

Summary Report / Oppsummeringsrapport

Part I: International Symposium
“Information security and legal aspects
– Who cares?”

Del II: Nasjonalt miniseminar
“Tilgang på langs”
Informasjonsdeling og sammenhengende pasientforløp:
Juridiske og sikkerhetsmessige aspekter

Eva Henriksen

Eva Skipenes

Ellen K. Christiansen

Leif E. Nohr

Title: Summary report from international symposium "Information security and legal aspects – Who cares?" and from the Norwegian seminar "Tilgang på langs - Informasjonsdeling og sammenhengende pasientforløp: Juridiske og sikkerhetsmessige aspekter."

NST-report: 11-2007

Project manager: Eva Henriksen

Authors: Eva Henriksen, Eva Skipenes, Ellen K. Christiansen, Leif Erik Nohr

ISBN: 978-82-92092-89-7

Date: 2007-10-18

Number of pages: 56

Keywords: Information security. Legal issues. Sharing of patient information. Cooperation in patient treatment.

Summary: This report is a summary of two events covering legal and security aspects for cooperation and information sharing in the healthcare sector: An international symposium, in English, being held as a parallel session at the annual telemedicine conference TTeC 2007 (part I) and a national seminar, in Norwegian, arranged after the closing sessions of the conference (part II).
Each part contains summaries of the presentations, including link to the power-point presentations and, for the symposium, also the abstracts submitted by the authors. A separate conclusion section is given for each part of this report.

Publisher: Norwegian Centre for Telemedicine
University Hospital of North Norway
P.O. Box 35
N-9038 Tromsø
Telephone: (+47) 77 75 40 00
E-mail: info@telemet.no
Web: www.telemet.no

This report may be freely distributed as long as the source is stated. The user is encouraged to state the name and number of the report, that it is published by the Norwegian Centre for Telemedicine, and also that the report in its entirety is available at www.telemet.no.

Tittel: Oppsummeringsrapport fra internasjonalt symposium "Information security and legal aspects – Who cares?" og nasjonalt seminar "Tilgang på langs - Informasjonsdeling og sammenhengende pasientforløp: Juridiske og sikkerhetsmessige aspekter."

NST-rapport: 11-2007

Prosjektleder: Eva Henriksen

Forfattere: Eva Henriksen, Eva Skipenes, Ellen K. Christiansen, Leif Erik Nohr

ISBN: 978-82-92092-89-7

Dato: 18.10.2007

Antall sider: 56

Emneord: Informasjonssikkerhet. Juss. Deling av pasientinformasjon. Samhandling.

Oppsummering: Rapporten er en oppsummering av to arrangement med tema juridiske og sikkerhetsmessige aspekter ved samhandling og informasjonsdeling i helsesektoren: Et internasjonalt symposium arrangert som en parallellsesjon i den årlige telemedisinkonferansen ved Nasjonalt senter for telemedisin, TTeC 2007 (Part I), og et nasjonalt miniseminar arrangert i etterkant av konferansen (Del II).

Rapporten inneholder en oppsummering av alle innledningene og de spørsmål som kom opp i etterkant, og har link til power-point-presentasjonene. For symposiet er innsendte abstracts tatt med i sin opprinnelige form, og det gis en kort presentasjon av foredragsholderne.

Utgiver: Nasjonalt senter for telemedisin
Universitetssykehuset Nord-Norge
Postboks 35
9038 Tromsø
Telefon: 77 75 40 00
E-post: info@telemed.no
Internett: www.telemed.no

Det kan fritt kopieres fra denne rapporten hvis kilden oppgis. Brukeren oppfordres til å oppgi rapportens navn, nummer, samt at den er utgitt av Nasjonalt senter for telemedisin og at rapporten i sin helhet er tilgjengelig på www.telemed.no.

English summary

Title: Summary report from international symposium "Information security and legal aspects – Who cares?" and the Norwegian seminar "Tilgang på langs - Informasjonsdeling og sammenhengende pasientforløp: Juridiske og sikkerhetsmessige aspekter."

Abstract: An international symposium in English and a national seminar in Norwegian were arranged in connection with the annual Tromsø Telemedicine and eHealth Conference (TTeC), on 13 June 2007. The two events focused on legal and security issues related to communication and sharing of electronic health information within and between institutions and healthcare levels.

The international symposium was arranged as one of the parallel sessions (no. 16) of the TTeC 2007. An audience of approximately 40 persons attended the symposium. The national seminar was arranged after the closing session of the main conference. Approximately 60 persons attended this seminar.

This report is divided into two parts, Part I for the international symposium and Part II for the national seminar. Each part contains summaries of the presentations, including link to the power-point presentations and, for the symposium, also the abstracts submitted by the authors. A separate conclusion section is given for each part of this report.

The big dilemma is to find means to ensure individual privacy and information security in healthcare and at the same time find ways of utilising the powers and possibilities of modern information and communication technology. The presentations given at the international symposium illuminated the need for further research with respect to how Privacy Enhancing Technologies and other measures can be used.

At the national level, we see the need for solutions supporting the cooperation between the healthcare levels, focusing especially on the need for the municipalities and primary healthcare. The healthcare system at the municipality level is not as uniform as at the hospital level. In the municipalities more bodies, institutions and organisations are involved, more people are working there, and the professionals are more diverse.

Preface

The international symposium and the national seminar were arranged in connection with the annual Tromsø Telemedicine and e-health Conference (TTeC), on 13 June 2007. The focus of TTeC 2007 was practice, research and development within the field of telemedicine and e-Health in elder care.

Both the symposium and the seminar focused on legal and security issues related to communication and sharing of electronic health information within and between institutions and healthcare levels. The focus on continuity of patient care creates the need for new ways of organizing the processing of and access to patient information for health personnel in the daily patient care. On a more overall level it is important to clarify the legal framework within which these services must operate, and the security requirements and ethical challenges this entails.

The objective was to give healthcare workers, patients/citizens, health managers, ICT-managers and system providers and developers an opportunity to meet and to exchange knowledge and experience about legal and security challenges. We wanted to discuss possible solutions related to the use of electronic health record systems, electronic communication, electronic observation of patients, mobile solutions, and telemedicine in the nursing and caring sector in general.

The international symposium was arranged as one of the parallel sessions (no. 16) of the TTeC 2007, before noon on 13 June 2007. An audience of approximately 40 persons attended the symposium.

The Norwegian seminar was arranged after the closing session of the main conference, between 14:00 and 18:00 on 13 June 2007. Approximately 60 persons attended the seminar.

This summary report is divided into two parts:

- Part I (in English) summarizes the international symposium
- Part II (in Norwegian) summarizes the national seminar.

Section 2 in each part contains summaries of the presentations, including link to the power-point presentations and, for the symposium (Part I), also the abstracts submitted by the authors.

A separate conclusion section is given for each part of this report.

The Norwegian seminar was financially supported by the Norwegian Centre for Telemedicine (NST) and the local Arena for health, innovation, and technology (HIT).

The production of this summary report was financially supported by NST and the Norwegian Research Council, NFR.

We hereby wish to thank HIT, NST and NFR for their financial support which enabled us to arrange and document the symposium and the seminar.

We also wish to thank all participants – the lecturers and the audience – who contributed to make these two arrangements successful.

Tromsø, 18 October 2007

Eva Henriksen, Eva Skipenes, Ellen K. Christiansen, Leif E. Nohr

Table of Content / Innhold

Part I: International Symposium: “Information security and legal aspects – Who cares?”	9
1. Introduction	9
2. The presentations	10
2.1 Short introduction by Steinar Pedersen, NST: Who Cares?	10
2.2 Leif Erik Nohr, NST: Legal framework for patient information management – a Nordic perspective	10
2.3 Mats Hagner, Carelink, Sweden: National patient summary and security infrastructure	14
2.4 Søren Duus Østergaard, IBM, Denmark: Security and privacy in telemedicine: How can we benefit from new technology to improve healthcare and maintain privacy?	17
2.5 Asbjørn Hovstø, ITS Norway: RFID for the elderly	21
2.6 Asbjørn Hovstø, ITS Norway: NETC@RDS: from the eye-readable EHIC to the electronic EHIC	24
3. Summary / Conclusions	27
Del II: Nasjonalt miniseminar: “Tilgang på langs - Informasjonsdeling og sammenhengende pasientforløp: Juridiske og sikkerhetsmessige aspekter” 29	
1. Innledning	29
2. Presentasjonene	30
2.1 Ellen K. Christiansen, NST: Introduksjon til dagens tema	30
2.2 Leif Erik Nohr, NST: Juridiske rammer for utveksling av helseinformasjon - et nordisk overblikk	35
2.3 Hilde Jordal, SHdir: Enkel og trygg tilgjengelighet til pasientopplysninger i EPJ ved ytelse av helsehjelp – vurdering av lovendringer	35
2.4 Knut Magne Augestad, NST/UNN: Informasjonsbehov i en klinisk hverdag	38
2.5 Egil Rasmussen, Stavanger kommune: Hvordan oppnå helhet og sammenheng i eldreomsorgen/pasientbehandlingen	40
2.6 Helge Veum, Datatilsynet: Datatilsynet og tilgang på langs	43
2.7 Ivar Berge, RRHF: Min Journal - elektronisk kommunikasjon mellom pasient og spesialisthelsetjenesten	45
2.8 Jorunn Bjerkan, NTNU: Internettbasert individuell plan - en flytsone?	47
2.9 Vigdis Heimly, KITH: Samtykkebasert kjernejournal	48
3. Avsluttende diskusjon	52
4. Oppsummering og evaluering	52
4.1 Oppsummering	52
4.2 Evaluering	53
4.3 Videre arbeid	54
Abbreviations / Forkortelser	55

Part I: International Symposium: “Information security and legal aspects – Who cares?”

1. Introduction

This international symposium was arranged as one of the parallel sessions (no. 16) of the annual Tromsø Telemedicine and e-health Conference (TTeC)¹, on 13 June 2007. The call for abstracts to the symposium was separate from the call for the main conference. Some of the speakers were specially invited in order to get presentations from the other Scandinavian countries, who have achieved a lot in the areas that were focused on in the symposium.

The goal of the symposium was to focus on legal and security issues related to communication and sharing of electronic health information within and between institutions and healthcare levels. The available technological solutions are not necessarily adapted to the way the nursing and caring sector is organised. The focusing on continuity of patient care creates the need for new ways of organizing the processing of and access to patient information for health personnel in the daily patient care.

The symposium should exemplify relevant legal and security issues based on experience from projects and services worldwide, focusing on ways of avoiding or overcoming possible barriers and solving problems. On a more overall level it is important to clarify the legal framework within which these services must operate and the security requirements and ethical challenges this entails.

An audience of approximately 40 persons attended this symposium and its six presentations.

The programme for the symposium is shown below. For online readers, the title of the presentations 2-6 is a link to the power-point presentations. Links to the presentations can also be found at http://www2.telemed.no/ttec2007/presentations/session16_wednesday/

1. Short introduction: Who cares?

Steinar Pedersen, NST

2. [Legal framework for patient information management – a Nordic perspective](#)

Leif Erik Nohr, NST

3. [National patient summary and security infrastructure.](#)

Mats Hagner, Carelink, Sweden

4. [Security and privacy in telemedicine: How can we benefit from new technology to improve healthcare and maintain privacy?](#)

Søren Duus Østergaard, IBM Denmark

5. [RFID for the elderly](#)

Asbjørn Hovstø, ITS-Norway

6. [NETC@RDS: from the eye-readable EHIC to the electronic EHIC](#)

Asbjørn Hovstø, ITS-Norway

Information about the symposium was made available on the TTeC 2007 web site.²

¹ <http://www.telemed.no/ttec2007>

² <http://www.telemed.no/information-security-and-legal-aspects-who-cares.412106-75468.html>

2. The presentations

The following sub-sections give a summary of each presentation and of the questions and comments that were raised afterwards. Abstracts are included in each sub-section. For the electronic version of this document, links to the presentations are inserted in the title of each sub-section and in the first picture of the Power-Point presentation.

First, a short introduction to the problem area was given by Steinar Pedersen.

2.1 Short introduction by Steinar Pedersen, NST: Who Cares?

Steinar Pedersen is the head of the Norwegian Centre for Telemedicine and has been since the start of this centre in 1993. He is also a medical doctor (MD), and an ear-nose-throat (ENT) specialist.

When Pedersen worked as a young doctor at the university hospital of Tromsø they had a patient with a urine stone. Pedersen had to operate him. He needed to give him antibiotics and asked if he had had any allergic reactions to antibiotics earlier. The patient said he didn't think so. He also told that he had been operated earlier in Oslo. Pedersen called the hospital in Oslo but that hospital couldn't find the patient's health record. They then gave him some penicillin, and he died because of an allergic reaction.

This incidence has influenced Pedersen's attitude towards the security aspects. If the question is: "Is security important?", then his answer is: "YES: But Availability is more important." It is extremely important that information is available when needed. It is necessary to balance between security and information need.

Pedersen also asked: "Where are the nurses and the doctors?" The doctors and the nurses do not take part in the discussions of these topics. The doctors tend to mean that the security is sufficient; it is the easy part of their work. What is difficult is to operate, to do the surgery.

2.2 Leif Erik Nohr, NST: [Legal framework for patient information management – a Nordic perspective](#)

Leif Erik Nohr has worked as a legal advisor at Norwegian Centre for Telemedicine for nine years. He is participating in several international projects and organisations.

Abstract

Legal framework for patient information management – a Nordic perspective

Nohr, LE. Norwegian Centre for Telemedicine

The legal systems in Denmark, Sweden, Finland and Norway have many similarities and there is a long tradition for cross border mobility of both health professionals and patients. The health structures of the Nordic countries are comparable and they all consider healthcare as a main pillar in the respective welfare states. The countries face many of the same challenges with lifestyle related diseases and an increasing population of elderly. Furthermore, all the Nordic Countries have been using electronic health records for many years and all countries are quite advanced within different aspects of e-Health.

All countries realise the potential of utilizing modern information- and communication technologies to provide better and more effective healthcare, to empower patients, to educate professionals, etc. We see a number of national initiatives in the Nordic Region to further develop e-Health, and they all address and discuss legal aspects and challenges of implementation of different e-Health solutions.

In practical use and implementation of relevant legislation, we see that there are differences between the countries. The legal framework might look similar, but there are important differences when it comes to how use of information and communication technology is

interpreted within the framework. Differences are seen both with regards to health legislation and regulations on processing of information.

This presentation will give a brief overview of the legal frameworks in the Nordic Countries and how this framework affects use and development of e-Health solutions. The presentation will also point at some of the discussions going on within the Nordic Region about legal challenges of e-Health and show examples of new legislation that is being suggested in some of the countries.

A summary of the presentation



The Nordic Healthcare systems have some common features:

- Public provision of healthcare is the basis in all countries and high quality healthcare is considered a fundamental part of the welfare state. An increasing amount of money is put into healthcare on all levels.
- Healthcare is governed by quite “massive” and strict legislation
 - Aimed at protecting money, professions, institutions and patients
- Patients’ Rights are guaranteed in all countries.
- The use of information technology in the Nordic countries is increasing and this includes the use of IC technologies in healthcare. Telemedicine and e-health services are relatively highly developed.
- E-health strategies are in force or in the making
- All countries have an infrastructure in place. Dedicated healthcare networks
- The Nordic countries face the same demographic challenges, where lifestyle related diseases and more elderly people are key factors.
- Focus on more continuous provision of healthcare, patient centred healthcare and care given as close to the patients as possible.

In the Nordic region the main challenge is to find ways of fully utilizing the potentials of information technology in healthcare without jeopardizing the legal rights of patients, confidentiality, treatment, etc. With regards to legal issues, the challenge is to provide a framework that takes quality, patients’ rights, professional duties, efficiency requirements and security requirements into account. At the same time information technology must be effective and useful in order to contribute to good and better care for patients.

Important information about the status of work on e-health within the Nordic countries can be found in these two reports:

- “E-health priorities and strategies in European countries”, e-Health ERA report, March 2007³
- “E-helse over landegrensene i Norden – muligheter og barrierer”, Rapport fra Nordisk samarbeidsforum for telemedisin, Nordisk Ministerråd, 2007 (In Norwegian)⁴

This presentation is to a large extent based on these reports.

Iceland



Iceland has in action a national strategy for the use of information in all public sectors, including healthcare. Core principles in this strategy are information security and protection of personal privacy.

With regards to e-health and telemedicine, these areas are regulated by existing legislation on healthcare and data protection. No specific e-health legislation is in force.

Some years ago, the DeCode case and the legislation passed in connection with this, caused a lot of debate and discussion about personal privacy, medical records and information security. According to our information, a number of circumstances have led to today's situation where neither the legislation nor the database is in use.

Finland



Finland has a healthcare system that is to a large extent decentralised and publicly funded. E-health and telemedicine services are highly developed and to some extent integrated in the overall provision of healthcare. Unlike many other countries, Finland has not established a dedicated national healthcare network. The focus has instead been on using secure commercial communication channels such as VPN.

Finland had their first strategy on utilising information technology in (i.a.) healthcare in 1996. Since then, work on development and implementation of such technologies have been built around a principle of citizen-centred, seamless service structures.

Temporary legislation on seamless service structures were passed in 2000, followed by work on preparing permanent legislation. Electronic health records are widely used in Finland. In addition, Finland is in the process of implementing a national e-prescription system with corresponding legislation being prepared. A national citizen's health portal will be launched in 2007.

In the near future a digital archive for patient documentation will be established with corresponding standards and legislation. All healthcare organisations will be obliged by law to join the national IT architecture for health, and the system will be fully implemented by the end of 2011.

Sweden



Sweden has had a national e-health strategy in force since 2006. The strategy also includes social care. The work with this strategy also aims at bringing laws and regulations in line with extended use of information and communication technologies. Sweden has a highly developed infrastructure with a dedicated national healthcare network.

³ http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

⁴ <http://www.norden.org/pub/sk/showpub.asp?pubnr=2007:709>

From a legal perspective it is very interesting that the Swedish authorities have started to work on a completely new and comprehensive legislation that will encompass all processing of personal patient information – The Patient Data Act (Patientdatalagen). The new act will be in the form of framework legislation with room for more detailed regulation on specific topics. Furthermore, the act will aim at providing both enhanced patient (information) security and strong privacy protection. Subject to specific conditions, care-providers can be given direct access to other's electronic records. Patients get a right to be informed about who has accessed their own medical records and they will be given the possibility to have direct access to their own records.

To summarize:

- National strategy since 2006 – includes social care
- Aim at bringing laws and regulations in line with extended use of ICT
- Information and infrastructure
- The new patient data act – a framework legislation with room for legislation at a more detailed level
- Strong security requirements
- Care providers – subject to conditions - can have access to other medical records
- Patients should have access to their own records

Denmark



Despite the notion that Denmark is the more liberal of the Nordic countries, also when it comes to information technology, information processing and healthcare, Denmark face many of the same challenges as the other countries do. Technology, organizations, legislation, etc. are important issues in Denmark as everywhere else. To some extent, however, Denmark seems to interpret legislation on data protection somewhat more liberal than (e.g.) Norway, leading to a more rapid development of some e-health services. But a lot of work is done in Denmark to analyse and develop the legal framework for telemedicine and e-health.

A number of initiatives in the strategy will over a very short period of time challenge some of the regulations in the Law on Patients' Legal Status. For instance, it will be imperative to clarify whether the existing legislation presents any barriers to displaying information originating from various registries, with the purpose of giving the health care professional a more holistic view of a patient's state of health.⁵

Denmark has a government strategy for information technology and healthcare (2003 – 2007). This strategy has, among other things, focused a lot on interoperability and standards. Denmark is in the process of implementing SnoMed⁶ as a common standard for terminology used in electronic health records.

According to the mentioned strategy, the goal is to implement a system in Denmark where each patient has only one health record within each region.

Health authorities in Denmark have done a lot to develop legal guidelines on issues like information security and consent.

⁵ National IT Strategy 2003 – 2007 for the Danish Health Care Service

⁶ <http://www.snomed.org/>

Norway



The Norwegian Health Ministry has issued its third strategic initiative Te@mwork 2007⁷ which is giving guidance on special focus areas for the use of information technology in healthcare. The government is also funding specific projects under this strategic initiative.

Continuity of care on all levels is one important goal in the strategic initiative, paving way for further development of cooperation between healthcare providers on all levels. In this kind of cooperation there is obviously a need for sharing of information and this is where use of information technology can help. Electronic health records are common in Norway – at all levels.

Norway has had regional health networks for some years and these are now merged into one national network.

There has been done a lot of work in Norway on legal aspects of telemedicine and e-health. In 2001 the Ministry issued guidelines on telemedicine and responsibility and in 2007 guidelines on access to and sharing of electronic health records. Telemedicine and e-health is provided under already existing legislation. The parliament has passed the Act on personal health data filing systems and the processing of personal health data (in Norwegian: Helseregisterloven)⁸ which gives specific regulation on processing of health data in accordance with health regulation and regulation on privacy and information processing.

Under existing Norwegian legislation there are limited possibilities for direct, electronic access to health records. From the outside of a healthcare institution such access is in practice prohibited. This legislation (or this interpretation of legislation) is currently under heavy debate in Norway, and it is reason to believe that the authorities will open up for more access possibilities in the near future.

Conclusions

All the Nordic countries have good and determined national strategies on e-health and/or telemedicine. They have good intentions and seem to put power behind them in terms of money and governmental interest in development of organisations, institutions and the legal frameworks. Not surprisingly, there is a strong focus on infrastructure in most of the Nordic countries, but there are significant differences when it comes to solutions. We see some examples now of cross-border healthcare initiatives that tries to utilize information technology possibilities.

Another common trend is that the Electronic health record (EHR) is changing. Instead of being looked at as an electronic version of the paper record, modern EHR systems are considered as more comprehensive information systems with new and better possibilities as tools in the provision of continuous healthcare. Modern EHR systems give new possibilities when it comes to sharing of information and instant access to updated information whenever and wherever needed. The challenges that these possibilities represent also in terms of legislation is widely acknowledged in all the Nordic countries, and serious work is done to develop and rethink the legal frameworks to a new – electronic – reality.

2.3 Mats Hagner, Carelink, Sweden: [National patient summary and security infrastructure](#)

Mats Hagner holds a Master degree in Engineering Physics. He has worked in the healthcare sector since 2003 and at Carelink since august 2006. Previously he has worked

⁷ http://www.shdir.no/vp/multimedia/archive/00002/Te_mwork_2007_May_200_2717a.pdf

⁸ <http://www.ub.uio.no/ujur/ulovdata/lov-20010518-024-eng.pdf>

many years as consultant, mostly in telecom. He is currently working as project manager at Carelink, managing the BIF-project: a national patient data security project which is the subject for the presentation

Abstract

National Patient Summary and Security Infrastructure

Leach E; Hagner M; Carelink, Sweden

1. National Patient Summary (NPÖ)

Currently in progress under Carelink's auspices is the National Patient Summary project, a national service for locating and accessing health record data and other healthcare records no matter where the information has been registered. This information includes details of diagnoses, examinations and treatment carried out. Authorised care personnel will have personal access to the patient summary subject to informed consent from the patient or her or his family. In due course, patients will themselves be able to access information about their own cases.

2. Basic services for information supply (BIF)

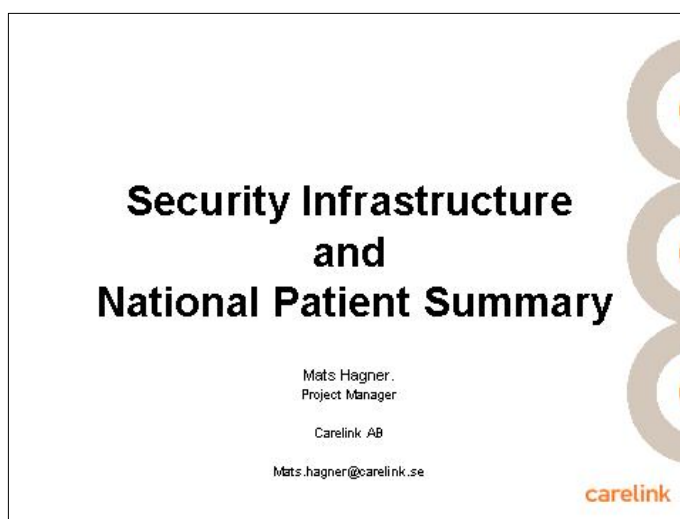
Healthcare is progressively becoming a process involving several healthcare providers, all contributing in their way to the healthcare of the patient, and healthcare is provided by both private and public organisations with an ever greater involvement from the private sector.

The patient's status is becoming more important which increases his/her demand for influence and access to healthcare records at anytime and anywhere.

Modern information and communication technology makes it possible to support this process while maintaining security and quality at high levels.

BIF (Basic services for information supply) is a security framework for national health applications that ensures integrity, confidentiality and patient security. It gives a unified way of handling central security issues like Single-Sign-On, access control, patient/care-professional, consent and logging. The user will also be able to access all relevant healthcare information with just one login.

A summary of the presentation



1. BIP (BIF)

The Swedish National Strategy for e-Health states that "an important current development is the removal of individual functions from a large number of e-Health solutions and the development of general or national common solutions".

BIP (Basic services for information provision) (BIF in Swedish) is first and foremost intended to be used between institutions, but could also be useful within large organisations. The

vision is to achieve a unified way to handle patient data with full information security within and between organisations. The work is governed by the new Patient Data Act, and regulations from the National board on health and welfare and the Data inspection board.

Each healthcare principal is responsible for controlling access to patient data. Prerequisites for access to patient data are:

- Securely identified user:
 - eID + healthcare certificate for healthcare personnel
 - eID for patients
- Need for patient data
- Engagement in care activity
- Consent from the patient
- Log – follow up

The current security solutions are characterized by:

- Users in many systems
- Heavy administration
- Non-dynamic

Service oriented architecture (SOA) is used to enable information exchange between separated services in a standardized, secure and controlled manner.

BIP is based on web services for

- authentication
- access control – attribute based access control (ABAC) – set of rules
- consent

The solution is based on OASIS-standards as XACML and SAML. It builds on the national security solutions SITHS, and is specified in a national “standard”. It is developed in cooperation with the IT industry. The first official version of the technical specifications will be ready by the end of June 2007. They will be put on the Carelink web pages.

The access decisions are made locally by each county council or each institution. They allow for different rules in different counties.

Example of a rule for patient data access was shown, as well as an illustration of the steps involved in an authentication and access control situation.

Summary of BIP:

- Uses Service Oriented Architecture (SOA)
- Uses strong authentication – PKI
- Has attribute based access control (ABAC)
- Procurement process starts in June 2007
- Planning to start implementation in one year from now on

2. Swedish National Patient Summary

The Swedish National Patient Summary is a summary of important patient information, like warnings, medication, lab tests, etc.

In the first phase it will only have a viewing functionality: find information and view it (i.e. no update). It could be integrated into care applications or used via separate clients.

Some basic conditions for the National Patient Summary: The Swedish healthcare sector has decentralized healthcare and decision rights, highly diversified IT systems, and a high level of computer literacy.

The reason behind a national health record is a need for interoperability and access to patient data:

- The patients have an increased wish to manage their own healthcare and care processes, and there is increased internet literacy among patients.

- Regional use: There is an exchange of patients between county councils and municipalities. A national health summary record is highly demanded from municipalities and it is a great demand from the regions, “the biggest benefit”
- Increased mobility between regions and nations, with healthcare guarantees and healthcare clusters
- Enhanced efficiency and healthcare quality with enhanced security, improved decision support and processes, reduced administration and testing costs, and improved clinical outcomes

By this project they do not want to change existing systems. Data will not be moved or copied into a central national database; instead, a distributed solution will be made where the local data repositories are kept on the network rim. The solution will extract information from the local systems. This will result in:

- Less legal and no ownership issues
- High scalability and performance
- No single-point-of-failure
- Fast implementation

The implementation is based on industrial solutions. This will result in reduced costs, reduced risks (will not become test bed for new technology), improved stability, continuous improvements with reduced R&D costs, and faster and simpler implementation. This enables them to focus on *using* the solution to improve quality and clinical results.

Key success factors are:

- Listen to the healthcare workers
- Don't reinvent the wheel – build on what others have done
- Coordinate with existing infrastructure, like security infrastructure
- Develop it stepwise instead of going for the big bang

Questions/comments from the audience

It was asked from the audience how they get rid of old information in the system, what they do to prevent an unlimited size of the database. The answer was that the database contains only a limited set of information, i.e. only the latest updated information.

Hagner pointed out that, for the moment, they do not plan to use this data for research purposes.

Another comment from the audience was that in Norway one of the difficult issues is to grant access in the cases where different bodies cooperate in following-up the patient. Hagner responded that in their system they only have possibility for giving access between different parts of the healthcare sector.

2.4 Søren Duus Østergaard, IBM, Denmark: [Security and privacy in telemedicine: How can we benefit from new technology to improve healthcare and maintain privacy?](#)

Søren Duus Østergaard has since 1970 worked in a number of management positions in IBM. He holds an MA in economics and is a member of the Danish Technology Council advising Government and Parliament in Denmark about technological issues. Since 1997 he has worked as a senior e-Government Advisor, responsible for business development with Government and Healthcare.

Among other topics he has worked since 1980 with secure infrastructure, security and privacy related issues, Public Key Infrastructure, antiterrorist tools and cross-border management solutions.

He is an external censor at the Copenhagen Business School and the IT University of Copenhagen in topics ranging from e-Business, Philosophy, Information Economics, and

Enterprise Architecture. He is a member of the advisory council of PRISE – Privacy & Security, an EU funded cooperation between four Technology Assessment organisations in Europe focusing on how to combine security and privacy issues in e-Government solutions in Europe.

Abstract

SECURITY AND PRIVACY IN TELEMEDICINE. How can we benefit from new Technology to improve Healthcare and maintain Privacy?

Duus Østergaard, Søren. Senior e-Government advisor, IBM-Europe, Denmark

New Technology is rapidly moving into home care and healthcare. Greatly helped by the combination of the demographic development that will increase the number of elderly persons over 65 dramatically in all European countries over the next few years, the lack of 'warm hands', social and healthcare workers providing service to people living in their own homes or in nursing homes – and the development of cheap, reliant sensors able to measure health and condition in numerous ways.

In the European Union's 7th framework program, Challenge 5 is directly aiming at boosting this development with a particular focus on making elderly and/or chronically ill persons living in their own homes able to master their own conditions.

But applied Telemedicine means that the entire value chain of service provisioning will be changed: Instead of family doctors keeping patient records in their drawers containing results of infrequent observations, monitoring can be around the clock, data on everything from heart beat, toilet visits, water consumption, physical activity, direct mapping of the clients location combined with detailed medical data on drug consumption, blood sugar etc. are collected, analyzed and stored electronically. Also the use of interactive video can provide a lot of users with direct connection to doctors as well as neighbours and relatives – plus, as a security measure – a direct link to police stations to watch doors for intruders.

All of this introduces new and intelligent ways to secure the condition of the individual and at the same time opens up the possibility for the following recipients of data:

- The client him/herself will need assurance under normal conditions and easy-to-understand guidelines if situation changes and are becoming less stable
- The social worker/case worker will be notified if assistance is required – administering drugs, checking of minor abnormal conditions
- The doctor will need to be alerted if major out-of-line changes occur, and in this case also rescuing services and/or a combination of home nurses and social workers will get involved and data shared in order to ensure the right treatment.
- Maybe the doctor wants a second opinion and will share the patient data with other specialists, maybe even in other countries
- Relatives and neighbours might be alerted/involved, if client has consented, and in some parts of Europe this will make up for the lack of social workers, typically deployed in the Nordic European countries.

The value chain illustrates that more and more tasks which we today will label as 'specialized' are moved down the value chain to lesser educated staff and in the end to the client him/herself. This raises a number of practical as well as legal questions:

Which types of data are we collecting?

What is the legal framework for protecting, using, sharing and exporting these data?

Can any of these types of data be used to directly discredit the client? (Sexual activity, alcohol habits, drugs?)

How can we create a role based ICT security model securing that only relevant staff gets access to patient data?

How can we define guidelines and policies that can be directly supported by ICT systems to enforce privacy legislation and in accordance with the European Directive on Data Protection?

How can we implement a flexible system that is also capable of handling situations where consent from client may not be possible to obtain?

What are the Privacy Enhancing Technologies that can help combine establishing a fine graded health safety net under the clients and meet the legal and moral requirements for data protection?

During the presentation I intend to cover the following issues:

- Trends in Telemedicine – the new value chain – Practical cases - and a couple of future scenarios
- The European Data Protection Directive and related legislation
- Role based security infrastructure – does it meet the requirements? What are the organizational implications?
- Personal identification and biometrics solutions
- Privacy Enhancing Technologies – are they applicable?
- Citizen views on privacy issues – based on work from the PRISE consortium

The dilemma is clearly between providing safe environments, easy-to-use measurement and feedback systems that can be understood and accepted by elderly people, and maintaining the high standard of personal integrity by applying optimal security and data protection measures. The presentation intends to give a few practical examples and underlines that solutions can only be found in a combination of legal, administrative and technical measures.

A summary of the presentation



The PRISE project, an EU funded cooperation between four technology assessment organisations in Europe, will develop criteria and guidelines for privacy and security research and technology development in FP7 (as a preparatory work for FP7). The project will also create some scenarios to present different security technologies and test these in different European countries.

Two telemedicine projects from Denmark were presented: The ElderTech project and the ECHO project.

The e-health landscape in Denmark is now changing dramatically. The municipalities become the owners of all the health record databases. The regions are only responsible for repairs. Hospitals become “the repair shops”...

1. The ElderTech project

This is a cooperation between IBM, the City of Aarhus and the Aarhus University to develop user-centred design principles and sample solutions for elder care. The idea is

that the patient will act as an integration point for the information. The patient is given the control.

The data is viewed in different ways by the different actors, e.g. by having different portals for the citizen/patient and for the care provider.

The project takes into account that it is not only medical data – a holistic view. The service will have to cover also safety and security and other aspects, e.g. support an intruder alarm.

2. The ECHO Target group

This is a part of an FP7 Challenge 5 project (IP), targeting elderly people with chronic diseases living in their own homes.

The project is developing a common platform that is to be tested by different cultures, i.e. in several regions in different countries. The privacy and security issues that are necessary to take into account will be addressed.

Duus Østergaard then discussed dilemmas related to security and privacy in telemedicine.

What do we understand by privacy?

- privacy as confidentiality?
- privacy as anonymity?
- privacy of identity? (separate from 'public role')
- privacy as self-determination – non-interference in own actions
- freedom to be left (completely?) alone
- privacy as control of personal data?

Where are the dilemmas?

- feeling safe – revealing all activities
- critical illness – who should know?
- continuous monitoring – false alarms
- automatic feedback – misinterpretation?
- correlation between measurements – quality of staff, quality of decisions?
- shared care – shared data (needed information when treating the patients)
- individualized care – 'Deep knowledge'
- legal requirements – research possibilities

Telemedicine trends:

A trusted health data network is important. The Danish health portal (sundhed.dk) is “down the road” to shared patient information in Denmark. It utilizes role based access and is secured by digital signatures, in addition to extensive logging of access and changes. By use of eID, every patient in Denmark can view his/her own information.

There are a lot of actors in telemedicine who need to follow the regulations.

IBM's Security Lab in Zurich has worked on the security of data elements in data records. This has been taken further by the IBM Almaden Lab (USA) with their “Hippocratic Database solution”, complying with HIPAA and its challenges. Important features are:

- formulation of policy filters to protect against unauthorised access to data elements
- user interface
- an interface that makes it compatible with any database
- role based access control can only protect data at the database record level, not at cell level

Medical centres have a wealth of information that can be leveraged to drive breakthroughs and deliver innovation in healthcare. However, data sensitivity, the fragmentation of records, and complexity in retrieving the same, have inhibited advances in this area. In order to open up this area to researchers, the Academic medical centre (AMC) in Amsterdam has set up a framework that addresses problems outlined, mitigates risks for practitioners and patients, and enables medical innovation to proceed.

Issues addressed by AMC's solution;

- Data integration through WebSphere Information Integrator (WSII)
- Disclosure control through Hippocratic database technology
- User interface to facilitate querying provided by Data Discovery and Query Builder

System benefits include efficient data management and privacy and security issues being enforced by the system. There is a need for intelligent systems that can analyse the data and select the important information.

Legal requirements and growing demand for personal data was also discussed in this presentation.

- Technology & tools
This involves aspects from SW development tools and techniques, SOA and federated security, to identity management, role based access, and privacy/policy management. More than 60 % is organization and procedures
- Regulatory compliance
Software systems should comply with privacy legislation like HIPAA, SOX, EU Data Protection Directive, etc., and with process standardization and improvement initiatives like ISO 9000, COBIT, ITIL, CMMI or 6-Sigma.
Legislation always reflects current understanding and ethical trade-off.
- Consumerism and pervasive medicine
There is a growing pressure for individualized information management and efficiency. Handheld and wireless devices are taking medical practice beyond hospital and clinical walls.
- Meeting the rising costs of more patients and less service manpower
The result of this will be a need to mitigate tasks from highly educated to normal care personnel with no clinical training. In addition, there will be an increasing need to include relatives and neighbours in the service chain, and to press for self management. A holistic approach does not only cover health and wellness but also safety and security.

Finally the following principles for data governance in telemedicine were recommended:

- Identity management based on qualified digital signatures
- Documented policies
- Fine grained access control: Identity – Role – Policy
- Logging and auditing of all access by policy

Legislation is focusing on "registries of data". Many countries need to revisit legislation on 'registers'. We need access to a variety of data sources to optimize treatment and reduce cost.

2.5 Asbjørn Hovstø, ITS Norway: [RFID for the elderly](#)

Asbjørn Hovstø has had several positions related to healthcare. He has been:

- Manager for ICT Operations in the Norwegian Institute for Public Health
- Secretary for European EDIFACT Group for Healthcare
- Project manager for Smartcard for Pregnancy

Now he works as project manager and expert in Security for ITS-Norway as responsible for the European project BioHealth. He also works for Standards Norway in different ICT projects in security and eHealth.

Abstract

RFID FOR THE ELDERLY

Hildebrand, Claudia^a; Hovstø, Asbjørn^b; Hans Demsk^a, Tomáš Trpišovský^c

^a GSF – National Research Centre for Environment and Health, Neuherberg, Germany

^b ITS-Norway - Norwegian Association for Multi-modal Transport Services, Rykkinn, Norway

^c IMA-Institut mikroelektronických aplikací s.r.o. (IMA), Praha, Czech Republic

Radio Frequency Identification (RFID) tags are frequently used for tracking. Virtually everything – from library books to heavy weight vehicles – can be followed up. A fairly new application is the use of RFID technology in healthcare.

RFID offers a large potential for improving healthcare for the elderly. As every item of interest can be tagged, the citizen's daily routine can be followed up from "outside" by caregivers or family. These can intervene if, for example, the person did not take his/her medication. Any change in the daily routine which may indicate the onset of a serious problem can be taken care of. The use of RFID may also increase the patients' safety in assuming the correct drug in the correct quantity as prescribed by the medical staff. Even by means of single-item tagging and temperature-enabled RFID tags, which ensure the integrity of the drug (e.g. that the drug has not been exposed to temperature higher than allowed). Moreover basic functions like lightning of rooms can be automated in order to support the inhabitant. This means that an elderly person can live at home longer. Whether the elderly will accept this kind of "virtual control" remains to be seen.

Privacy concerns persist to be a major obstacle to the wider spread use of RFID in healthcare. Persons and their habits can be identified via linkage and analysis of datasets collected from RFID-tags that are associated to him/her. This makes data protection a necessity. The German data protection law (§ 3 Abs.1 BDSG), for example, states that person-related data can only be collected and handled if the person has granted permission or by order of court. Until patients' privacy can be ensured, the use of RFID in healthcare remains a sensible subject.

Without a wide perception of RFID technology as sufficiently safe and secure all the achievable benefits will be useless. BioHealth, a European project on security related standardisation in healthcare, aims to stir the discussion on the ethical, legal and privacy implications of the technology including the possible prevention of tagging misuses. Particular attention will be paid to involving the stakeholders in the discussion and communicating issues of general interest to the public. The BioHealth website⁹ provides information on the benefits as well as limitations and threats in order to enable a proper use of RFID tags.

The mobility of the citizen asks for European inter-operable solutions. These require – besides European legal solutions – technical interoperability based on standards. RFID Standardisation activities in Europe are managed by Task Group 34 (TG 34) of the European Telecommunications Standards Institute (ETSI) and, at the ISO level by JTC1 / SC31 / WG2. Information thereof will also be made available at the a.m. website.

⁹ <http://mirc.gsf.de/biohealth>

A summary of the presentation



BioHealth is a project within the Europe INNOVA program for applied research. A main focus of the project is applied security.

IT solutions for the healthcare sector must fulfil a number of additional requirements (source: US Institute of Medicine). They must be safe, effective, patient-centric, just-in-time, efficient, and equitable.

The use case utilized in the project is use of RFID applications in a Czech military hospital. The employees' data for ID are used for attendance control, access control and payment in the restaurant, the canteen, vending machines, etc. RFID technology is used for tracking personnel, patients, and equipment/supply. The purpose is to enable data – usually on the identity of an object – to be transmitted wirelessly using radio waves.

There are different kinds of RFID tags:

- passive tags – small and inexpensive, external power supply
- active tags – larger, battery powered, writeable
- NFC tags – near-field communication – safe two-way interactions via wireless communication limited to literally touching distance – the new way

RFID can be used for improving the care and to make it safer for patients to stay at home. Any change of daily routine may indicate the onset of a serious problem.

A project from the 6th framework started last autumn, Cognow, which addresses some of these issues.

Privacy concerns related to use of RFID:

- Are we collecting and using personally identifiable information for other purposes without knowledge?
- Is there a lack of transparency?
- Could there be an abuse of data, because data is captured by someone?
- Could the use of RFID result in excessive aggregation of data?

It is necessary to secure RFID data by encryption and by transmission protocols. The user should also be allowed to de-activate the tag when wanted.

Questions/comments from the audience

As response to a direct question Hovstø confirmed that this technology could communicate with a PC at the patient's bed.

The use of RFID in the food stores was commented: The groceries use more money on technology than the hospitals. In groceries, privacy is not an aspect, it is just used to check

which food has arrived or left the store. We need someone to control the security in the hospitals.

Another comment from the audience was that some people say that we start using this technology too early, to which Hovstø responded that this is why it has to be tested out in real case studies.

2.6 Asbjørn Hovstø, ITS Norway: [NETC@RDS: from the eye-readable EHIC to the electronic EHIC](#)

About **Asbjørn Hovstø** – see section 2.1.5 above.

Abstract

NETC@RDS: from the eye-readable EHIC to the electronic EHIC

NADER Noel, SESAM-VITALE EIG, Le Mans, France

During the Spring 2003 European Council in Barcelona, the Member-States and the EFTA countries decided on the introduction of the European Health Insurance Card (EHIC) after 1st June 2004. Now in 2007, the EHIC – “another piece of Europe in your pocket” – has reached complete potential coverage of the 450 Million European citizens, serving as legal proof of entitlement for cross border access to non-planned healthcare.

Currently the EHIC is an eye-readable plastic- or even paper-card with only some administrative visual information on it. A strong political will supports efforts to introduce an electronic EHIC, which shall pave the way for more efficient access procedure and post-processing of administrative and reimbursement data to achieve financial benefits, trigger IT-modernisation and ensure basic interoperability between health telematic infrastructures of member states.

It is accepted common sense that the electronification of the EHIC will not happen by the simple introduction of a new chip card, but by parallel coexistence of various carriers and distribution means. The electronic EHIC in a process view consists of data capture and verification of entitlements rights. Especially the verification of entitlements rights is viewed as a high priority by many social security organisations throughout Europe, because the visual EHIC bears no security features. Efforts to introduce the electronic EHIC are formally coordinated within the Technical Commission of the Administrative Commission for Mobility of Migrant Workers (CASSTM), situated at DG Employment.

Since September 2002, the NETC@RDS Consortium has developed and tested practical solution implementations for the e-EHIC in pilot regions of 10 Member-States (namely: Austria, Czech Republic, Finland, France, Greece, Hungary, Germany, Italy (Regions of Lombardy and Venice), Slovak Republic, and Slovenia). Today NETC@RDS is a growing Pan-European Consortium initiative representing statutory partners acting on behalf of healthcare authorities from 13 of the 27 Member-States and two EFTA countries (Lichtenstein and Norway) willing to introduce an electronic EHIC that is accepted in specific service sites. It mirrors the overall European situation with having both card-issuing and non card-issuing nations involved.

In practical terms the cross border reading of health insurance chip cards and online verification of both national health insurance cards and the visual EHIC has been implemented. The established online verification infrastructure for cards or entitlement rights is the first real pan-European interconnection of different member states in the eHealth sector. Potential benefits of this approach include the future transmission of medical data as well, since the secure infrastructure is capable of extending to other services. The central positioning of the project is to serve as an experimental test bed for the electronification of the EHIC, which results are then proposed for consideration for European regulatory bodies.

This activity was sponsored in three subsequent market evaluation projects (A-1, A-2, and A-3) by the European Commission, DG INFSO e-TEN Programme. An Investment Plan including a costs/benefits assessment and risk analysis was delivered to the Commission by fall 2006 – together with technical recommendations, a comprehensive draft legal framework

for the e-EHIC, and an evaluation report on the pilots – as part of the Phase A1, A2, and A3 Market Validation project deliverables.

The proposal successfully submitted by the NETC@RDS partners in response to the e-TEN Call 2006/1 is intending to move the electronic services based on the EHIC dataset from the Service Validation Phase A (already completed), forward to the Initial Deployment Phase B. This deployment will enable European wide healthcare access for citizens based on the accepted available evidence of entitlement which can be an eye readable EHIC, a national health insurance electronic card, or indeed any other nationally adopted physical or electronic medium.

A practical benefit for mobile citizens will be the broader range of permissible access tokens and procedures in pilot sites: in many cases when the visual EHIC is not available, benefits in kinds can be granted upon e.g. a domestic health insurance card. The number of pilot sites will be increased to 305 healthcare providers offering the NETC@RDS services. Highly available online verification servers will be set up in all participating nations, with a legal framework in place to regulate the terms and condition of delivery and acceptance of entitlement data set. The initial deployment activity will be accompanied by an evaluation of the services and dissemination of project results to foster the further extension of the solution and future anchoring into European legislation.

The specific objective of the project to involve as many partners as possible, including those from “the not-yet NETC@RDS Member States” to reach a critical mass has been successfully accomplished by the gradual increase of the project consortium from initially 4 nations in 2002 to now more than 15. The sustainability of the efforts is underlined by participation of major social security organisations and governmental backing. Potential European funding and by herewith documented formal support by the European Commission shall enable the NETC@RDS consortium and its participating social security organisations to deploy the e-EHIC solution in a sustained manner.

A summary of the presentation



NETC@RDS is a project in the e-TEN programme with a budget of 20 M€ The project has 28 partners from 16 European countries.

Phase A of the project is finished. Phase B (initial deployment) started June 11 2007. (Kick-off this week in Tromsø).

New infrastructure is being built up in Europe to foster mobility and skills inside EU with common rules for social protection (the European Health Insurance Card - EHIC). Minimum requirements: eye-readable card (a temporary solution), while we wait for chip cards (the electronic version).

The NETC@RDS project's challenge is to demonstrate the potential of the same service for all EU/EFTA citizens based on different but interoperable national/regional IT infrastructure.

An electronic European Health insurance card (e-EHIC) is a digital process with the result of a trustworthy data set for entitlement at the healthcare provider. It can also be used for associated inter-state back office e-billing reconciliations.

Thus, the introduction of a new specific health insurance smart card is not necessary, whilst the e-EHIC trustworthy dataset can be obtained either by scanning the eye-readable EHIC or by reading national/regional health smart cards and then checking data on-line.

The participating countries must accept all levels of cards (eye-readable, chip-based etc) that are agreed upon.

A pilot/demo was run in Germany summer 2006 during the football world cup.

Full deployment (phase C) will start in 2010.

Phase B includes:

- Extending the consortium from 20 partners in 10 countries to 26 partners in 15 countries + some self-funded observers
- Defining a common information system security policy (ISSP), to be agreed between all participating countries.
- Plan for initial deployment of 566 services points in 305 service sites.
- Extending the service to the e-billing procedure (based on EC regulation)
- Collaboration with related projects and industry partners
- Cooperation with the CASSTM/TC and the CEN/ISSS WS e-EHIC
- Evaluation of the service and assessment of the socio-economic impact

Impacts and benefits:

- For patients:
 - significantly simpler and faster procedures
- For healthcare providers
 - less administration and manual typing of data, speeding up costs refunding
- For health insurance providers
 - less administration, improved reliability and security of data
- For the EU
 - Jointly developed, harmonised solutions and expertise, based on existing national systems,
 - Validated professional basis for imminent political decisions on electronic European Health Insurance Cards

It shall be possible to check what kind of health insurance the patient has via this system.

In the chip card also medical data can be stored. This is being tested in Germany, for instance.

3. Summary / Conclusions

All presentations expressed the increasing need and demand for access to patient information. This is the case for both patient record information and health information that can be registered by and retrieved from (medical) sensors. The use of electronic health record systems and medical sensors, and the possibility for electronic communication, makes it possible to access patient information across organisation boundaries in a new and easy way. As pointed out by Søren Duus Østergaard (see section 2.4 above), new technology is rapidly moving into home care and healthcare, greatly helped by the development of cheap, reliant sensors able to measure health and condition in numerous ways. The amount of information from these sources will be too huge for both patients and healthcare professionals to handle in an efficient way. Intelligent systems will be needed, that can analyse the data and select the important information.

Since the technology exists, there is a wish (or demand) from the patients, and in some cases also from family members and relatives, to have access to the patient's own health information and to have the possibility to communicate electronically with healthcare providers. It is a trend that the patients themselves must take a greater responsibility for preventive healthcare and the follow-up of their own health. One reason for this is the rising costs caused by more patients and less service manpower in the healthcare sector (Søren Duus Østergaard, section 2.4). This creates a need for access to own health information and for advices and counselling from the healthcare services.

As pointed out by Mats Hagner (section 2.3 above), there is an exchange of patients between county councils and municipalities in Sweden. A national health summary record is therefore highly demanded from municipalities. There is also a great demand for this from the regions. The situation is the same in Norway. In addition, we see an increased mobility between regions and nations, with healthcare guarantees and healthcare clusters. The mobility of the citizens brings about a need for European inter-operable solutions. These require – besides European legal solutions – technical interoperability based on standards (Asbjørn Hovstø, section 2.5).

The privacy aspect is, however, a challenge. Ethical, legal, and security issues must be considered and clarified. In the Nordic region the main challenge is to find ways of fully utilizing the potentials of information technology in healthcare without jeopardizing the legal rights of patients, confidentiality requirements, treatment, etc. (Leif E. Nohr, section 2.2 above). How can we define guidelines and policies that can be directly supported by information and communication technology systems to enforce privacy legislation and be in accordance with the European Directive on Data Protection? This was asked by Søren Duus Østergaard (section 2.4), who also presented the following list of important ethical dilemmas with respect to measuring health and other conditions "online":

- feeling safe – revealing all activities
- critical illness – who should know?
- continuous monitoring – false alarms
- automatic feedback – misinterpretation?
- correlation between measurements – quality of staff, quality of decisions?
- shared care – shared data (needed information when treating the patients)
- individualized care – 'Deep knowledge'
- legal requirements – research possibilities

From all the presentations there seemed to be a common opinion that digital signatures should be used for the handling of and access to health information. The availability of a secured infrastructure like a health network was also pointed out as a prerequisite. All the Nordic countries, except Finland, have dedicated health networks. Finland's strategy is to use public networks with secure solutions like VPN and PKI.

Cross-border solutions do, in reality, not exist. As pointed out in the abstract for the NETC@RDS presentation (see section 2.6 above), the established online verification

infrastructure for cards or entitlement rights by the NETC@RDS Consortium is the first real pan-European interconnection of different states in the e-Health sector.

Balancing between privacy and the need to feel safe is not necessarily easy. An important question, raised by Søren Duus Østergaard (section 2.4), is: "What are the Privacy Enhancing Technologies that can help combine establishing a fine-graded health safety net under the clients and meet the legal and moral requirements for data protection?"

Technologies mentioned in several presentations include:

- eID, electronic ID solutions for both healthcare workers and patients
- Service-Oriented Architecture (SOA)
- role-based access techniques
- use of standards
- security policies

With regards to RFID, Asbjørn Hovstø (section 2.5) pointed out that privacy concerns persist to be a major obstacle to the wider-spread use of this technology in healthcare.

The presentations given at this symposium illuminate the need for further research with respect to how Privacy Enhancing Technologies and other measures can be applied in order to ensure privacy of individuals in healthcare settings at the same time as access to health information is ensured for those who need it and are accredited for it.

Del II: Nasjonalt miniseminar: “Tilgang på langs - Informasjonsdeling og sammenhengende pasientforløp: Juridiske og sikkerhetsmessige aspekter”

1. Innledning

Dette nasjonale miniseminalet ble arrangert i etterkant av den årlige konferansen “Tromsø Telemedicine and eHealth Conference” (TTeC)¹⁰, og startet like etter den avsluttende lunsjen på konferansens siste dag, 13. juni 2007. “Bakteppet” for dette seminaret var blant annet symposiet tidligere på dagen, og en workshop om “Tilgang på tvers” i juni 2006. Hensikt og målsetting med seminaret var å forsøke å få et overblikk over relevante juridiske og sikkerhetsmessige utfordringer knyttet til bruk av elektroniske virkemidler i pleie- og omsorgssektoren i Norge. Vi ønsket å diskutere noen av de konkrete utfordringer det er viktig å få løst for å kunne skape de sammenhengende pasientforløp vi ser for oss i framtiden. For å oppnå dette så var det som nødvendig at både nasjonale beslutningstakere og representanter for helsepersonell i pleie- og omsorgssektoren så vel som i spesialisthelsetjenesten var representert blant foredragsholderne. Det var også viktig å få med representanter fra leverandørsiden for å presentere mulige IT-tekniske løsninger på noen av utfordringene. Innledere ble derfor invitert med sikte på å oppnå nevnte målsetting.

Det var egen påmelding til miniseminalet, som hadde om lag 60 deltakere. Innlederne var spesielt invitert utfra tema. Programmet var utarbeidet av Nasjonalt senter for telemedisin som arrangerte seminaret sammen med HIT Nord-Norge¹¹.

Informasjon om miniseminalet var lagt ut som en egen web-side på hovedkonferansens nettsted¹². I tillegg ble det sendt ut invitasjon på e-post til HIT Nord-Norges medlemmer og andre relevante kontakter.

Programmet for miniseminalet er vist nedenfor. For de som leser denne rapporten elektronisk er tittelen på hvert innlegg også en link til tilhørende power-point presentasjon. Linker til alle presentasjonene finnes også på <http://www.telemed.no/index.php?id=519922>, under overskriften “Program med link til presentasjonene”.

¹⁰ <http://www.telemed.no/ttec2007>

¹¹ <http://www.telemed.no/index.php?cat=39259>

¹² <http://www.telemed.no/index.php?id=519922>

Program

Møteleder: Eva Henriksen, NST

- 13:45 – 14:30 **Velkommen** v/ Eva Henriksen, NST, og Tove Normann, HIT
[Introduksjon til dagens tema](#) v/ Ellen K. Christiansen, NST
[Nordiske trender](#) v/ Leif E. Nohr, NST
- 14:30 – 14:45 [Status for pågående lovarbeid i SHdir](#) v/Hilde Jordal, SHdir
- 14:45 – 15:45 **Hvordan oppnå helhet og sammenheng i pasientbehandlninga/eldreomsorgen? Situasjonen sett fra ulike ståsted i helsesektoren. Behov og mulige løsninger basert på eksempler fra:**
[Spesialisthelsetjenesten](#). Knut Magne Augestad, kirurg, gastrokir. avd. UNN / stipendiat NST
[Kommunene](#). Egil Rasmussen, Stavanger kommune
- 15:45 – 16:00 **Kaffepause**
- 16:00 – 16:15 [Hva mener Datatilsynet om deling av informasjon på tvers av etater og nivå i helse- og sosialsektoren?](#) v/ Helge Veum, Datatilsynet
- 16:15 – 17:00 **Informasjonsformidling og deling av informasjon mellom ulike aktører i helse- og omsorgssektoren, og mellom pasienter og disse. Ønsker, intensjoner og utfordringer.**
[Min Journal. Elektronisk kommunikasjon mellom pasient og spesialisthelsetjenesten](#) v/ Ivar Berge, rådgiver IT-avdelingen Rikshospitalet
[Individuell plan. Eksempel på behov for og utfordringer ved elektronisk løsning.](#) v/ Jorunn Bjerkan, stipendiat NTNU
[Kjernejournal – juridiske og sikkerhetsmessige utfordringer \(prosjekter i Trondheim og Tromsø\)](#) v/ Vigdis Heimly, KITH
- 17:00 – 17:10 **Kort pause**
- 17:10 – 17:50 **Paneldebatt.** I panelet: Innlederne
Runde: Synspunkter på miniseminaret/problemstillingene
Fremtidsvyer - bekymringer og håp. Hvilke hensyn mener vi må ivaretas for/i fremtiden? Realistiske målsettinger? Pasientens rolle som forvalter av informasjon om seg selv.
- 17:50 – 18:00 **Kort oppsummering**

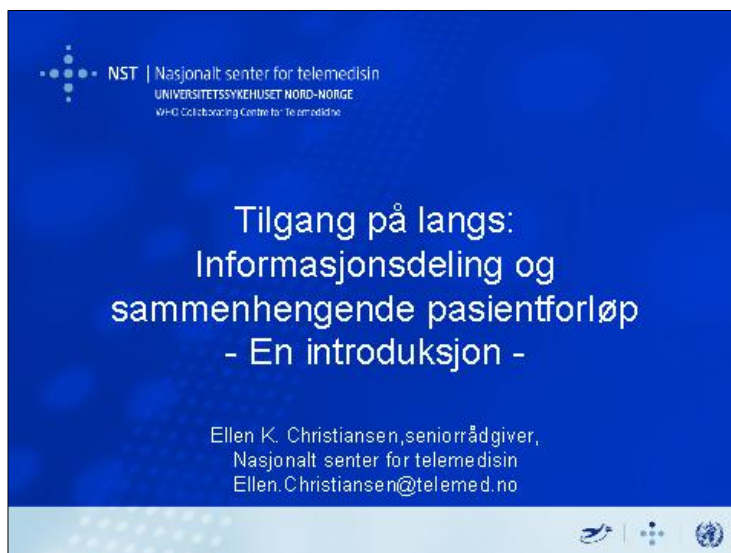
2. Presentasjonene

I de følgende avsnittene gis en oppsummering av hver enkelt presentasjon og de spørsmål og kommentarer som kom i etterkant. Linker til presentasjonene er lagt inn i hver overskrift og i det første bildet fra Power-Point-presentasjonen.

2.1 Ellen K. Christiansen, NST: [Introduksjon til dagens tema](#)¹³

Ellen K. Christiansen er seniorrådgiver og jurist ved Nasjonalt senter for telemedisin og har vært ansatt siden november 2000.

¹³ Innlegget er bearbeidet og supplert i den skriftlige fremstillingen.



Introduksjon

Opptakten til miniseminaret var først og fremst en workshop avholdt i Tromsø 1. juni 2006 om "Tilgang på tvers og deling av pasientopplysninger". Målgruppe for denne var nasjonale beslutningstakere, regionale helseforetak, helsepersonell, leverandører av elektroniske pasientjournalssystemer og ansatte i forskningsmiljøer. Tema den gang var ulike juridiske og sikkerhetsmessige problemstillinger knyttet til hvem som kan og skal ha tilgang til elektroniske pasientjournaler i gitte situasjoner og diskusjoner rundt det. I oppsummeringen av workshop'en ble det foreslått videre oppfølging i form av et seminar om "tilgang på langs" som et virkemiddel i et sammenhengende pasientforløp. Med "tilgang på langs" mente man både tilgang på tvers av forvaltningsnivåene, men med særlig fokus på dimensjonen "på langs" i et livsløp som i perioder vil kunne omfatte sykdom og behov for helsetilbud på flere nivåer.

Helsepersonellovens §§ 25 og 45 sett i sammenheng med helseregisterloven § 13

Bestemmelsene i helsepersonelloven (hlspl) (1) §§ 25 og 45 hjemler begge unntak fra hovedregelen om taushetsplikt i lovens § 21. Hlspl § 25 omhandler utveksling av pasientopplysninger i forskjellig former mellom "samarbeidende personell", både muntlig og skriftlig. Det siste tolkes dit hen at det også kan omfatte tilgjengeliggjøring av journalopplysninger (2). Samarbeidende personell kan befinne seg både i og utenfor den enkelte virksomhet. Hlspl § 45 omhandler bare journalopplysninger til "andre som yter helsehjelp". Disse kan også befinne seg både i og utenfor egen virksomhet. Journalopplysninger er opplysninger nedtegnet i journal, og omfatter følgelig i hovedsak opplysninger om behandling som er ytt (tilbakelagte "episoder"), i tillegg til eventuelle nedtegnelser om den aktuelle situasjon. For begge bestemmelser er det et vilkår at pasienten ikke skal ha motsatt seg utlevering. Unntakene omfatter bare opplysninger som er nødvendige for at mottaker skal kunne yte forsvarlig helsehjelp/kunne gi helsehjelp på forsvarlig måte. Den mest iøynefallende forskjellen på vilkårene i de to bestemmelsene, er kravet i hlspl § 45 om at det skal nedtegnes at opplysninger er levert ut. Man kan spørre seg hvorfor det ikke stilles det samme uttrykkelige krav til nedtegnelse dersom journalopplysninger utleveres til samarbeidende personell med hjemmel i hlspl § 25. Kan det være tanken at all formidling av journalopplysninger per definisjon er hjemlet i hlspl § 45? Det kan synes uklart hvilke konsekvenser det skal få at hlspl § 45 har bestemmelsen om at det skal fremgå av journalen at opplysninger er formidlet videre. Dersom journalopplysninger om en pasient kan utleveres til samarbeidende personell med hjemmel i hlspl § 25, bør det vel også fremgå av journalen når slik utlevering har funnet sted? Det er vanskelig å se at denne passusen i seg selv skulle være en begrunnelse for ulik praksis rundt eventuell utlevering av journalopplysninger etter de to bestemmelsene.

Skillet mellom "samarbeidende personell" og "andre som yter helsehjelp" er på mange måter interessant, idet det samme helsepersonell kan inneha begge roller samtidig, avhengig av hvilket ståsted man velger å se det fra. Det samme helsepersonell som er definert som

samarbeidende personell rundt en pasient i en aktuell sykdoms-"episode", vil kunne være definert som "andre som yter helsehjelp" når de innhenter journalopplysninger om pasientens tidligere sykdomsforløp fra egen eller annen virksomhet. Med bakgrunn i dette anser jeg at "samarbeidende personell" kan få kommunisert (bl.a.) journalopplysninger om en aktuell episode med hjemmel i hlspl § 25, mens utlevering av journalopplysninger om tidligere ytt helsehjelp (tidligere episoder) til det samme personellet etter omstendighetene skal hjemles i hlspl § 45. Dette er åpenbart et mulig tema for diskusjon og klargjøring.

Disse bestemmelsene i hlspl gir i og for seg ingen direkte anvisninger på hvordan pasientopplysningene kan eller skal formidles. De sier for eksempel ingenting om når opplysningene kan gjøres tilgjengelig ved at helsepersonell får tilgang til og kan hente ut opplysningene direkte fra pasientens elektroniske pasientjournal (EPJ). De gir bare anvisning på når unntak fra taushetsplikten er lovlig; dvs. hvem som kan gis opplysninger og på hvilke vilkår.

Det er helseregisterloven (hlsregl) § 13 som uttrykkelig regulerer hvem som kan gis direkte tilgang til helseopplysninger som behandles iht. helseregisterloven (3). Loven regulerer behandling av helseopplysninger i helseforvaltningen og helsetjenesten som skjer helt eller delvis med elektroniske hjelpemidler og annen behandling av helseopplysninger når de inngår eller skal inngå i et helseregister. Journalsystemer er definert som et behandlingsrettet helseregister og inkluderer både det som er omtalt som manuell pasientjournal og elektronisk pasientjournal (EPJ), under forutsetning av at formålet er å yte helsehjelp, jf hlsregl § 2, pkt. 7 og kommentarene til den (4). I henhold til denne bestemmelsen er det bare den som arbeider under den databehandlingsansvarliges instruksjonsmyndighet som kan gis tilgang til helseopplysningene i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldene bestemmelser om taushetsplikt (3). Under databehandlingsansvarliges instruksjonsmyndighet er i all hovedsak bare ansatte i virksomheten, selv om instruksjonsmyndighet også kan avtales i forbindelse med bestemte oppdrag (5). Det å slippe ansatte i andre virksomheter inn i en virksomhets EPJ-system, anses iflg. Datatilsynet uforenlig med å ivareta plikten til å sikre opplysningenes konfidensialitet iht. hlsregl § 16, jf. kommentarutgaven til helseregisterloven, s. 92 (4). Dette begrunnes i at det medfører en sikkerhetsrisiko som ikke er akseptabel.

I forbindelse med helsepersonelloven § 45 er det uttrykkelig uttalt i forarbeidene til loven at siden bare opplysninger om tidligere ytt helsehjelp som er nødvendige for å yte forsvarlig helsehjelp i den aktuelle situasjon kan utleveres, kreves en konkret vurdering av nødvendigheten før utlevering (6). Med bakgrunn i dette har det vært hevdet at utlevering iht. § 45 i prinsippet ikke kan skje ved at noen gis tilgang til hele eller deler av pasientjournaler i EPJ-systemer, dersom dette ikke også innebærer en forhåndsvurdering av berettigelsen av utlevering. I den forstand kan en likevel si at hlspl § 45 i praksis gir anvisning på hvordan opplysningene (ikke) kan tilgjengeliggjøres. Det er ikke skilt mellom helsehjelp som er ytt i og utenfor egen virksomhet.

I rundskriv IS-7/2006 fra Sosial- og helsedirektoratet om tilgang til og utlevering av pasientopplysninger i elektroniske pasientjournaler, er det skilt mellom egen og andres virksomhet når det gjelder utlevering av journalopplysninger om tidligere ytt helsehjelp. Det er vektlagt at det skal fremgå av journalen at opplysninger er gitt til andre, noe som også tilsier at det er utlevering i henhold til hlspl § 45 som er omtalt. Det heter imidlertid i denne forbindelse: "Hvis det er snakk om å gi opplysninger til andre i egen virksomhet, kan det skje ved at mottakerne får tilgang til de aktuelle helseopplysningene i EPJ-systemet." (7) Det er muligens reelle hensyn som er begrunnelsen for dette synet. Det er også pekt på at tilgangsstyring internt ikke må hindre helsepersonellet i å utføre sine lovpålagte plikter forsvarlig. Det er ellers ikke sagt noe nærmere om hvilke konkrete krav som eventuelt stilles til tilgangsstyring når opplysninger om tidligere helsehjelp skal tilgjengeliggjøres for ansatte i egen virksomhet. Journalnedtegnelser om tidligere ytt helsehjelp til "andre som yter helsehjelp" *utenfor* den enkelte virksomhet, kan i følge det samme rundskrivet bare utleveres etter forespørsel og en vurdering av relevansen.

Hlspl § 25 stiller i likhet med hlspl § 45 krav om at opplysningene skal være nødvendig for å kunne yte forsvarlig helsehjelp. I rundskriv IS-7/2006 fremgår det at Sosial- og helsedirektoratet åpner for at også samarbeidende personell innenfor den enkelte virksomhet iht. hlspl § 25 skal kunne få tilgang til virksomhetens EPJ-system for å hente ut journalopplysninger, under forutsetning av at det er etablert tilfredsstillende tilgangsstyring. Det er et uttrykkelig krav at vedkommende skal ha autorisasjon, at det er fattet beslutning om at det

skal ytes helsehjelp til den pasienten det gjelder, at logg føres og følges opp og at det gis nødvendig informasjon og opplæring til de ansatte. Autorisasjon "innebærer at en person i en bestemt rolle er gitt bestemte rettigheter til lesing, registrering, retting, sletting og/eller sperring av helseopplysninger". Det heter videre i rundskrivet at "Taushetsplikten ivaretas ved at en person bare tildeles autorisasjon til å gå inn i deler av EPJ-systemet som direkte kan knyttes til vedkommendes arbeidsoppgaver og roller." Dersom opplysningene skal gis til samarbeidende personell utenfor virksomheten, må de utleveres som ellers, siden ansatte i andre virksomheter ikke vil være underlagt databehandlingsansvarliges instruksjonsmyndighet.

Tanken bak dette kan være at en slik løsning ivaretar taushetsplikten ved at tilgangen styres og at arbeidsgiver har mulighet til å kontrollere/følge opp egne ansatte. På denne måten ivaretar virksomhetens ledelse plikten til å sørge for at pasientopplysningene både er tilfredsstillende sikret og på samme tid tilgjengelige. Hlsregl § 13 er til hinder for at ansatte utenfor virksomheten kan tilegne seg pasientopplysninger på samme måte.

Det kan være flere gode grunner til å legge seg på en slik linje innenfor gjeldende lovgivning. Det legger opp til en viss smidighet innad i systemet, samtidig som man, i tråd med kravet i hlsregl § 13, ikke åpner systemene for helsepersonell som man ikke har mulighet til å instruere og/eller iverksette sanksjoner i forhold til. Det at praksisen skal være den samme for de to bestemmelsene (hlspl §§ 25 og 45, hhv. samarbeidende personell og andre som yter helsehjelp) virker også logisk med begrunnelse i at vilkårene for utlevering i de to bestemmelsene er nesten likelydende.

Helseregisterloven § 13 kan sis å ha en mer begrenset selvstendig betydning enn det som ofte kommer klart frem i diskusjoner. Det er neppe bare denne bestemmelsen som er til hinder for direkte tilgang til EPJ for ansatte i andre virksomheter. Siden bare opplysninger som er nødvendig for å gi pasienten forsvarlig helsehjelp kan utleveres/tilgjengeliggjøres til andre som yter helsehjelp iht. hlspl § 45, kreves en eller annen betryggende form for forhåndsvurdering før opplysninger gjøres tilgjengelige/gis ut. Dette er, blant annet iflg. forarbeider og rundskriv IS-7/2006, til hinder for at pasientopplysninger kan formidles til ansatte utenfor virksomheten via tilgang til virksomhetens EPJ-system. Man har riktignok valgt å åpne for at opplysningene kan gjøres tilgjengelige for ansatte innenfor virksomheten via EPJ-systemet, både til samarbeidende personell og "andre som yter helsehjelp". Men utlevering til ansatte i andre virksomheter krever altså iht. helselovgivningen en forhåndsvurdering, noe som i og for seg også er i tråd med vilkårene i hlsregl § 13.

Kravet om en forhåndsvurdering er lite omtalt i forbindelse med hlspl § 25. Det fremgår ikke, så vidt vites, uttrykkelig av verken forarbeider eller andre kommentarer at det legges opp til den samme forhåndsvurdering ved utlevering av journalopplysninger til samarbeidende personell utenfor virksomheten. Dette til tross for at vilkårene for utlevering er nesten identiske i de to bestemmelsene. Hvis en forhåndsvurdering ikke er påkrevd iht. hlspl § 25, kan det muligens hevdes at det er hlsregl § 13 alene som er til hinder for at samarbeidende personell i én virksomhet kan gis tilgang til en annen virksomhets EPJ-system for å tilegne seg journalopplysninger om en pasient det samarbeides om i en aktuell situasjon. Dette er i så fall et spørsmål som med fordel kunne være gjenstand for diskusjon.

Sammenhengende pasientforløp og behovet for informasjon

God samhandling rundt pasienten og sammenheng mellom ulike helsetilbud er uttalte mål i norsk helsevesen. Dette er blant annet trukket fram i NOU 2005:3 Fra stykkevis til helt. God samhandling er trukket fram som en forutsetning for en sammenhengende behandlingsskjede. God informasjonsflyt ses på som én av forutsetningene for at helsetjenesten skal fungere godt for pasienter med behov for helhetlige, langvarige og koordinerte tjenester. Elektroniske pasientjournaler i alle deler av helsetjenesten er en forutsetning for helhetlige pasientforløp (8). Det som her er kalt "helhetlige pasientforløp" går under litt ulike betegnelser i ulike sammenhenger, herunder sammenhengende pasientforløp, gode pasientforløp, sammenhengende tiltak og godt koordinerte pasientforløp, for å nevne noen. Alle handler om god samhandling mellom de ulike aktører i helsevesenet som har ulike og overlappende oppgaver i forhold til samme pasient, her er de omtalt som sammenhengende pasientforløp. Det er bred enighet om at en av forutsetningene for å få til dette, er at de som skal yte tjenester, har den informasjon om pasienten som de trenger for å yte forsvarlig helsehjelp.

Dette virker tilsynelatende både selvsagt og enkelt, og det handler om helhet og sammenheng. Men: Hva er egentlig et sammenhengende pasientforløp? Fra hvem sitt ståsted og på hvilken måte skal det henge sammen? Hvor lenge skal det henge sammen? Og hvis målet med informasjonsutveksling og -formidling er et sammenhengende pasientforløp: Hvordan kan det legges opp til rutiner og ordninger rundt dette som skaper sammenheng over tid samtidig som taushetsplikten ivaretas?

I midtveisevalueringen av S@mspill 2007 (9) er det stilt spørsmål ved om sammenhengende forløp bare betyr at forskjellige pleiere og behandlere har tilgang til felles data, eller om det betyr at disse arbeider sammen i en felles prosess. Det kan stilles spørsmål ved om ikke et sammenhengende pasientforløp er noe helsepersonell og *pasienter/pårørende* må samarbeide om i en felles prosess.

I rapporten er det også pekt på at IT-støtte kun er ett av flere ulike midler til å skape et sammenhengende pasientforløp. Forfatterne mener at dersom det skal være mulig å få til et sammenhengende forløp, forutsetter det teoriutvikling. Spørsmål som stilles er: Hva er et pasientforløp? Og: Er for eksempel en diabetiker som behandles for ulike lidelser involvert i ett eller flere pasientforløp?

Det kan og har vært hevdet at vi vet vi for lite sikkert om behovet for å formidle pasientinformasjon og i hvilke situasjoner det er til stede. Hvilken type informasjon er vital når? Det er også begrenset viten om hvilke konsekvenser manglende eller mangelfull tilgang til pasientinformasjon medfører i praksis. Skal det kunne sies noe fornuftig om de reelle behov, må det ses i sammenheng med en uttrykt målsetting for hva man ønsker å oppnå med slik formidling. Ønsker man å oppnå sammenhengende pasientforløp? Færre dødsfall? Friskere pasienter? Mer adekvat behandling? Mer effektiv behandling? Billigere behandling? Mindre dobbeltarbeid? Mindre gråsoner? Mer fornøyde pasienter?, for å nevne noen mulige gevinster.

På denne bakgrunn kan det hevdes at diskusjonen om (mer utstrakt) tilgang til elektroniske pasientjournalssystemer på tvers av virksomheter og forvaltningsnivåer har lett for å bli for snever. Problematikken må både ses i sammenheng med hva man ønsker å oppnå med det, hvilke andre virkemidler som skal benyttes for å nå målet, samt gjeldende og mulig fremtidig lovgivning på området.

Det kan også være relevant å diskutere mulige alternative måter å formidle pasientinformasjon på. Det er eksempler på at helsepersonell på kommunalt nivå har uttalt at dersom de hadde fått epikriser i tide og pålitelig og oppdatert informasjon om medisinbruk fra spesialisthelsetjenesten, ville de foretrekke det. De ville da få dekket sitt behov for informasjon om pasienten, og kan slippe å skulle forholde seg til andre(s) elektroniske journalssystemer. Diskusjonen rundt en eventuell endring av helseregisterlovens § 13 sett i sammenheng med helsepersonellovens §§ 25 og 45 er både relevant og nødvendig, men det er også viktig å ta i betraktning at behovet for tilgjengelighet må avveies mot plikten til å sikre opplysningenes konfidensialitet. Dette kan ses på som en av grunnene til at det blir så viktig å se dette i en større sammenheng.

Videre diskusjoner

- Hva er et sammenhengende pasientforløp?
- Hva er informasjonsbehovet i et sammenhengende pasientforløp?
- Hvilken pasientinformasjon kreves for en forsvarlig pasientbehandling?
- Hvilke risikoer oppstår eventuelt som følge av mangel på pasientinformasjon i gitte situasjoner?
- Avveiningen av behovet for tilgjengelighet og plikten til å sikre opplysningene
- Hvordan kan behovet for pasientinformasjon i ulike situasjoner oppfylles?
- Hvordan strukturere EPJ?
- Hvilke virkemidler kan og skal benyttes?
- Viktigheten av å se ulike virkemidler i sammenheng!

Referanser

1. LOV 1999-07-02 nr 64: Lov om helsepersonell m.v. (helsepersonelloven)
2. Anne Kjersti Befring Bente Ohnstad Helsepersonelloven –med kommentarer, Fagbokforlaget 2001, s. 139
3. LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
4. Sverre Engelschiøn, Christine Lie Ulrichsen, Bjørn Nilsen: Helseregisterloven Kommentartutgave, Universitetsforlaget 2002, s. 52
5. Hilde Jordal, seniorrådgiver/avdelingsdirektør, Sosial-og helsedirektoratet i foredrag 13. juni 2007
6. Ot prp nr 13 (1998-99) Om lov om helsepersonell m v (helsepersonelloven), Sosial- og helsedepartementet, s. 240
7. Rundskriv IS-7/2006 Rundskriv vedrørende tilgang til og utlevering av opplysninger i elektroniske pasientjournaler, Sosial og Helsedirektoratet, s. 15
8. NOU 2005: 3 Fra stykkevis til helt En sammenhengende helsetjeneste Innstilling fra et utvalg oppnevnt ved kongelig resolusjon av 17. oktober 2003. Avgitt til Helse-og omsorgsdepartementet 1. februar 2005.
9. Midtveisevalueringen av S@mspill 2007, Avsluttende rapport, Rambøll Management, 2006, s. 9

2.2 Leif Erik Nohr, NST: Juridiske rammer for utveksling av helseinformasjon - et nordisk overblikk

Leif Erik Nohr er juridisk rådgiver og har vært ansatt ved Nasjonalt senter for telemedisin siden 1998.



(Dette foredraget var en norsk versjon av det som ble holdt under symposiet (på engelsk). Vi nøyer oss her med å vise til dette – se avsnitt 2.2 i del 1.)

I evalueringen av seminaret var det flere som fremhevet oversikten over nordisk praksis som relevant og interessant. Dette er et tema vi vil følge opp i det videre arbeidet, særlig med henblikk på hvordan sikkerhetsmessige spørsmål blir behandlet og løst i de andre nordiske landene.

2.3 Hilde Jordal, SHdir: Enkel og trygg tilgjengelighet til pasientopplysninger i EPJ ved ytelse av helsehjelp – vurdering av lovendringer

Hilde Jordal er seniorrådgiver i Sosial- og helsedirektoratet (SHdir).



Mens de to foregående foredragsholderne snakket om hva vi har i dag, handler denne presentasjonen om hva vi kan få i framtida.

SHdir har fått et oppdrag fra HOD. I oppdragsbrevet står det hva departementet ønsker:

- Forslag til lovendringer med sikte på at pasientinformasjon kan deles – eller gjøres tilgjengelig for behandlende helsepersonell i og mellom virksomheter som yter helsehjelp, herunder vurdere
 - ansvarsforhold for pasientopplysningene
 - IT-løsninger for enklere kommunikasjon
 - bedre og raskere tilgang uten at personvernet forringes
 - kjernejournal som kan gi tilgang til kritisk informasjon
- Forslag til forskrift om sikkerhetsmessige tiltak

SHdir har fått en frist ut året 2007 for dette arbeidet.

Bakgrunn

Innføringen av elektronisk pasientjournal (EPJ) har pågått over mange år. Først i 2001 ble det slått fast i lov at behandlingsrettede helseregistre kan føres kun elektronisk. Nå er papirjournalen mer unntaket enn regelen. Det er forventninger om at EPJ skal gi bedre diagnostikk og behandling, og effektivisering av driften av helsetjenester. Det har vært en omorganisering i helsevesenet, også internt på sykehus, som gjør at det er behov for å endre måten man får tilgang til informasjon på. Det har vært et sterkt press på endring av regelverket.

Målet for prosjektet er å bidra til at nødvendig og relevant pasientinformasjon skal være tilgjengelig på en betryggende måte ved tjenstlig behov for å understøtte helhetlige pasientforløp, slik at behandlingen ikke stopper opp pga mangel på informasjon. Pasientperspektivet og helsepersonells rolle som samarbeidspartner i forhold til pasienten skal ivaretas. Man må legge opp til ordninger hvor også pasienten får slippe til. Pasientjournalen skal fungere som et arbeidsverktøy i tråd med intensjonene i lov og forskrift.

Elementer som inngår i prosjektet:

- Analyse av
 - medisinsk/helsefaglig behov
 - behov for omstrukturering i helsesektoren
 - prinsipper for å oppnå klare ansvarsforhold
 - dagens samhandlingsmønstre
 - pasientens selvbestemmelse og integritet
- Vurdering av modeller/modellelementer/e-løsninger som
 - kjernejournal
 - tilgang til journalopplysninger på tvers av juridiske enheter

- "Felles journal" der behandlere på tvers av virksomheter og nivåer fører i felles journal
- pasientindeks
- pasientbåret informasjon
- ev. andre løsninger

Prosjektet skal ende opp med en anbefaling av modell/modeller.

SHdir skal lage forslag til lovendringer (står hlsregl § 13 for fall?). Tanken er at hvis noen har fått et oppdrag (uten gjennom et ansettelsesforhold) så skal det kunne gis tilgang til det elektroniske journalsystemet innenfor de begrensninger som fremgår av helselovgivningen. SHdir skal også utarbeide utkast til forskrift om sikkerhetsmessige krav. Hvis man får enklere tilgang, må dette kombineres med strengere sikkerhetsmessig kontroll. Pasientene må føle seg trygge på at kun de som trenger informasjonen og har rettmessig krav på den, får den.

SHdir tar gjerne imot innspill på følgende elementer/problemstillinger:

- Pasientindeks – foreligger det et behov for det?
- Hvilke forhold tilsier at det trengs tilgang på tvers av virksomheter?
- Er det spesielle behov ved enkelte typer tjenester? F.eks. legevaktjenester
- Hvilke løsninger for enklere tilgang bør man konsentrere seg om?
- Andre innspill til prosjektet

Spørsmål/kommentarer/diskusjoner som kom opp:

Det ble spurt fra salen om det sitter pasientorganisasjoner i arbeidsgruppen. Hilde Jordal svarte til dette at de nå kun har en intern arbeidsgruppe, og at vil trekke inn de det er behov for underveis. De vil også prøve å trekke inn pasientorganisasjoner, men tiden tillater ikke å gå ut bredt til alle relevante miljø.

Til spørsmål om de ser på problemstillingen om forsikringselskap kan få tilgang til EPJ via samtykke, ble det svart at det ligger utenfor mandatet til prosjektet.

Fra UNN ble det kommentert at det var mye godt å høre i dette innlegget, og at de kommer til å benytte anledningen til å komme med innspill. Det ble videre sagt at det som bekymrer dem når de prøver å etterleve regelverket i dag, er at det de erfarer som viktig hindres av lovgivningen. Det er mye informasjonsutveksling som er dårlig dokumentert og som foregår i lukkede rom, f.eks. innen radiologi. Det er innebygde rutiner som gjør at dette foregår på en sikker måte, men regelverket tillater egentlig ikke at det foregår. De utveksler informasjon til pasientens beste. De anbefaler derfor arbeidsgruppen om å prøve å få delta i den kliniske virkeligheten, f.eks. på morgenmøter på sykehus.

På UNN har de vært flinke til å bruke loggene for å avdekke snoking i ettertid. Men den pasienten som det har vært flest journaloppslag på i første halvår 2007 på UNN har 14.000 oppslag gjort av 238 aktører. Hvordan skal man kunne kvalitetssikre loggene i ettertid? Noen foreslår å la pasientene få tilsendt logg på alle oppslag i journalen sin. Hvordan skal dette gjøres på en fornuftig måte?

Det ble videre kommentert fra salen at "pasientbåret informasjon" er et begrep med god klang og god smak. Man må ikke glemme at journalen også er en viktig bærer for informasjon til pasienten selv. Gjennom den har mange fått nyttig informasjon både om diagnose og behandling, men også om hvordan helsepersonell har tenkt og vurdert.

En av tilhørerne hadde utfra innlegget oppfattet at problemstillingen i § 13 kan ses mildere på hvis en person har et oppdrag på et sykehus, men ikke er ansatt. Tilgang utenfra kan dermed til en viss grad løses gjennom spesielle avtaler. Det ble også foreslått en løsning med "stafett-basert" tilgang ved overføring av pasienten fra ett sykehus til et annet.

2.4 Knut Magne Augestad, NST/UNN: Informasjonsbehov i en klinisk hverdag

Knut Magne Augestad¹⁴ er kirurg ved gastrokirurgisk avdeling på UNN og stipendiat ved NST. Som stipendiat er han prosjektleder for prosjektet Nye telemedisinske tjenester ved en kirurgisk avdeling¹⁵.



Knut Magne Augestad tok utgangspunkt i to pasientgrupper som oppleves som de mest problematiske med tanke på informasjonsflyt: kreftpasienter og akutte hendelser.

1. Pasienter med tykktarmskreft

Dette er den tredje vanligste krefttypen i Norge, med ca 2000 nye tilfeller pr år.

Pasientene følger et fastlagt kontrollopplegg i fem år etter operasjonen. Ved å gjennomgå et slikt kontrollopplegg kan man oppdage tilbakefall tidligere og tilby ny operasjon.

Hverdagen på en kirurgisk poliklinikk preges av mange konsultasjoner, lange ventelister, komplisert logistisk mønster innad på sykehuset (blodprøver, røntgenbilder og møte med flere spesialister samme dag), og komplisert samhandling mellom fastlege og spesialist. Når en henvisning kommer inn har sykehuslegen liten mulighet for å få informasjon om det man lurer på. Telefonen er eneste hjelpemiddel, men fastlegene er så lite tilgjengelig på telefon at dette sjelden benyttes. Henvisninger er av veldig varierende kvalitet når det gjelder anamnese, tidligere sykdommer, medikamenter og klinisk undersøkelse. Man får av og til henvendelser av typen "Pasienten har vondt i maven. Ønsker utredning". Polikliniske notat fra sykehuset er også av varierende kvalitet.

Samhandlingen om eldre pasienter er ofte problematisk. Eldre pasienter kan ha mange lidelser. Disse pasientene har gjerne mange "treffpunkter" med helsevesenet på mange nivåer (fastlege for blodtrykkskontroll, medisinsk avdeling for KOLS, kirurgisk avdeling for tykktarmskreft, etc). Det kan være forskjellige årsaker til de ulike medisinske konsultasjoner. Pasienter selv blir ofte informasjonskilde. Dette kan være problematisk, særlig når pasientene er litt demente, eller ikke husker hvilke medikamenter de bruker eller hvilke funn som ble gjort ved tidligere undersøkelser. Det er svært vanskelig å innhente informasjon mellom nivåene. Spesialisten må som regel ringe fastlegen for å få informasjon, og fastlegen må ringe spesialisten. Begge er lite tilgjengelig på telefon, og man kan fort gi opp forsøkene på å få tak i henholdsvis fastlegen eller spesialisten.

¹⁴ <http://innsia.custompublish.com/index.php?cat=35873&XY&showdetails=348999>

¹⁵ <http://www.telemed.no/augestad-knut-magne.520355-4549.html>

I 2004 ble det på UNN gjort 485 konsultasjoner for kontroller av CRC (Colo-Rectal Cancer, kreft i tykktarm/endetarm). Pasientene hadde andre problemstillinger som ble "hengende i luften" fordi man ikke fikk tak i fastlegen.

Et igangsatt forskningsprosjekt¹⁶ skal forsøke å gi svar på to ting:

1. Må alle kontrolleres på poliklinikken?
2. Hvordan bedre samhandlingen mellom nivåene? Kan Norsk helsenett brukes?

Det skal gjøres en randomisert kontrollert studie hvor man sammenligner kvalitet på kontroll hos fastlege med kontroll på poliklinikk.

Et godt etterkontrollopplegg er viktig for å forlenge forventet levetid etter inngrep for tykktarmskreft.

I dag brukes et papirskjema ved poliklinisk kontroll. Skjemaet scannes inn som et vedlegg til journalen. Fastlegen får en kort rapport, men har ingen mulighet til å få en helhetsoversikt over det som står på skjemaet. Ved hver av kontrollene skal det tas blodprøver og ved noen kontroller skal det tas røntgen av lungene og foretas en klinisk undersøkelse. Målet med kontrollene er å skolere pasientene, påvise tilbakefall og bedre behandlingsresultatene.

Hva møter pasienten i de fem årene med etterkontroller? Hvilke treffpunkter har de med helsevesenet?

- 16 oppmøter på kirurgisk poliklinikk
- Blodprøver 16 ganger
- 8 røntgenundersøkelser
- To kikkhullsundersøkelser av tykktarmen
- Møter hos fastlegen
- Kommunal pleie- og omsorgssektor
- Eventuelle andre besøk pga andre sykdommer

Prosjektets forslag til løsning:

Det skjer en stadig økende bruk av Norsk helsenett. 60 % av alle henvisninger i Helse Nord går elektronisk. Vi tror det er et stort uforløst potensial. Prosjektet ønsker å utvikle et elektronisk kontrollkort slik at fastlegen, spesialisten og andre med behov kan gå inn på skjemaet og se hva som har foregått med pasienten. Kontrollkortet skal være tilgjengelig fra sykehusets journalsystem (DIPS), fastlegejournaler og for pasienten selv.

Prosjektets målsetting i hht protokoll:

- Bedre samhandling mellom spesialist og fastlege
- Brukervennlig
- Oppdatere kontinuerlig fastlegejournal og sykehusjournal
- Inneholde opplysninger om røntgenundersøkelser, blodprøve (CEA), koloskopi, anamnese og klinisk undersøkelse
- Tips til fastlege vedrørende anamnese, klinisk undersøkelse, tegn på residiv
- Maler for henvisning (røntgen, koloskopi, osv)
- NB! Klare rutiner ved mistanke om tilbakefall

2. Situasjon nummer to: akutt hjelp

To unge kvinner på vei fra Harstad til Tromsø kolliderte front mot front ved Laksvatn (ca 50 km fra Tromsø). De ble fraktet til UNN. Begge var bevisstløse da de kom inn og kunne ikke redegjøre for eventuell medisinbruk, allergier eller annet. Vakhavende lege ringte til sykehuset i Harstad for å finne ut hva de hadde vært utsatt for tidligere. Det kunne i denne situasjonen vært veldig hensiktsmessig med direkte tilgang til journalen deres i Harstad.

På sommeren er det ekstra stort behov for tilgang til journalopplysninger i andre helseforetak pga pasienter på feriereise; bl.a. mange eldre som kommer med hurtigruta. I dag er det svært vanskelig å få tak i nødvendig informasjon. Dette gjelder ved alle hendelser som

¹⁶ <http://www.telemmed.no/onkolink.450501-51252.html>

endrer bevissthetsnivået til pasienten, dvs. ulykker og indremedisinske tilstander. Er telefon godt nok? Nei, her må vi få bedre løsninger.

Spørsmål/kommentarer/diskusjoner som kom opp:

Det ble fra salen spurt om informasjonsutvekslingen går fortere enn før nå når 100 % av epikrisene fra UNN går elektronisk, eller om det har skjedd andre ting som gjør at det går fortere. Til det var svaret at det varierer fra avdeling til avdeling.

Fra kommunenes ståsted ble det påpekt at informasjonen i et slikt kontrollkort vil være nyttig også for Pleie- og omsorgssektoren (PLO) i kommunene, da en stor del av disse pasientene er eldre som allerede er innenfor PLO sitt ansvarsområde.

2.5 Egil Rasmussen, Stavanger kommune: Hvordan oppnå helhet og sammenheng i eldreomsorgen/pasientbehandlingen

Egil Rasmussen er prosjektleder i Stavanger kommune. Han har hatt ansvar for diverse prosjekt som har gått på innføring av nye tekniske løsninger: automatisk trygghetsalarm-sentral, nøkkelbokser, multidose, EPJ, meldingsutveksling. Rasmussen har i mange år vært med på strategiske diskusjoner i forhold til utvikling av tjenesten. Arbeidet med meldingsutveksling har gitt ham et nært samarbeid med sykehuset.



Kommunenes pleie- og omsorgssektor er i volum på nivå med spesialisthelsetjenesten og har flere ansatte. I helseforetakene er man frustrert over mange gamle som de ikke kan få gjort noe for på sykehuset og som heller bør ut i kommunene. Fastlegene er veldig selvstendige og det er ikke enkelt å samhandle med dem. Det er lettere å samhandle med pleie- og omsorgstjenesten.

I kommunehelsetjenesten er det behov for samhandling i flere retninger:

- internt i kommunene (fysioterapi, ergo, pleie- og omsorgstjeneste, hjelpemiddelkontor, bestillertjeneste, etc)
- med fastlege
- med helseforetak ved overføring fra/til sykehus
- med andre instanser
 - hjelpemiddelsentral (veldig vanskelig å få på banen, mye frustrasjon)
 - tannlege
 - sosialkontor, NAV
 - skatteetat (for å kreve betaling for tjenestene)

- med pasient
- med pårørende

I det følgende diskuteres løsninger i de ulike retningene slik de er realisert i Stavanger kommune:

Løsning 1 – internt: Pleie- og omsorgssystem, EPJ-system for pleie- og omsorgssektoren.

Dette er en sammensatt journal med individuell plan, behandlingsplan, diagnoser, løpende rapportering, medikamenter, prøvesvar, korrespondanse og meldingsutveksling, brukers nettverk og tjenester. Mye informasjon om brukeren er samlet her. Det er et saks-behandlingssystem, og det håndterer arbeidsplanlegging, turnus og fravær. Man har håndtering av ressurser og lager. Det benyttes av mange forskjellige helsepersonell som sykepleiere, hjelpepleiere, omsorgsarbeidere, miljøpersonale, assistenter, fysioterapeuter, ergoterapeuter, merkantile, hjelpemiddellager. Systemet fungerer også som kommunikasjon mellom avdelinger om pasienter.

Løsning 2a – fra sykehus til kommune:

I Stavanger har de tatt i bruk elektroniske meldinger fra sykehus til kommune. Tidligere hadde de "pasientbåret" informasjon på lapper som ble lagt i veska til pasienten. Det fungerte relativt bra, men var lite leselig.

De elektroniske meldingene som er tatt i bruk er:

- Utskrivningsrapport fra sykepleier og lege (tverrfaglig epikrise)
- Lege-epikrise
- Rapport/henvisning til fysioterapi, ergoterapi
- Rapport fra lege og sykepleier ved søknad om kommunale tjenester
- Melding om utskrivningsklar pasient
- Melding om innleggelse/utskrivning
- Laboratoriesvar

Løsning 2b – fra kommune til sykehus:

Følgende elektroniske meldinger er tatt i bruk:

- Innleggelsesrapport inkludert medikamentkort
- Henvisning
- Dialogmelding
- Avviksmelding

Gjennom arbeidet har man sett at avvik oppstår veldig ofte, og det er svært viktig å håndtere disse.

Løsning 2c – elektronisk meldingsutveksling med andre

- Fastleger
- Apotek/multidoseleverandør
- Hjelpemiddellager
- Sosialkontor/NAV
- Skatteetat
- Pasient
- Pårørende

Løsning 3: Informasjonsdeling

Følgende elektroniske meldinger er tatt i bruk:

- Kjernejournal
- Individuell plan
- Helsekort for gravide

- Hjelpemidler – bestilling, behandling, distribusjon (det er viktig å vite hvor langt en bestilling har kommet)

Erfaring med adressering av meldinger:

- Adressering er nøkkelen til å senke terskelen for å sende meldinger, og til sikkert og rasjonelt mottak
- Valgte en løsning som er robust mot interne omorganiseringer i kommunen, og mot flytting av pasient mellom avdelinger
- Sender til sykepleier, lege, fysioterapeut, ergoterapeut, saksbehandler
- Journalsystemets meldingsmottak finner ut hvilken avdeling som dokumenterer aktuell tjeneste, og varsler ansvarlig e-meldingsmottaker på denne avdelingen, samtidig som meldingen også legges i pasientens journal
- Dersom avdelingsmeldinger ikke er lest, varsles ansatte i avdelingen når de logger seg på journalsystemet. De kan eventuelt overta meldingsansvaret hvis de er autorisert til det

Erfaring med stans i meldingsstrøm:

- I perioder kommer ikke meldingene fram. Årsaker kan være:
 - Avsender leverer utskrift til pasient, men venter med å godkjenne av ulike grunner
 - Stanset av ROS-modul og ansvarlig er syk eller på reise
 - Tilsvarende problem med andre program i meldingskjeden til avsender
 - Tilsvarende problem med program i meldingskjeden hos mottaker
- Feil hos avsender oppdages som oftest først i kommunen

Erfaring med feilsendinger:

Meldinger blir feilsendt, f.eks. til feil kommune. Det hender også at sykehuset sender meldinger til kommunen om pasienter som verken har eller skal ha pleie- og omsorgstjenester etter utskrivning. Det er viktig å ha rutiner for håndtering av feilsendte meldinger. I Stavanger kommune går meldinger om pasienter som ikke finnes i journalsystemet fra før, automatisk til sentral e-meldingsansvarlig. Avvik meldes i passordbelagt vedlegg til e-post som sendes til avtalt adresse på sykehuset og følges opp der. Avvik noteres i eget dokument med tanke på statistikk.

Utfordringer:

Lovgivning er en utfordring. Kommunens tjenester til eldre er dels hjemlet i helsetjenestelov, dels i sosialtjenestelov. Disse lovene har ulike regler når det gjelder dokumentasjon av tjenesten og personalets adgang til å utveksle informasjon. Dette er særlig problematisk i forhold til bofellesskap.

Dokumentasjon er en annen utfordring. Det er krav om journalansvarlig i forhold til institusjoner, men det er ingen krav til journalansvarlig på kommunenivå, selv om de fleste kommuner benytter et felles journalsystem for hele kommunen. For å få gode dokumentasjonsrutiner ved bruk av EPJ, er det nødvendig med sentral journalansvarlig som har avgjørende innflytelse på dokumentasjonsrutinene i virksomhetene. Vi trenger lovgivning som pålegger dette.

Samhandling med eksterne er også en utfordring. Det er behov for bedre informasjons-overføring mht medisinerer. I første omgang er det behov for et medisinkort i innleggelsesrapport fra pleie- og omsorgssektoren, og tilsvarende fra lege. I neste omgang er det ønskelig med et medisinkort i kjernejournalen.

Det er også behov for bedre informasjon om tjenestestatus. Sykehus må kunne finne ut om en pasient har kommunale tjenester som har behov for informasjon fra sykehuset, f.eks. melding om innleggelse/akuttinnleggelse, utskrivningsrapport og tverrfaglig epikrise og melding om utskrivning eller død.

Eksempler på situasjoner der det er spesielt stort behov for bedre informasjonsutveksling er terminal pleie i hjemmet, psykisk utviklingshemmet i bofellesskap, på dagsenter og/eller på skole, pasient som er utskrevet fra sykehus og som pendler mellom hjem og sykehjem,

brukere på midlertidige sykehjems- eller rehabiliteringsopphold i Spania og brukere som har behov for individuell plan.

2.6 Helge Veum, Datatilsynet: [Datatilsynet og tilgang på langs](#)

Helge Veum er overingeniør i tilsyns- og sikkerhetsavdelingen i Datatilsynet.



Helge Veum innledet med å si: "Jeg er en av dem som er glad i §13". Datatilsynet liker hlsregl § 13 og tankegangen bak den. Men tilsynet forstår også at det er problemstillinger i det praktiske livet som kan være vanskelig.

Datatilsynet mener imidlertid at mye av samhandlingen kan løses innenfor de rammene vi har i dag. Veum mente at vi hadde fått ryddige presentasjoner av reelle problemstillinger på dette miniseminar. Han ser at mye kan løses ved hjelp av meldingsutveksling, men at metodene og løsningene må på plass for at det skal fungere. I forhold til Augestad og UNN anser han at mye av oppfølgingen kan gjøres ved meldingsutveksling. Nødinformasjon og akutte hendelser kan ikke i samme grad løses innenfor gjeldende lovgivning.

Datatilsynets roller er todelt i denne sammenheng

- fører tilsyn med gjeldende regelverk (tilsynsrollen)
- deltar i diskusjonen rundt morgendagens regelverk (ombudsrollen)

Datatilsynets ønske er at pasientens vern skal ivaretas. De ser også at det er god informasjonssikkerhet at informasjon er tilgjengelig når den trengs.

Deling av informasjon er greit der det er lov (i forhold til taushetsplikt), og elektronisk deling er selvfølgelig greit.

Men deling av informasjon gjennom å bruke felles data (tilgang til hverandres data) på tvers av organisasjoner, er uheldig. Det gir en ansvarsfragmentering. Det er ikke godt personvern at ansvaret er uklart med hensyn på korrekte, oppdaterte opplysninger og hvem som har ansvar hvis opplysninger kommer på avveie. Uklare ansvarsforhold undergraver reell kontroll. Deling av informasjon gjennom tilgang til hverandres data er også ulovlig i dag. Hlsregl § 13 setter de nødvendige skranker her, og hoveddelen av dem er fornuftige.

Datatilsynet ønsker at man i størst mulig grad gjør bruk av eksisterende prinsipper med forsendelsesbasert kommunikasjon som gir aktivitet hos avgiver for å vurdere hva som er nødvendig å sende fra seg. Dette kan løse de fleste utfordringer, f.eks. med tanke på kontrollkortet nevnt tidligere i seminaret.

Men man må se på hva som *ikke* kan løses med meldingsutveksling. I dag har man bl.a. behov innen

- geriatri

- kommunal-/primær-/spesialistsamarbeid
- kommunalt samarbeid (kommunal legevakt på tvers av kommuner)

Datatilsynet vil fokusere på å løse problemer primært med dagens lovgivning, og sekundært med lovendringer. Man vil uansett ha behov for strukturert informasjon og standardisering. Dette er fortsatt en utfordring. Man har kommet et stykke på henvisnings- og epikrise-sida, men ikke så langt når det gjelder standardisering av kommunikasjon av annen journal-informasjon. Dette må ikke bli en unnskyldning for å spasere inn og ut av hverandres journal-system. Vi har et viktig skille mellom virksomhetene. Skal vi

- lage de nødvendige åpningene – eller
- rasere skillet mellom virksomhetene

Det er mye som er vanskeligere enn kommunikasjon mellom store helseforetak. Men det er disse man hører mest fra. Man hører ikke like store rop fra kommunal sektor og i forhold til f.eks. individuell plan.

Tilsyn med hensyn på tilgangsstyring internt viser mange brudd i forhold til regelverket, og gir inntrykk av at "grunnmuren mangler". Helseforetakene har ikke tilstrekkelig kontroll internt i egen organisasjon. Er det da riktig å slippe andre inn?

En fullstendig nasjonal pasientjournal anses som et "worst case" fra et personvernspunkt. En begrenset kjernejournal kan være et alternativ, men ikke uten samtykke fra pasienten, og ikke som erstatning for ryddig kommunikasjon som må på plass innad i helsesektoren mellom de ulike virksomheter. Det er en lang vei å gå når det gjelder å utrede hvor mye og hvordan dette skal gjøres.

Sårbarhet i forhold til tilgjengelighet. Før hadde man kun avhengighet av eget system. Nå har man avhengighet av eget system, av andres system og av nettverk, f.eks. for at den nye e-Resept-løsningen skal fungere. Dette får nasjonale konsekvenser. Tilgjengelighet må få større fokus.

Når man samler mye informasjon følger alltid argumentasjonen om at man får større sikkerhet når man har sentrale løsninger. Men det skulle bare mangle at ikke sikkerheten er større når konsekvensen av sikkerhetsbrudd også blir større.

Oppsummering:

- Skillet vi har i dag har en hensikt
- Begrens endringer til der hvor de er nødvendige
- Hva blir konsekvensene av endringene – både i forhold til personvernet og helsehjelpen?

Spørsmål/kommentarer/diskusjoner som kom opp:

Fra salen ble det kommentert at det ikke er vanskelig å være enig i prinsippet, men et hakk vanskeligere i praksis... Det ble ikke sagt noe om løsninger ved akutsituasjoner. Hvor mange menneskeliv er det forsvarlig å miste per år for å ivareta personvernet? Og hva legges i begrepet begrenset kjernejournal? Når man utleverer informasjon i form av meldinger eller lignende får man kopier og leger kan ta beslutninger basert på informasjon som ikke lenger er "up to date". Denne bekymringen har vært reist.

Svaret på dette var at Datatilsynet vil være forsiktig med å uttale seg om hva som er nødvendig. Man forventer å høre de gode argumentene fra helsesektoren og helsemyndighetene.

I forhold til å samle inn informasjon fra andre, så er man forpliktet til å kontrollere om den informasjonen man har er oppdatert. Kanskje må kollegaen be om å få utlevert ny informasjon selv i stedet for å lese en kopi av det han eller hun har fått tidligere. Skal den som oppdager en allergisk reaksjon som tidligere ikke har vært kjent, være forpliktet til å oppdatere de som har fått utlevert informasjon tidligere? Man har sett på tilsyn at man får brist på dokumentasjonsplikten fordi journalsystemene er så åpne som de er i dag. Dette er vanskelige saker. Hva våger man å gi fra seg av informasjon hvis systemene er for åpne?

Når det gjelder akutsituasjoner bør vi kanskje snakke om kjernejournaler. Her er det kanskje viktig å la individet bestemme selv. Begrepet "begrenset kjernejournal" er nok smør på flesk:

En kjernejournal er begrenset. Datatilsynet er ikke klar til å gi tydelige anbefalinger. Kanskje pasienten skal bestemme, etter råd fra legen?

Det kom også en kommentar fra salen om problemet med redundans: Ved utlevering så vil (de utleverte) kopiene før eller senere kunne bli for gamle, bli utdaterte. En kommentar til dette var at det kanskje bør være en plikt å også utlevere alle oppdateringer etterpå.

Fra salen ble det spurt om de får informasjon om hvor hyppige akuttituasjonene er? Helge Veum svarte at de ikke har sett noen tall, men regner med at dette må komme på bordet.

Fra UNN ble det svart at det antakelig ikke er gjort noen undersøkelser på akkurat det. Behovet for akuttinformasjon er relativt sjelden, men *når* det er behov for det er det viktig. De gangene pasientene sendes ut fra sykehuset uten epikrise, f.eks. når de overflyttes til et annet helseforetak må man ringe og etterspørre informasjon, men dette tar for lang tid.

Til dette repliserte Helge Veum at da kan man jo stille spørsmål om hvorfor det ikke er sendt en ordentlig epikrise når den burde gå? Hvorfor setter man ikke inn kreftene her, i stedet for å gjøre drastiske nasjonale endringer som kan svekke personvernet? Vi må se på hva som egentlig er problemet.¹⁷

2.7 Ivar Berge, RRHF: [Min Journal - elektronisk kommunikasjon mellom pasient og spesialisthelsetjenesten](#)

Ivar Berge er rådgiver ved IT-avdelingen ved Rikshospitalet-Radiumhospitalet HF.



Min Journal er et samarbeidsprosjekt mellom flere helseforetak, ledet av Rikshospitalet-Radiumhospitalet HF (RRHF). Første skisse til løsningsbeskrivelse kom i 2002. Systemet har vært i drift siden høsten 2006, men foreløpig med svært begrenset omfang. Det er planlagt en betydelig utvidelse av bruken høsten 2007.

Det er flere grunner til at RRHF satser på dette nå:

- Etterspørsel fra pasientene
- Etterspørsel i egen organisasjon
- Positive erfaringer og dokumenterte effekter i andre land
- Naturlig konsekvens av satsningen på Klinisk Portal der samtlige systemer i organisasjonen integreres

¹⁷ Dette er eksempel på et tema som vi burde hatt tid til å diskutere i en avsluttende debatt

Sentrale elementer ved løsningen er bl.a. tanken om å ha "alt på ett sted", dvs. å lage en mest mulig foretaksuavhengig løsning slik at pasienter som behandles ved flere helseforetak skal slippe å forholde seg til flere portaler. Et annet sentralt element er sikkerhet. Under utviklingen har det vært høyt fokus på sikkerhet, tett dialog med Datatilsynet og samarbeid med bankene om PKI (eID/BankID). Man ville skape et robust, skalerbart og fleksibelt utgangspunkt å bygge videre på. Det har vært en viktig tanke at "One size doesn't fit all".

Løsningen er fleksibel og kan enkelt tilpasses ulike pasientgrupper, teoretisk helt ned på individnivå. Dette gjelder både innhold, tjenester og til en viss grad design. Brukerne kan også gjøre en del tilpasninger selv.

Pasientene er veldig modne og ivrige. Teknologien er grei og sikkerheten er bra. Organisasjonen er utfordringen. Det er mye usikkerhet og frykt og ulikt hvor langt de forskjellige avdelingene har kommet med tanke på å skulle ta dette i bruk.

Første versjon har følgende basisfunksjonalitet:

- Innholdspubliserings – kan tilpasses de ulike pasientgruppene
- Sikker og lovlig meldingsutveksling mellom pasient og spesialist, med varsel til ekstern e-postadresse. – Det er en kjent sak at "alle" helseforetak kommuniserer ulovlig med pasienter i dag.
- Skjemaer – anamnese med mer. Her er det mange anvendelsesområder, f.eks. skjemaer som sendes ut til pasientene i forkant av et besøk, pasienttilfredshetsundersøkelser mm. Det kan trekkes ut data som legges inn i klinikkens datasystemer. I dag ligger det skjema på web'en hvor man kan endre, avlyse eller bestille time elektronisk. Det er ingen autentisering, men skjemaet forsvinner fra web-sida når det er utfyllt, og behandles manuelt internt.
- Vedlikehold av egen kontaktinformasjon for pasienten
- Dagbok for pasienten

RRHF har mange aktiviteter rundt Min Journal i 2007. Noen av dem er:

- "Blodspor": Innrapportering fra blødere
- Lipidklinikken – SmartDiet-skjema – har en spesiell løsning for å lage skjemaet. Kliniker og pasient kan sitte sammen og se på skjemaet.
- Cochlea/hørselsentralen
- Transplantasjon – pasienter med et langvarig og komplekst forløp. Vil jobbe med koordinering av forløpet.
- Integrasjon med Klinisk Portal, et annet av RRHF sine systemer.
- Epikrise – ønsker å tilby alle polikliniske pasienter elektronisk epikrise inneværende år.
- Bestilling av journalkopi. Det koster kr 900 pr journalkopi, men sykehuset får refundert kr 250. Trenger ikke nødvendigvis sende ut hele journalen og kan ha en dialog på hva pasienten trenger.

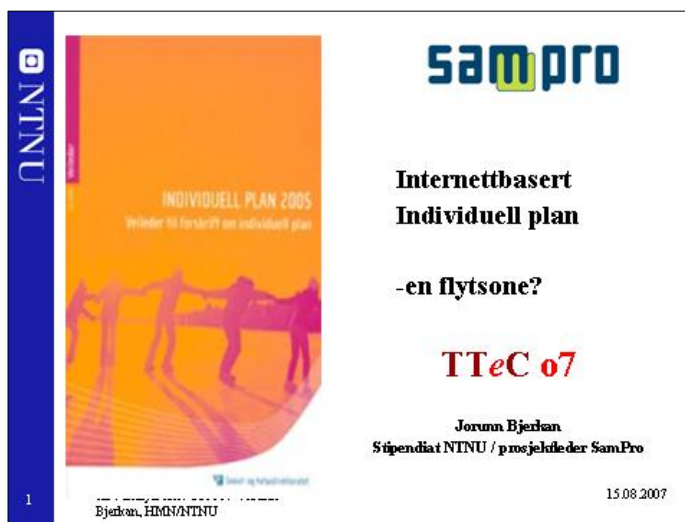
Innføringen av Min Journal har vist noen spesielle problemområder:

- Frykt og skepsis hos mange i organisasjonen. Mange er redd for å bli nedlesset av e-post, noe som har vist seg å ikke være tilfelle. Man vil gjøre en grundig dokumentasjon av løsningen for blødere for å vise at man kommer ut i pluss. Det er ikke så vanskelig å oppdra pasientene med hensyn på hva de kan sende til hvem.
- Ansvarsfordelingen mellom leddene i helsetjenesten. Spesielt har man sett dette når det gjelder premature barn som går mellom ulike foretak over en periode.
- Økonomi – hvem skal betale for hva, f.eks. autentiseringsløsningene og eID-kortene?
- Forvaltning – stor grad av desentralisering er nødvendig, og god opplæring ute i avdelingene samt klare ansvarsforhold. Den som sender en melding *må* få svar.
- Kobling mellom Min Journal-bruker og pasient – spesielt i forhold til barns journal. Innlogget bruker må kobles med rett pasient. For en del foreldre skal tilgangen til barnas journal opphøre ved fylte 18 år, for andre ikke.

Dette produktet er ikke til salgs. Alle som ønsker å delta er velkommen til å delta, spesielt innenfor opplæring og mestring.

2.8 Jorunn Bjerkan, NTNU: [Internettbasert individuell plan - en flytsone?](#)

Jorunn Bjerkan er stipendiat ved NTNU, og sykepleier med Master of Information Technology in Healthcare. Hun er også prosjektleder for SamPro.



Individuell plan (IP), hva skal det være? Kun Norge har lovfestet rett til IP. Mange blander sammen den individuelle planen med rehabiliteringsplaner og pleieplaner. Det skal kun være én individuell plan per tjenestemottaker. Tjenestemottakeren skal ha en fast koordinator. Alle som har behov for langvarige og koordinerte tjenester har rett til å få utarbeidet en individuell plan.

Det er mange generelle utfordringer knyttet til bruk av IP. Riksrevisjonens rapport, helse-tilsynsrapporter og forskningsrapporter viser at IP i liten grad er etablert, og det er lite kunnskap om IP i kommunene og helsesektoren. De planene som er etablert er ulikt oppdatert og i ulik grad distribuert til samhandlingsaktørene. Tjenestemottakerne har ofte manglende innsyn i egen IP.

Produktet Unique SamPro ble laget som en internettbasert løsning for individuell plan. Den skulle være internettbasert og tilgjengelig utenfor helsenettet for at pasientene og NAV, skoler m.fl. skulle få tilgang. Den er nå i drift i kommersiell fase (driftes av Hemit). Løsningen har differensiert tilgangskontroll og sterkt fokus på sikkerhet. Leverandøren har ventet på den nasjonale PKI-løsningen, men har måttet velge noe annet i mellomtida. Det har vært jobbet mye med å få på plass dokumentasjon av ansvarsforhold, hvem som er koordinator, etc.

Prosjektet SamPro i Helse Midt-Norge RHF var en pilot som gikk over to år i fem kommuner. Det har blitt kjørt en iterativ prosess med flere runder med utprøving og videreutvikling.

Noen av erfaringene og utfordringene ved tjenestemottakernes bruk av Unique SamPro har vært:

- IP er ikke lenger bare tjenesteytternes verktøy
- Flere brukere er egne koordinatører
- Teknologi til glede og besvær
 - kreativ bruk av løsningen
 - e-terapi og dagbok
 - frafall av hele grupper eller enkeltaktører

Brukerne vil ha enkle verktøy, gode utskrifter, enklere pålogging enn i dag. Frafallet har skyldtes praktiske, organisatoriske og andre årsaker. Der bruker og koordinator samarbeider tett, fungerer løsningen bra.

Det har vært mange tekniske utfordringer i utviklings- og pilotfasene, som bl.a. netthastighet (har variert fra analoge linjer til høyhastighetslinjer), ulike nettlesere, pop-ups, påloggingsproblemer, bruk av mobiltelefon, pc-tilgang/internetttilgang og ulik kompetanse på IKT-bruk blant ansatte.

Organisatoriske utfordringer generelt og i Unique SamPro har vært av ulike typer, både relasjonelle, faglige og administrative. Man kan f.eks. få en endring av maktbalansen, det kan være uenighet mellom fagfolk og tjenestemottaker og det kan være en synlig uenighet mellom fagfolkene i ansvarsgruppene. Andre spørsmål som reiser seg er om kommune/sykehus har ansvar juridisk for det de ikke selv har skrevet. Og hva med dokumentasjonsplikten? Hvem skal skrive hva i SamPro? Hvem skal betale hva av en lisens som ligger og flyter mellom nivåene? Andre problemstillinger kan være at etatene ofte har lav planleggingskompetanse og lav samhandlingskompetanse.

Man møter også juridiske utfordringer, som:

- tilgangskontroll/samtykke
- ansvar i henhold til journalføringsplikten
- ansvar for innhold og gjennomføring
- eierskap til data – er det pasienten eller planeier som eier dataene?
- hvor går sensitivitetsgrensen når pasienten selv skriver?
- uklarhet mellom SHdir, Datatilsynet og Helse- og omsorgsdepartementet

Man ser en tendens til en glidende overgang fra Behandlingsplan til IP og videre til Egenjournal.

2.9 Vigdis Heimly, KITH: [Samtykkebasert kjernejournal](#)

[Vigdis Heimly](#) er sjeffrådgiver ved KITH (Kompetansesenter for IT i helse- og sosialsektoren AS). Hennes hovedkompetanse er innen elektronisk samhandling, helsenet, prosjektledelse, samhandlingsprosesser og nordisk og øvrig internasjonalt samarbeid.



Presentasjonen omhandlet først og fremst fyrtårnprosjekt for kjernejournal for medisinkort. Det ble også sagt noe om hvordan dette kan utvides til en nasjonal løsning.

Hovedaktører i prosjektet er Trondheim kommune med prosjektene Fyrtårn Trondheim og SUMO-prosjektet, Nasjonalt senter for telemedisin med prosjektet Nettbasert legemiddelkort og Stavanger kommune med prosjektet Fyrtårn Stavanger.

Dette er et stort nasjonalt prosjekt med mye oppmerksomhet. Samtlige journalleverandører i Norge er med i prosjektet. Det er også samarbeid med Elin-prosjektene, NSEP, KITH, e-Resept-prosjektet og NAF-Data.

Bakgrunnen for prosjektet er at feilmedisinering er et stort problem i primærhelsetjenesten. Kartlegginger har påvist feil i mer enn halvparten av medisinkortene. Legemiddelopplysninger i epikriser er også til dels svært mangelfulle. Reduksjon av feilmedisinering kan resultere i færre dødsfall, reduserte lidelser hos pasientene og gi et årlig innsparingspotensial på 3 mrd kroner pr år.

Med unntak av de perioder en pasient mottar behandling fra spesialisthelsetjenesten, har fastlegen det overordnede medisinske ansvaret for pasienten. For at fastlegen skal kunne ivareta dette ansvaret, må andre behandlere utlevere nødvendige opplysninger vedrørende pasientens bruk av legemidler mv. Fastlegen utleverer også opplysninger til andre som yter helsehjelp, f.eks. til den kommunale pleie- og omsorgstjenesten. Helseopplysninger kommuniseres på papir, muntlig, og noe også elektronisk, mellom fastlegen og andre som yter pasienten helsehjelp. Kvaliteten er variabel. Ofte må behandler trekke konklusjoner på mangelfullt oppdaterte opplysninger.

Prosjektet "Samtykkebasert kjernejournal"

Med samtykkebasert kjernejournal ønsker man å oppnå følgende forbedringer:

- Opplysninger *til* fastlege
 - Utleveringen må skje betydelig raskere
 - Kvaliteten av opplysningene må bli bedre

Målet er at fastlegen skal få utlevert opplysninger om alle forskrivninger så fremt pasienten gir sitt samtykke. For å oppnå dette bør opplysninger om legemidler utlevert på resept overføres fra apotek til fastlege

- Opplysninger *fra* fastlege

Når det foreligger en forespørsel om utlevering som er dekket av et samtykke pasienten har gitt, skal utlevering kunne skje uten manuell behandling fra fastlegens side

Tre legesenter i Trondheim med fire fastleger per senter deltar i prosjektet. Hver lege har 10-15 pasienter som kommunen administrerer legemidlene for.

For å muliggjøre utlevering av journalopplysninger uten eksplisitt godkjenning av fastlegen i hvert enkelt tilfelle, må det etableres et system som sikrer at:

- Det ikke kan utleveres andre opplysninger enn det pasienten har samtykket til
- Fastlegen har full kontroll med den enkelte utlevering
 - Hvilke opplysninger som skal kunne utleveres
 - Til hvem opplysningene skal kunne utleveres

Denne løsningsmodellen er gitt betegnelsen "Samtykkebasert kjernejournal". Den inneholder kjerneopplysninger fra journalen. Opplysningene behandles i henhold til pasientens samtykker.

Fastlegen er databehandlingsansvarlig for EPJ og dermed også for kjernejournalene. For fastleger som ikke er selvstendig næringsdrivende, blir den virksomhet de er ansatt i, databehandlingsansvarlig. For å sikre at kjernejournalene er tilgjengelig hele døgnet, etableres det en kopi av denne hos en ekstern databehandler. Fastlegene som deltar i Fyrtårn Trondheim inngår en databehandlingsavtale med Trondheim kommune.

Etablering av kjernejournal er et tilbud til pasienter med spesielt behov, dvs. de pasienter hvor kommunen har overtatt ansvaret for administrering av legemidler (10 – 15 pr. deltagende fastlege). På sikt kan tilbudet bli gitt også til andre grupper.

Fastlegen informerer pasienten om hva etablering av en kjernejournal innebærer. Beslutning om hvilke utleveringer som skal tillates tas av fastlegen og pasienten i fellesskap. Det vil ikke bli tillatt utleveringer i andre situasjoner enn de som pasienten har gitt sitt eksplisitte samtykke til.

Om den tekniske løsningen:

- Den som har behov for opplysninger sender en e-Melding med forespørsel om utlevering. Dette er en egen funksjon i EPJ-systemet.

- Dersom det foreligger beslutning om utlevering som dekker situasjonen, utleveres opplysningene. Utleveringen skal skje automatisk som et svar på forespørselsmeldingen.
- Utleveringen registreres automatisk i EPJ.
- Det utvikles funksjonalitet for kommunikasjon med kjernejournalen i "alle" EPJ-system.
- Ved bruk av web-services vil svaret på en forespørsel kunne komme "umiddelbart".

Nasjonal kjernejournal?

Statsråd Sylvia Brustad uttalte i Stortingets spørretime 6. februar 2007:

- [...] Vi trenger også, slik vi ser det, felles informasjons- og kommunikasjonsløsninger som legger til rette for at aktørene i tjenesten skal ha tilgang til oppdatert informasjon i møte med bruker og pasient. Det kan bl.a. gjøres ved at vi oppretter en såkalt nasjonal kjernejournal [...]

og 29. mars 2007:

- [...] Å opprette en nasjonal journal vil kunne bidra til å bedre kvaliteten i behandlinga ved at helsepersonell får tilgang til kritisk pasientinformasjon på tvers av helseforetak og nivåer i helsetjenesten vår.
- En nasjonal journal kan inneholde opplysninger om hvor opplysninger finnes, og den kan inneholde deler eller hele den individuelle pasientjournalen [...]

Fyrtårn Trondheim utvikler en generell løsning som kan danne grunnlaget for en nasjonal kjernejournal:

- "Alle" EPJ-system får nødvendig funksjonalitet for kommunikasjon med kjernejournalen
- "Alle" dokumenttyper vil kunne håndteres
- Kun allmennlegenes EPJ-system får nødvendig funksjonalitet for administrasjon av kjernejournaler

Kjernejournalssystemet kan håndtere alle typer dokumenter så lenge disse "pakkes inn" iht. standarden. I kjernejournalen lagres dokumentene på det format de mottas, og de utleveres på samme format. Begrensinger ligger kun i de systemer som skal kommunisere med kjernejournalen og som skal håndtere innholdet.

Pasienten bør kunne være en aktiv aktør i forbindelse med bruk av kjernejournal. Pasienten bør få tilgang til kjernejournalen, f.eks. gjennom "Min side". Pasienten bør kunne føre en egenjournal som kan inngå som en del av kjernejournalen, og pasienten bør kunne registrere regler for hvem som skal få tilgang til opplysninger fra kjernejournalen. Men pasienten kan ikke stå helt fritt her. Det må sikres at utvalget av opplysninger det gis tilgang til ikke gir et så misvisende bilde at det medfører fare for feilbehandling.

Gravide bør kunne få tilgang til "helsekortet" gjennom en kjernejournal-løsning.

Innhold i en nasjonal kjernejournal vil kunne være:

- Opplysning om hvem som fører journal for pasienten, med episodedata som indeks til de enkelte journaler
- Opplysninger relatert til legemiddelbruk
- Cave, allergier, blodtype, etc.
- Opplysning om enkelte kroniske sykdommer
- Opplysning om eventuelle "aktive" henvisninger
- Kontaktinfo fastlege og annet relevant helsepersonell
- Nærmeste pårørende m/kontaktinformasjon
- Eventuelle reservasjoner mot bestemte behandlingsformer
- Opplysning om organdonasjon

Spesielle anvendelser for en nasjonal kjernejournal kan være individuell plan, helsekort for gravide og egenjournal.

Forslag til endringer i hlsregl §§ 6 og 13

KITH sendte 25. september 2006 et brev til SHdir med kopi til HOD med flere hvor det ble påpekt en del problemer med helseregisterlovens §§ 6 og 13, og kom med forslag til justeringer. KITH har så langt ikke fått svar på henvendelsen...

Her er KITHs forslag til endringer (ny tekst står i kursiv):

§ 6 Behandlingsrettet helseregister

- Behandlingsrettede helseregistre kan føres elektronisk. Det skal fremgå av registeret hvem som har registrert opplysningene. Dette kan gjøres ved hjelp av elektronisk signatur eller tilsvarende sikker dokumentasjon.
- Regionale helseforetak og helseforetak, kommune og annen offentlig eller privat virksomhet som tar i bruk behandlingsrettede helseregistre, er databehandlingsansvarlig for opplysningene. Foretaket og kommunen kan delegere databehandlingsansvaret.
- *Virksomheter som samarbeider om å ivareta oppgaver etter apotekloven, kommunehelsestjenesteloven, sosialtjenesteloven, tannhelsestjenesteloven, smittevernloven eller spesialisthelsestjenesteloven kan benytte et felles behandlingsrettet helseregister dersom oppgavens art gjør dette formålstjenelig. Virksomhetene må i så fall skriftlig avtale seg imellom hvem som skal være databehandlingsansvarlig for det felles helseregistret.*

§ 13 Tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon:

- *Tilgang til helseopplysninger i behandlingsrettet helseregister kan gis når dette følger av lov og tilgangen ikke er forbudt ved annet særskilt rettsgrunnlag.*
- *For øvrig kan bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, gis tilgang til helseopplysninger. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt.*

Oppsummering:

- Fyrtårn Trondheim utvikler en generell løsning for regelstyrt, rask og sikker utlevering av EPJ-opplysninger
 - til helsepersonell med legitimt behov
 - i tråd med de samtykker pasienten har gitt
- "Alle" leverandører implementerer ny funksjonalitet i EPJ-systemene for kommunikasjon med kjernejournalen
- Løsningen er fleksibel. Den kan lett utvides med nye typer informasjonsinnhold og nye regler for samtykkebasert utlevering. På sykehus kan kjernejournalene håndteres av EPJ-systemet
- Det er behov for en nasjonal tjeneste for videreformidling av forespørsler om utlevering fra kjernejournal

3. Avsluttende diskusjon

I stedet for den planlagte paneldebatten ble det bare tid til en kort oppsummerende diskusjonsrunde.

Hilde Jordal påpekte at SHdir har to roller: Utarbeide nye lover og forvalte regelverket. Å fortolke regelverket og utarbeide rundskriv er en viktig del av dette arbeidet.

Man må ikke tro at det å åpne opp for direkte tilgang gjør alt enklere. Det er mulig i dag å holde seg innenfor lovverket. Mange sier det er vanskelig å få ting utlevert. En årsak kan være at HF-ene har bygd ned arkivorganisasjonen og bemanningen som trengs for å få utlevert nødvendig informasjon slik at andre virksomheter kan utføre sitt arbeid på en forsvarlig måte. Direktoratets pågående prosjekt skal ikke føre til at man kan svitsje mellom det ene og det andre uten videre.

Knut Magne Augestad presiserte at han er opptatt av hvordan ting fungerer i dag i det praktiske liv. Du finner ikke et eneste foretak som har egne ansatte for å finne fram journalopplysninger som andre ber om. Eneste mulighet er å ringe til vakthavende lege hos dem man trenger informasjon fra.

Jorunn Bjerkan sa seg enig med både Datatilsynet og SHdir. Man skal være varsom med å åpne opp for mye. Hun hadde ikke inntrykk av at det er ønske om å åpne ukritisk. Det er en bevissthet rundt dette, men det finnes noen dårlige organisatoriske rutiner. Man må finne løsninger som fungerer i praksis og som ivaretar personvernet samtidig som brukerne får tilgang til det de trenger.

Hilde Jordal kommenterte at hun forstår godt klinikerne som bare finner eksempler på løsninger som ikke er gode nok. SHdir har forutsatt i rundskriv at det skal legges til rette for at utlevering kan skje på en rask måte.

4. Oppsummering og evaluering

4.1 Oppsummering

Det kan se ut til at helseregisterloven § 13 er under sterkt press for tiden. Det nødvendiggjør viktige diskusjoner.

Ett svært viktig spørsmål er hvordan man skal sikre pasientopplysningene tilstrekkelig dersom hlsregl § 13 endres slik at andre enn de som står under databehandlingsansvarliges instruksjonsmyndighet gis direkte tilgang inn i EPJ-systemer. Dette kan føre til at ansvarsforholdene rundt sikring av pasientopplysninger blir uklare. Finnes det andre måter å etablere klare ansvarsforhold og betryggende ordninger på enn hva som er tilfelle i dag?

Det er også nødvendig å få et klarere bilde av hva behovet er for tilgang inn i andre virksomheters EPJ-systemer. Det er viktig å presisere hva slags tilgang det er snakk om (lese- og/eller skrivetilgang). Dette må ses i sammenheng med målsettingen med tilgangen, ulike situasjoner, ev. konsekvenser av manglende tilgang, mv. I denne forbindelse kan en også reflektere over hvorvidt diskusjonen om behovet for tilgang helt eller delvis er oppstått og blitt så engasjerende fordi vi ikke klarer å få de ordninger vi har til å fungere. Vi har hørt kommunale helsearbeidere si at gode epikriser til rett tid og pålitelig informasjon fra spesialisthelsetjenesten om hvilke medikamenter pasienten skal ha, ville føre til at de ikke ville ha behov for eller ønske om tilgang inn i andre virksomheters journaler. Dette synspunktet er godt egnet som utgangspunkt for refleksjon rundt temaet.

Det gjør også inntrykk når Datatilsynet beskriver hvor dårlig tilgangsstyringen fungerer *internt* i virksomhetene i spesialisthelsetjenesten. Det er et spørsmål hva man da gjør når man i tillegg snakker om å slippe ansatte i andre virksomheter inn i disse systemene med den økte sikkerhetsrisiko det medfører.

Husk også invitasjonen fra Hilde Jordal til å komme med innspill til det pågående arbeidet med å vurdere lovendringer.

Det ble i løpet av miniseminalet uttalt at helsepersonell ikke bryr seg så mye om å diskutere farene ved "tilgang på tvers". De er først og fremst opptatt av å gi pasientene best mulig helsehjelp og derved opptatt av å få den informasjon om pasienten de trenger for at denne skal bli best mulig. Dette fikk vi dessverre ikke tid til å diskutere. Vår oppfatning er at helsepersonell gjennomgående er sterkt opptatt av taushetsplikten og å sørge for at pasientopplysninger ikke havner på avveier. Diskusjonen om klare ansvarsforhold rundt behandlingen av pasientopplysninger som sikrer det samme, er dermed meget godt egnet til å engasjere helsepersonell i alle deler av helsevesenet. Deres oppfatninger kunne utvilsomt være til stor nytte for de i Sosial- og helsedirektoratet som for tiden arbeider med disse spørsmålene. Det samme tror vi også gjelder pasientenes synspunkter.

4.2 Evaluering

Deltakerne på miniseminalet fikk levert ut et enkelt evalueringsskjema. Det inneholdt spørsmål om de var blitt tilført noe nytt, om de hadde forslag til andre problemstillinger som burde vært tatt opp, om de hadde formening om hvordan temaet skulle følges opp videre og om deres mening om form og gjennomføring av miniseminalet. Vi mottok ni svar, noe som ikke er tilstrekkelig for å trekke bastante konklusjoner, men som likevel kan danne grunnlaget for en "stemningsrapport".

Positive tilbakemeldinger

Det ble gitt gjennomgående positive tilbakemeldinger på at både Datatilsynet og Sosial- og helsedirektoratet redegjorde for status i sitt arbeid og bidro til å "løfte" problemstillingene. Kombinasjonen av dette og praktiske eksempler var godt egnet. Det var generelt sett bra at miniseminalets program var sammensatt slik at kompleksiteten rundt "tilgang på langs" ble godt belyst. Det var en god blanding av utøvende nivå med erfaringer og løsninger opp mot rammer og føringer. Det kom godt frem at det er mange som har roller og ansvar i dette. Det var også interessant å høre om praksis i de andre nordiske land.

To sitater:

"Beste seminaret under TTeC."

"Før skrek vi at noe måtte gjøres, nå snakker vi om hvordan det skal/må gjøres."

Forbedringspotensialer

Vi fikk gjennomgående kommentarer til at lokalet var uegnet og at det skulle vært servert noe å bite i. Det ble også pekt på at det ble for dårlig tid, at tidsrammene ikke ble tilstrekkelig fulgt opp og at det ikke ble tid til diskusjon. Programmet var i utgangspunktet for stramt satt opp. En av deltagerne pekte også på at markedsføringen av miniseminalet hadde vært for dårlig.

Forslag til fremtidige temaer

- Oppfølging av Sosial- og helsedirektoratets pågående vurdering av og forslag til nødvendige lovendringer som gjør at informasjon kan deles eller gjøres tilgjengelig for behandlende helsepersonell i og mellom helseforetak, i og mellom private sykehus og i og mellom private sykehus og helseforetak, herunder vurdering av ansvarsforhold for pasientopplysningene. Hvilke problemer vil dette løse, hvilke ikke?
- Om Datatilsynenes rolle i de øvrige nordiske land og oversikt over deres ordninger rundt elektronisk formidling av pasientopplysninger.
- Diskutere tilgang til pasientopplysninger med utgangspunkt i kommunehelse-tjenesten praktiske hverdag og deres behov.

- Viktig å holde temaet varmt, så det ikke blir for stor avstand mellom de som yter tjenestene og det rammeverket de skal virke innenfor.

4.3 Videre arbeid

Vi planlegger å følge opp denne problematikken videre overfor de samme målgruppene, i første omgang med utgangspunkt i kommunehelsetjenestens virkelighet, da diskusjonene hittil i hovedsak har hatt sitt utgangspunkt i spesialisthelsetjenestens behov.

Det er en forutsetning at representanter fra sentrale helsemyndigheter og Datatilsynet vil delta.

Tilbakemeldingene tilsier at vi er på rett vei når det gjelder sammensetningen av programmet, men at vi må være mye mer nøye med å sette opp en realistisk tidsplan og følge den opp. Folk vil gjerne ha god tid til å diskutere. Det vil bli lagt stor vekt på å skaffe et godt egnet lokale.

Vi må også sørge for et opplegg for en målrettet og god markedsføring.

Abbreviations / Forkortelser

This list contains explanations for most of the abbreviations used in this report. Note that several of these abbreviations also have other meanings, in other contexts.

ABAC	Attribute-based access control
AMC	Academic Medical Centre (Amsterdam)
BIF	Bastjänster för Informationsförsörjning (English: BIP)
BIP	Basic services for Information Provision (Swedish: BIF)
CASSTM	Administrative Commission on Social Security for Migrant Workers
CEA	Karsinoembryonalt antigen (protein som viser forhøyet nivå i blodprøve ved CRC)
CEN	European Committee for Standardisation
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and related Technology
CRC	Colo-Rectal Cancer (kreft i tykktarm/endetarm)
EDIFACT	Electronic Data Interchange For Administration, Commerce, and Transport
e-EHIC	Electronic EHIC
EHIC	European Health Insurance Card
EHR	Electronic Health Record (Norwegian: EPJ)
eID	Elektronisk ID
ENT	Ear, Nose and Throat
EPJ	Elektronisk pasientjournal (Engelsk: EHR)
e-TEN	(type of projects in EU's FP7)
ETSI	European Telecommunications Standards Institute
FP7	Seventh Framework Programme (EU's 7. rammeprogram for forskning)
HF	Helseforetak
HIPAA	Health Insurance Portability and Accountability Act (USA)
HIT	Arena for helse, innovasjon og teknologi
hlsregl	Helseregisterloven
hlspl	Helsepersonelloven
HOD	Helse- og omsorgsdepartementet
ICT	Information and Communication Technology (Norwegian: IKT)
ID	Identifikator (English: Identifier)
IKT	Informasjons- og kommunikasjonsteknologi (English: ICT)
INFSO	INFormation SOciety
IP	Individuell plan
IP	Integrated Project (type of projects in EU's FP7)
ISO	International Organisation for Standardisation
ISSP	Information System Security Policy
ISSS	Information Society Standardization System
IT	Informasjonsteknologi (English: Information Technology)
ITIL	IT Infrastructure Library
ITS	Intelligent transport systems and services
KITH	Kompetansesenteret for IT i Helse- og sosialsektoren

KOLS	Kronisk obstruktiv lungesykdom
MD	Medical doctor
NAV	Arbeids- og velferdsforvaltningen i Norge
NFC	Near-Field Communication (type of RFID tag)
NFR	Norges forskningsråd (English: The Research Council of Norway)
NOU	Norges Offentlige Utredninger
NPÖ	Nationell patientöversikt (<i>Sverige</i>)
NSEP	Norsk senter for elektronisk pasientjournal
NST	Nasjonalt senter for telemedisin (English: Norwegian Centre for Telemedicine)
NTNU	Norges teknisk-naturvitenskapelige universitet
OASIS	Organization for the Advancement of Structured Information Standards
PC	Personal Computer
PKI	Public Key Infrastructure
PLO	Pleie- og omsorgssektoren
R&D	Research and Development
RFID	Radio Frequency Identification
ROS	Risiko og sårbarhet
RRHF	Rikshospitalet-Radiumhospitalet HF
SAML	Security Assertion Markup Language (an OASIS standard)
SHdir	Sosial- og helsedirektoratet
SITHS	Säker IT i Hälso- och Sjukvård (Swedish national healthcare security project)
6-Sigma	(a set of practices developed to systematically improve processes by eliminating defects)
SOA	Service-Oriented Architecture
SOX	Sarbanes-Oxley Act (<i>USA. This act defines which records are to be stored and for how long. The legislation also affects the IT departments whose job it is to store a corporation's electronic records.</i>)
SW	Software
TTeC	Tromsø Telemedicine and eHealth Conference
UNN	Universitetssykehuset Nord-Norge
VPN	Virtual Private Network
WSII	WebSphere Information Integrator
XACML	eXtensible Access Control Markup Language (an OASIS standard)