problems with an introduction of Electronic Patient Journal?

6.2.2 The results we got from these questions:

1. The information that is needed about the patient is name, address, date of birth, and National Identification No. The routines depend much on the situation, but it is important that the patient is properly identified.
2. The doctors thought that an Electronic Patient Journal would help them make a better diagnosis. This is because they can see what other doctors have done earlier that day or what medical history the patient has, for instance it is nice for the doctors to see what kind of medicines the patient has been given earlier that day. Patients often have trouble remembering names of the medicine and in what portion it has been given. The expectations they had to the Electronic Patient Journal is that it will ease their journaling, but then it had to be simple and easy to use. It is important that the Electronic Patient Journal is not too complicated because then it would not be used at all. They also thought that the medical offices need Electronic Patient Journal to keep up with time.
3. The doctors think that the Electronic Patient Journal will ease their work routines, but it is important that when the Electronic Patient Journal is introduced that there will not be "double work". They think that it will ease their organization of the journals and that it will not lead to big changes in the organization. They also think that it will not be a strain to start using Electronic Patient Journals. Although some introduction must be done.
4. Concerning using computers the doctors think that the general computer knowledge is variable but mostly good. Some old doctors do not like computers at all, but younger doctors are already familiar with the use of a computer and are more ready to start using the Electronic Patient Journal. In general the doctors are ready to start using Electronic Patient Journals, but that there has to be some introduction to the program like courses for the doctors. The negative effect of this is that the doctors will have to use precious time to learn how to use the new system instead of helping people who need medical attention.
5. The doctors are sceptical about the introduction cost of the system. For instance there will have to be invested some money in new equipment and new upgraded programs. They are also sceptical to if the Electronic Patient Journal can keep the professional secrecy that is required of such a system. Also that the journals will be kept in secure registers so no other than those who should have access to it will get it.

6.2.3 What we concluded from the results

When doctors receive patients they have to identify the patient. The rest of the procedure will depend on what condition the patient is in.

The doctors think that Electronic Patient Journals are needed to keep up with time and they are ready to use it, and that it will help them make a better diagnosis and journaling in general. The Electronic Patient Journal must be simple to use if it should be used in medical offices. The doctors do not have time to get to know a very complicated system.

They all agree that Electronic Patient Journals will ease their work routines and that there will not be big changes in the organization. We believe there will be changes in the organization of medical offices when the Electronic Patient Journal is introduced. When a new technology is introduced into a business it will lead to changes in the organizational structure. To reduce these changes in organizational structure, the Electronic Patient Journal system, has to be developed together with the doctors. This way they have something to say on what the program looks like and how it works. [16]

The doctors themselves think that the Electronic Patient Journal is necessary to keep up with the development in the society as a whole. Therefore it is good to see that the doctors in medical offices in general think they have good knowledge in using computers. In the survey done by Hallvard Lærum, Gunnar Ellingsen and Arild Faxvaag, they concluded that the doctors had good knowledge to computers. We do think that doctors in medical offices in general have better knowledge to computers than those in hospitals. This is because doctors in medical offices have had better access too and have used computers for a longer time than doctors in hospitals. There will always be some among the doctors that is negative to the new technology, and that will maybe apply more for the older than younger doctors. This will have to be dealt with to make the medical offices a part of the 21st Century.

The cost of implementing such a system is also a common concern amongst the doctors. If the Electronic Patient Journal shall become a success the medical offices has to be connected together. They have to invest in the new programs and maybe new computers. This will be an expensive investment and we believe that the government has to give money to the medical offices to meet the standards the 21st Century will demand.

The doctors where concerned about the professional secrecy. The professional secrecy will be maintained as good as possible in Electronic Patient Journal systems, but there will always be a possibility that someone that should not have access to a journal will get it. This is both because the Journals will be easier to access because they are stored at the same place and because human curiosity will always come into play. Most security breaks are made possible because of human mistakes. In Electronic Patient Journal systems every access into a journal should be logged to get a preventive effect on the human security.

7 Specification of the “Treatment register”

Here we will specify what we think will be a solution to how Electronic Patient Journal system can be implemented for medical offices participating in a roster for critical medical treatment.

If you look at the medical office agreement and those medical offices participating, you can imagine a small hospital with different departments. The departments have some information they can share, but not all. Local medical offices are the different departments, while “Treatment register” is the central register in a hospital. In addition the local medical offices have a register of their own.

7.1 Starting conditions

Before we specify our solution we have set some conditions that have to be in place.

7.1.1 System

Firstly we had to find out if we should try to make our own system or add to another solution already in place. If we should make our own system it would have taken us many years to specify. Therefore we chose to build on existing systems and rather make an extra module to one of those.

There are several different EPJ systems on the market, systems both for medical offices and for hospitals. The EPJ systems in use today in hospital are designed to take care of the tasks specified in the EPJ standard. This includes important subjects as security and confidentiality. Therefore we see it as a good choice to use one of those systems to further develop the uses of EPJ. The EPJ systems in hospitals are also designed too communicate between different wards. This makes sure that the infrastructure we will need for an EPJ system in our solution, already is in place. Also in the further development of the solution we expect the hospitals to come along with the medical offices in the “Treatment register” solution. The hospitals are large organisations and therefore it would be difficult to make them change the EPJ system. Medical offices are smaller offices and it would be easier for them to change the EPJ system than for the hospitals. Therefore we think it is a good solution to adapt to the hospitals now. The standard on the messages should be in the same format no matter what system is used. This is so the different systems can send information into a “Treatment register” regardless of the system.

7.1.2 Laws and regulations

When we made this solution we had to look on the Norwegian laws to find out what was allowed and what was not. We have tried to find a solution that has good basis in the Laws, but there might be faults considering we have not studied the laws into detail.

The “Treatment register” is aimed at treating patients. Regulation § 6 of the Health Register Law says that registers which are aiming at treating patients may be kept electronically. The register has to show who has registered the information. This might be done by electronic signature or other secure methods. Businesses that use registers aimed at treating patients have the responsibility of the data processing. The King in council may in a regulation gives more specific decisions about registers aiming at treating patients.

Since this is probably the first time it is registered such a register aiming at treating patients we suggest that one apply to the Health Department for a research project status on this. The Data Inspectorate should be informed about the project and should be asked for approval. This is to make sure the protection of personal privacy is taken care of and to get a participant outside the health service to make sure the laws are followed.

In all treatment of patients it is important that the patients approve the use of their information. This is stated in § 5 in Health Register law. Since this is the first time such a project is done we would suggest that an approval of the inhabitants in the communities that is participating is collected.

‘The Electronic Patient Journal systems have to make sure that the professional secrecy is maintained. This is very important. [23]

7.1.3 Security

The reason we chose the use of PKI and VPN as a means of transferring the data securely is that these are both well established security measures both in the public and the private sector.

By using PKI you would get the basic security measures; *authentication, integrity, confidentiality* and *signature services*, which must be present in such a system. The downside to PKI is that you have to involve a third party, the Certificate Authority. In Norway the biggest CA is Zebsign which is fusion of Telenor and The Postal Service (Posten)

VPN makes sure that you get a secure connection between to points that are not necessary on the same network. A comparison to VPN is an expensive system of owned or leased lines that can only be used by that organization. Except that VPN is a much cheaper solution compared to leasing dedicated lines.

Scalability is also a big advantage with VPN. Using leased lines would be an ok solution if the company did not expand, but they often do. Let us say a company has two branch offices, they would then only need one line to interconnect. But if that company expanded into three branch offices they would suddenly need three lines as well, four branches would require six lines, and five would require ten lines and so forth. This would be extremely expensive in the long run and would limit the flexibility for growth. This is highly relevant to the medical offices; imagine that each medical office is a branch office in that company. It is not hard to imagine the costs to connect these offices via leased lines. This is not necessary with the use of VPN because of its scalability, you just need an internet connection and you are good to go.

7.1.4 Other conditions

This solution is designed for medical offices with an Internet connection. We have also been thinking about alternative solutions for the doctors. For instance when they are standing at a car accident and need information about a patient. We will take a look on how to solve such situations with the aid of the “Treatment register, in the section about possible additions to the system later in this chapter.

The doctors say they want a simple and easy to use solution and therefore we have tried to keep it as simple as possible. When we say we want to build on existing EPJ systems it is of course not up to us how those solutions are. But the extra module we specify should at least be as simple as possible.

The journal in the “Treatment register” should not be too large. Even tough there are good connections between the medical offices there will still be offices where it is only possible to get access too the Internet through modem, therefore large pictures and videos should not be included in the journal unless it is absolutely necessary to make a good diagnosis or too treat a patient.

7.2 Overview of the ”Treatment register” solution

You use one of the EPJ systems in use in hospitals in Norway today and upgrade it with some more functions. You have a “Treatment register”. In this register the information that is needed to make a diagnosis and give aid to a patient will be stored. This information is taken from the original patient journal in the local medical office and stored in the “Treatment register”. The EPJ system is used both on the local register and on the “Treatment register”. Then you can look on the system like this: a hospital with different departments, see fig. 18.

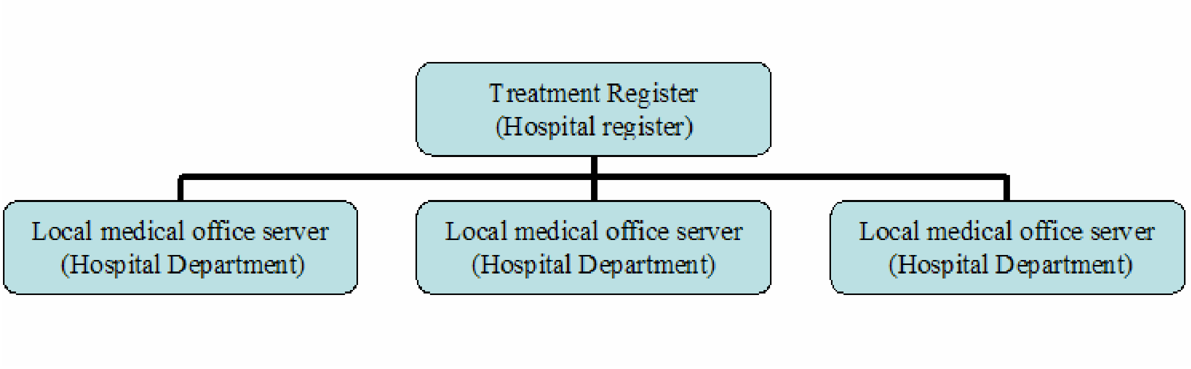


Figure 17: The connection between the "Treatment register" and the local medical offices.

The local servers send information into the "Treatment register". To get information out of the "Treatment register" you need to have access to it and there has to be done a "Decided Action". In other words, the EPJ system controls who gets access to the journal or not.

7.3 Architecture in the "Treatment register"

Here we will look on a solution to how the structure of the register could look.

7.3.1 Basic architecture

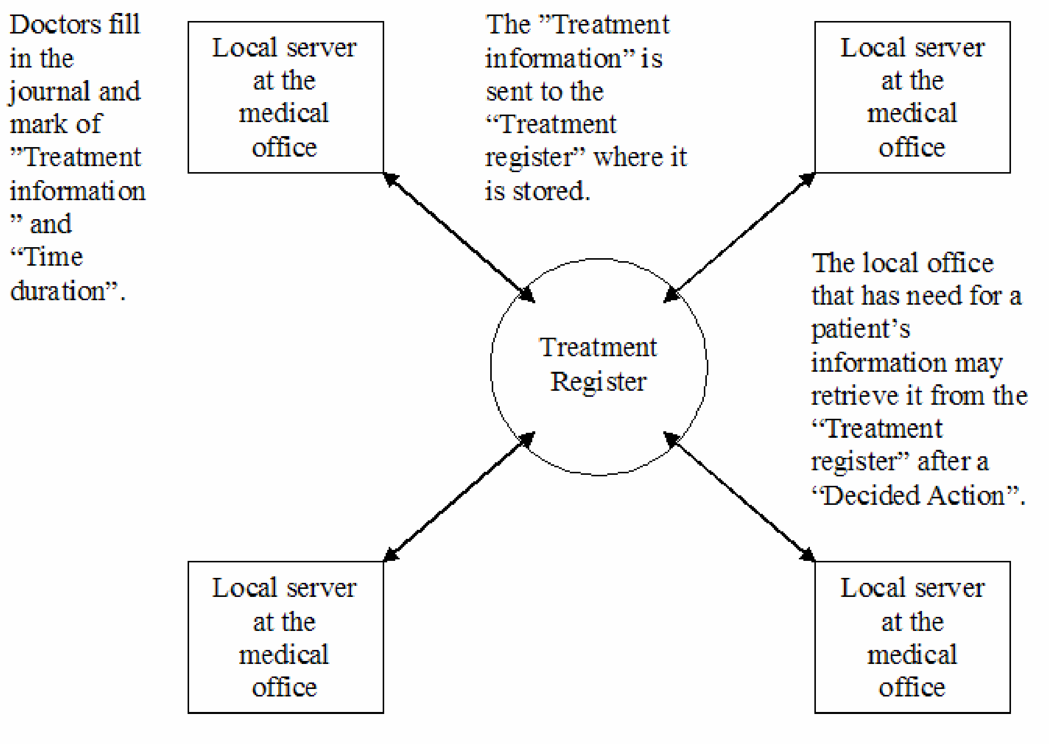

Doctors fill in the journal and mark of "Treatment information" and "Time duration".
Local server at the medical office
The "Treatment information" is sent to the "Treatment register" where it is stored.
Local server at the medical office
Treatment Register
The local office that has need for a patient's information may retrieve it from the "Treatment register" after a 'Decided Action".
Local server at the medical office
Local server at the medical office

Figure 18: How the "Treatment register" works.

Each health business shall establish their own register for patient journals, and have full responsibility for their system according to Regulation of Patient Journals § 4 (Forskrift om pasientjournal § 4). Each health business have full data processing responsibility for their own system according to the Health Register Law § 6 (Helseregisterloven § &). Each system should have their own system for access control. These have to be attended to even if it is organized a central operation on the systems.

Because of this the patient journals have to be stored in a local register and the "Treatment information" in a central register. The central register duplicates the "Treatment information" from the journals in the local register. If a patient is treated outside of local office time there has to be sent a message to the local register with update on "Treatment information" from the central register.

7.3.2 The different components in the system

Main register: The main register is where the "Treatment information" is stored. Here it is possible to access the information that is needed to treat a patient coming to a causality clinic. You have to make a "Decided Action" to access the information in this register. Look at chapter (2.3.2)

Local server: Here the Electronic Patient Journal is stored. In this server the patient journal is used as it is in the medical offices today.

"Treatment information": This is the key to the whole system. The information that should be delivered to the main register is the information that can be important for a doctor to make a better diagnosis and give health aid. We will come back to the "Treatment information" in the section about EPJ system, but we will first show why we mean that this is a possible solution.

We will look on two paragraphs in the Health Personnel Law:

§ 25. Information to co-operative personnel

> Unless the patient says you cannot, the information can be given to co-workers when this is necessary so that you can provide the proper healthcare.

§ 45. Transfer, delivery of and access to journal and journal information

> Unless the patient says you cannot, the health personnel mentioned in § 39 can give the journal or information in the journal to other people who perform healthcare after this law, when it is necessary in order to provide the proper healthcare. It shall appear from the journal that other health personnel have been given access to the journal.

From these two laws we can conclude that, information important for giving health aid, may be given to other health personnel unless the patient oppose it. [23]

7.4 EPJ system

Here we will specify how the module we would add to an EPJ system should be.

7.4.1 Components in the EPJ system

These are the different element we think the system should have.

"Treatment information": This is the information a doctor could use to make a diagnosis and give health aid to the patient. When the doctor is writing in the patient's journal, he checks off if the information that is written shall be stored in the "Treatment register". When the information in the patient journal is stored in the local register, the information that has been checked (by the use of a check box) as "Treatment information", it is sent to the "Treatment register". What information that could be classified as "Treatment information" differs alot. Maybe there should be written some specification on what kind of information should be classified, but that will have to be done together with a doctor or the Health Department.

"Time duration": This is an option where the doctor sets the time for how long this information will be in the "Treatment register". The doctor checks off, at the same time as he checks off if it is "Treatment information", for how long the information will be stored in the "Treatment register". The "Time duration" option is there because there is no use for old information, because you no longer need it in order to make a diagnosis or give health aid.

"Decided Action": To keep track of who is accessing information from journals in the "Treatment register" there has to be a "Decided Action". This is important to avoid human curiosity since the "Decided Action" is logged. This will also make it easy for the main doctor to see who has accessed the journal.

The system as whole should be easy to use. Not too complicated structure and not too many different options. This is because the doctors do not have time to get to know complicated systems. The EPJ system should provide the doctors with a system easy to use and one that saves time for them.

7.5 Securing the system

In this section we will look at the security within the Electronic Patient Journal system, both securities inside and outside the system.

7.5.1 Security within the EPJ system

The Norwegian Electronic Patient Journal standard standardizes the rules for security in Electronic Patient Journal systems. Since we are thinking about implement these changes into an Electronic Patient Journal system for hospitals we have had a look at security within one of those. We choose DIPS since this system is open source.

The system is based on events and categorizing of data instead of ordinary rules. This is important so the system can be adapted to each of the different hospital's needs. They have access control both at the function level and the data level. This makes it possible to give a restricted number of people access to a patient journal for instance based on what role they have in the system, for instance a doctor that has a day job as a main doctor and an evening job as casualty clinic doctor. When the doctor is at day job he should not have the same access as when he is on evening duty.

In DIPS there are also high logging activity based on what kind of logging activity that is wanted. There is also a solution for emergency access called “bluelightfunction” (blålysfunksjonen). This function gives access to data that normally is not accessible by that person. The use of this function has a high degree of logging.

Most security breaks are caused by human mistakes, either by losing passwords, giving it away or just making it possible for others to access data. Because of this, the doctors have to be made aware of the responsibility they have to make sure no one else can access the system.

7.5.2 Security in open networks

For communication between the client machines at the medical offices and the server(s) we think that the use of PKI and VPN is the best and most secure solution.

By using PKI you obtain 4 very important factors; authentication, integrity, confidentiality and you get signature services, in which all of them support non-repudiation to ensure that the transactions are legally valid and irrevocable (see chapter 5.3 PKI – Public Key Infrastructure for more details).

To secure the connection between the medical offices and the “Treatment register” one should use Virtual Private Network. This way the information that is sent between the medical offices and the “Treatment register” will be tunnelled so it can not be intercepted or decrypted. By using a Virtual Private Network, patient’s journals will be secure and not be available to everyone accessing the Internet.

7.6 Example

Here is an example of how we think it should be like.

A man, let us call him Patient A, is from Kviteseid and uses the local health service and is registered in the local register. The patient visits his regular doctor at 11 O’clock. He is ill and the doctor starts to give the patient medication. The doctor then writes in the patient journal what kind of medication he has given to patient A, what symptoms patient A had and the diagnostic he has given patient A. He then tags the information as “Treatment information” and set the “Time duration” in the patient journal. The journal is stored in the local register and the “Treatment information” is sent to the “Treatment register” and stored there.

At 19 O’clock patient A’s conditions is worsening. He then goes to the casualty clinic since his main doctors office time has ended. There the attending doctor makes an “Decided Action” that the patient needs help. He then looks up patient A’s journal from the “Treatment register”. He can then see what symptoms patient A had earlier, what the main doctor’s diagnostic of patient A was and what kind of medicine he has given patient A. Now that he has better access to information about the patient he has a better basis to make a decision about how to treat patient A.

7.7 Possible additions to the “Treatment register” solution in the future

Here are some additions that we would like to see in the system in the near future.

First extension for this solution would be to implement the hospitals together with the medical offices in sending information to the “Treatment register”. If this is done both the medical offices and the hospitals will at any time have the best possible information for treating patients. If the hospitals and medical offices start to co-operate with “Treatment registers” it should be possible to connect the whole of Norway together. If this is implemented all across the country you could be sure that the doctors had the best possible information available to treat you if you had become ill somewhere else than where you originally live.

In the future it will probably be the best solution that the whole journal is stored in a large central register. But until that register is allowed by law and the infrastructure in health Norway is better than it is today, this will not be possible. But we hope that in the future all patient journals will be placed in a central register.

7.7.1 Using EPJ at an accident site

We have also thought of a solution that the doctors, or ambulance drivers, can use while being at the site of an accident. We thought that the use of PDA’s or perhaps mobile phones could be used while in the “field”. With a PDA they could contact the server where the journals are stored and download the information down to the PDA. This way they would get all the updated information concerning the patient’s health record instantly, and thus know every single detail that is imperative in order to provide with the best health care possible that the circumstances would allow.

There are however some downsides in using a PDA or mobile phone. The data will be transmitted over a wireless link which is not as secure as a wired transfer. One could “easily” sniff some packet on their way down to the PDA and maybe get some information. But this data would in any case be encrypted so the person who intercepted the packets would have to know the deciphering key in order to make the data readable. But what is really the most important thing; saving a persons life or worrying about someone else seeing his journal and wait until you get to the hospital/medical office in order to know all there is about the patient.

Further more, one possible way to minimize the risk of other people “eaves dropping”, would be that the mobile instruments the doctors use had a special chip that would be verified by the cells (antennas) that the telecommunication providers use. In addition to this the equipment used would utilise a bandwidth separated from all other radio transmissions. By doing it this way it would not be as easy to get information if you are not authorized to get it. If you do not have the chip in your PDA then you do not get access, simple enough. Realising this would of course have to involve a telecommunication company such as for example Tele 2 or similar, which we doubt is not an impossible task.

One other thing that would have to be taken into consideration is what should be downloaded to the PDA. The screen on the PDA’s, or mobile phone’s for that matter, are not very big so the information would have to be as little as possible, but still enough to give the right diagnosis.

Too solve the problem with PDA’s and mobile phones, the “Treatment register” should categorize the information that is being stored in it. There could be two or three different categories, one for PDA/mobile phones and one for PC at the medical office. The profile for the latter one would contain all the information in the journal while the profile for the PDA/mobile phone would only include the most important information such as blood type, allergies, if the patient is a diabetic or not and so on. This way the information would be small enough to fit on the smaller screens of the PDA’s or the mobile phones.

8 Conclusion

In this thesis we have studied how it is possible to use Electronic Patient Journals in a Medical Office Agreement. We have studied the Electronic Patient Journal, Norwegian rules considering Electronic Patient Journals, how to transfer and store information securely and Public Key Infrastructure. We have also studied how doctors think about Electronic Patient Journals and at the end we made a specification to how we think Electronic Patient Journals could be implemented into the Medical Office Agreement.

From the questionnaire we found that the doctors are ready to start using the Electronic Patient Journal system and that they think it will help them in their work. Mostly they have all good computer knowledge and are motivated to start using it. But the systems have to be simple and should not have too many complex functions.

These systems will of course cost some money and in addition some of that money will have to be spent on courses and introductions to the systems so the doctors get a good start with the system.

Through the specification we have done, we have shown that it is possible to make a register (“Treatment register”) that obtain information, critical for diagnosis and emergency case, about patients within the Norwegian laws. There are some conditions to this register though; the most important one is that you have to ask for patient’s approval. By adding some specifications to the existing systems we think the “Treatment register” should be a good solution to how the Medical Offices Agreement can have access to necessary information about patients all the time.

By using a combination of PKI and VPN it is fully possible to transport data from two different machines on two completely different networks, for example from county A to county B. This is as secure as it can get, but is it secure enough? We would say yes. But there is always a certain risk of being hacked by unwanted intruders no matter what precautions you take. But by the use of authentication, digital signatures and the other security measures described in this thesis you minimize the chance of getting attack.

It is also important to keep up-to-date with all of the latest software and upgrade to ensure you have the most secure solution possible.

Appendix A – Abbreviations

BMJ – British Medical Journal
CA – Certificate Authority
CEN - Comitè Europèen de Normalisation
CMS – Cryptographic Message Syntax
CRL – Certificate Revocation List
DC – Digital Certificate
EPJ – Electronic Patient Journal
IPSec – IP Security
KITH – Kompetansesenter for IT i Helsevesenet
L2TP – Layer 2 Tunnelling Protocol
LAC – L2TP Access Concentrator
LNS – L2TP Network Server
MIME – Multi-Purpose Internet Mail Extension
NCS – Network Computing Spectrum
NHS – National Health Service (Great Britain)
PAS – Patient Administrative Systems
PBE – Password Based Encryption
PKCS – Public Key Cryptography Standards
PPP – Point-to-Point Protocol
PPTP – Point-to-Point Tunnelling Protocol
PRNG – Pseudo Random Number Generator
PTD – Personal Trusted Devices
PKI – Public Key Infrastructure
RA – Registration Authority
S/MIME – Secure Multi-Purpose Internet Mail Extension
SSL – Secure Socket Layer
VPN – Virtual Private Network
PDA – Personal Digital Assistant

Appendix B – References

As of 21st of May all of these links were fully functional.

[1] The Norwegian Health Departments website
http://odin.dep.no/hd/

[2] The Norwegian social- and health department's website "*Lov om helseregistre og elektronisk behandling av helseoplysninger"*
http://odin.dep.no/hd/norsk/publ/hoeringsnotater/030005-990298/index-dok000-b-n-a.html

[3] Google *"Internet Search Engine"*
http://www.google.com

[4] DIPS Homepage
http://www.dips.no/dipsnew.nsf/Display/Startside

[5] Software Innovation's DocuLive
http://www.software-innovation.no/Produkter/DocuLive.html

[6] INFOMEDIX Website
http://www.tehc.no/Support/IFOMEDIXmain.htm

[7] The British Department of Health website *"The NHS plan in full"*
http://www.doh.gov.uk/nhsplan/nhsplan.htm

[8] The British Department of Health website *"Information Policy Unit"*
http://www.doh.gov.uk/ipu/index.htm

[9] NHS Information Authority Portal Site *"ERDIP - Electronic Record Development and Implementation Programme"*
http://www.nhsia.nhs.uk/erdip/pages/default.asp

[10] RSA Security *"Public-Key Cryptography Standard"*
http://www.rsasecurity.com/rsalabs/pkcs/

[11] Arbeids og administrasjonsdepartementet *"Forskrift om elektronisk kommunikasjon med og i forvaltningen*
http://odin.dep.no/aad/norsk/regelverk/lover/002001-120011/index-dok000-b-n-a.html

[12] Arbeids og administrasjonsdepartementet *“Veiledning til forskrift om elektronisk kommunikasjon med og i forvaltningen*
http://odin.dep.no/aad/norsk/aktuelt/nyheter/002001-120010/index-dok000-b-n-a.html

[13] Datatilsynet
http://www.datatilsynet.no

[14] EPJ-Obervatoriet
http://www.epj-observatoriet.dk/

[15] Zebsign
http://www.zebsign.no

[16] CHRISTENSEN, GRØNLAND, METHLIE
Informasjonsteknologi
Strategi, Organisasjon, Styring
3. utgave • Cappelen Akademisk Forlag, 1999

[17] Kvalitetssikring av elektronisk pasientjournal i sykehus
http://kvalis.ntnu.no

[18] **A patchwork planet** ”*The heterogeneity of electronic patient record systems in hospitals”*
by Gunnar Ellingsen and Eric Monteiro
http://iris23.htu.se/proceedings/PDF/27final.PDF

[19] RFC Editor RFC 2661 *“Layer Two Tunnelling Protocol (L2TP)”*
by W. Townsley and A. Valencia from Cisco Systems
A. Rubens from Ascend Communications
G. Pall and G. Zorn from Microsoft Corporation
B. Palter from Redback Networks, August 1999
ftp://ftp.rfc-editor.org/in-notes/rfc2661.txt

[20] KITH
http://www.Kith.no

[21] Elektronisk pasientjournal standard
Arkitektur, arkivering og tilgangsstyring
Del I: Funksjonsrettet beskrivelse
http://www.kith.no/EPJ/Rapporter/EPJ-HS-del1-v1.pdf

[22] Elektronisk pasientjournal standardisering
Arkitektur, arkivering og tilgangsstyring
Del II: Tekniske spesifikasjoner
http://www.kith.no/EPJ/Rapporter/EPJ-HS-del2-v1.pdf

[23] **Norges lover**
Helseregisterloven
http://www.lovdata.no/all/nl-20010518-024.html
Helsepersonelloven
http://www.lovdata.no/all/nl-19990702-064.html
Forskrift om pasientjournal
http://www.lovdata.no/for/sf/hd/hd-20001221-1385.html

[24] PKCS #1
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html

[25] PKCS #3
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-3/index.html

[26] PKCS #5
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5/index.html

[27] PKCS #6
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-6/index.html

[28] PKCS #7
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html

[29] PKCS #8
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-8/index.html

[30] PKCS #9
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-9/index.html

[31] PKCS #10
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html

[32] PKCS #11
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html

[33] PKCS #12

http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html

[34] PKCS #13
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-13/index.html

[35] PKCS #15
http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html

[36] Survey done by Lærum, Ellingsen and Faxvaag published in ”Tidsskrift for Den norske lægeforening”
http://www.tidsskriftet.no/pls/lts/PA_LTS.Vis_Seksjon?vp_SEKS_ID=622468

[37] Survey done by Lærum, Ellingsen and Faxvaag published in British Medical Journal 8 December 2001.
http://bmj.com/cgi/content/full/323/7325/1344?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=&author1=Faxvaag&searchid=1015323593821_2174&stored_search=&FIRSTINDEX=0&resourcetype=1,2,3,4,10

[36] The PKI page
http://www.pki-page.org/