



Report on identified legal issues of the Baltic eHealth project

Leif Erik Nohr
On behalf of the
Baltic eHealth Legal Group



Title: **Report on identified legal issues of the Baltic eHealth Project**

Authors: Leif Erik Nohr, Legal Advisor, Norwegian Centre for Telemedicine, Norway
Leif.erik.nohr@telemed.no
Manolis Nymark, Legal Advisor, Socialstyrelsen, Sweden
Manolis.Nymark@socialstyrelsen.se
Marika Zmenja, Legal Advisor, East-Tallin University Hospital, Estonia
marika.zmenja@itk.ee
With contribution from other members of the Baltic eHealth Project www.baltic-ehealth.org

Number of pages: 28

This report may be freely distributed as long as the source is stated. The user is encouraged to state the name of the report, that it is published as part of the Baltic eHealth Project, and also that the report in its entirety is available at www.baltic-ehealth.org.

Preface

This report is a first deliverable from the legal group of the Baltic eHealth Project. The Baltic eHealth project is part-financed by the European Union (European Regional Development Fund) within the BSR Interreg III B programme.

This report aims at identifying some of the most important legal issues and problems which the project raises. The report is based on general knowledge of issues usually relevant for projects like this and feedback and discussions from members of the Project, both the lawyers and others. At the meetings and workshops where members of the legal group have attended, legal issues have frequently arisen. This both shows that these issues are important and crucial in the world of telemedicine and eHealth, and it shows that the project partners have been genuinely interested in these issues and in discussing them.

We have not covered all imaginable issues or questions in this report. Someone once compared legal issues in telemedicine with peeling an onion; there is always another layer. It has been necessary to concentrate our efforts on the issues we believe to be most important, and try to discuss these more in depth. The second deliverable from this group will be a set of guidelines on legal issues that we hope can further clarify some aspects. We also aim at making the guidelines more dynamic in the sense that they can be subject to changes based on experience from using them in "real life".

We hope that this report can serve as reference, that it might create awareness on issues the reader might not have considered before and that it might trigger discussions. Telemedicine and eHealth is still a field of massive and rapid development and this is obviously affecting legislation and legal issues. In that sense, this document is more of a status report on how we consider the situation as of today.

Tromsø, Norway, June 22nd 2005

Leif Erik Nohr

On behalf of the Legal Group of the Baltic eHealth Project

Table of contents

1.	On Legal Issues in General	5
2.	Privacy, Confidentiality and Data Security	6
2.1	The issue	6
2.2	Problems and challenges	7
2.3	On health networks	10
2.4	Project specific issues	10
2.5	Further actions.....	11
3.	Responsibility	12
3.1	The issue	12
3.2	Official legal interpretations	13
3.3	Project specific issues	15
3.4	Further actions.....	15
4.	Licensure	16
4.1	The issue	16
4.2	Questions.....	16
4.2.1	Is there a need for a special license in telemedicine/eHealth?	17
4.2.2	In what country must a doctor be licensed?	17
4.3	Further actions.....	19
5.	Patients' Rights.....	20
5.1	The issue	20
5.2	Patients' rights in the Baltic eHealth project.....	20
5.3	Further actions.....	21
6.	Reimbursement/payment	22
6.1	The issue	22
6.2	Further actions.....	22
7.	Contract issues.....	23
7.1	Further actions.....	23
8.	Informed Consent	24
8.1	The issue	24
8.2	Requirements for valid consent.....	24
8.2.1	Personal competence.....	24
8.2.2	Unrestrained	24
8.2.3	Information.....	24
8.3	Formal requirements. Consent forms and documentation	25
8.4	Withdrawal	25
8.5	Consent is not a contract.....	26
8.6	Project specific issues	26
8.7	Further actions.....	27

1. On Legal Issues in General

It might be useful to start off with a few words on working with legal issues in eHealth in general. This project, as many other within the field of telemedicine and eHealth, tend to regard law – regulations – as *barriers*, at the outset. The main purpose of the contribution of legal experts is often (usually?) to send them out on a mission to find and remove legal barriers as they stand in the way of the development and/or use of a given solution or service.

We have deliberately chosen to name this a report on legal *issues* rather than barriers as we believe that legislation and regulations should not be considered as barriers, at least not at the outset. National and international legislation on health care and data processing is the framework we have to work within if we shall have any hope in keeping up legitimacy and acceptance for the work we do. It is true that developing and expanding technological innovations challenge existing frameworks – legal and other, but we believe that the most fruitful approach in conjunction with this project is to work towards finding solutions that can exist within existing laws and regulations. One should not lose sight of the fact that existing legislation is based on principles and considerations that are important and essential for the whole aspect of health care provision.

Our task should be to identify and clarify the legal issues that are relevant for this project. Hopefully we will find that much of what we plan to do can be done within existing legislations. But naturally, if we find “real” legal *barriers* to further development of our services, it should be our duty to point them out and to suggest solutions to overcome them.

2. Privacy, Confidentiality and Data Security

2.1 The issue

These issues stand out as some of the most important in the whole area of telemedicine and eHealth. The health care sector is a massive producer of information and is strongly dependent on information of different kinds and from different sources to be able to function. On top of this, most of this information is considered sensitive. A doctor – patient, patient – nurse or client-provider relationship is based on trust and at the core of this base is confidentiality. The provider is dependent on the information given by the patient or client and the patient/client rely on that the provider will consider the information given as confidential. Confidentiality is a core “virtue” of any provider of care and/or help to patients or clients.

The professional duty of confidentiality is regulated under national health acts and/or health personnel acts. As an example, the Norwegian Health Personnel Act (Helsepersonelloven) states in its article 21 that:

“Health personnel shall prevent others from gaining access to or knowledge of information relating to people’s health or medical condition or other personal information that they get to know in their capacity as health personnel.”
(Official translation)

This article impose both an active and a passive duty on health care personnel; both a duty to actively protect such information and a duty not to give out such information, being it orally or otherwise. And the Norwegian Patients Rights Act establishes confidentiality as a right for the patient.

Similar legal provisions can be found in most countries. In a way it can be said that this is the legal standard or requirement that organisations, routines and technology must meet. eHealth solutions must provide levels of security and safety that meets these legal requirements and enables personnel to use the solutions without the risk of breaching an important professional duty.

Regulations on data processing have relevance in health care when it comes to processing of information, and especially in terms of processing by electronic means. Under the Data Processing Directive and national Data Processing legislation, one needs a legal foundation for processing of health information. Such a foundation is found in health care legislation, especially in relation to provisions on medical-/health records and exchange of information.

Another important aspect of this issue, that one may find less debated, falls under the category “safety”. This encompasses more than safety from unauthorized intrusion to systems but adds the aspect of keeping information safe, making sure that the stored information is valid and true and having it stored in a way that makes it possible for an authorized person to access it. Imagine a network. It contains *confidential* information in one way or the other, free of use for privileged users e.g. on a Right-to-Know-basis. The network is however encapsuled in a “steelcage” of administrative, physical and

technical security measures, thus making the information *safe* for non-privileged users.

The right to privacy is considered a Human Right. The right to privacy is derived from the notion of individual autonomy and integrity. Respecting and enhancing (in our case) patients' and clients' rights to privacy is showing respect for personal integrity and autonomy.

Introducing "e-solutions" to health care should not jeopardize any of these important principles. Hardware, software and communication need to be built and used in a way that secures information, meet confidentiality requirements and uphold the right to privacy of those whose information is stored and processed. This is not a small task for any information-system, being it paper-based or electronic.

On the other hand, one should recognise the benefits of implementing information technology solutions in health care. IT is regarded by the health care providers as a tool to meet general and primary goals specific for the health care sector in terms of e.g. cost efficiency, co-operation between health care providers, continuity of care, patient safety, etc. In this perspective IT tend to increase the risk of a collision between those general and primary goals and – on the other hand – the legal interest of upholding the patient's right to privacy.

2.2 Problems and challenges

Modern information- and communication technologies in a way represents a new "information culture" compared to the way information is regarded within health care. In the latter setting, the focus is (or has been) on gathering and storing as little information as possible and keeping it as secret as possible. Modern information technology is in essence more about make storing of huge amounts of information possible, spreading it widely and without limits, and making it widely accessible. Merging these two cultures obviously meets challenges, conflicts of interests and barriers.

Several laws regulate information processing under national legislations. Privacy and security is protected under Data protection acts in all Nordic countries, In addition EU regulations¹ apply both to the EU- and the EEA countries. In terms of health care provision, specific legislation is in force, regulating the duty of confidentiality for health care personnel with additional penal provisions. Acting with respect for the patient's privacy and right to confidentiality is a fundamental part of what constitutes responsible and good conduct by the health care provider.

As there may be state-to-state differences between legislations, they all have patient confidentiality in common. The main goal is to establish the basis for trust and confidence in the doctor – patient setting. And it is first and foremost health laws that sets the standards that modern technology must meet. The challenge is to create, establish and implement solutions that meet strict confidentiality requirements. And the term "solutions" in this respect not only refers to hard- or software but also to organisational changes, new practices and, not to forget, ethics.

The use of modern information- and communication technologies leads to new and exiting possibilities in health care. But it can not be ignored that the same use represents new treats towards the integrity and safekeeping of health information. And many of the so-perceived legal barriers are found where the realities of existing regulations on confidentiality, privacy and security meet the possibilities and desires of ICT. Not all that can be done with these new tools in terms of storing, accessing and communicating information can be done due to legal hindrances, and not everything that can be done, should be done. The challenge is to a large extent to find acceptable technological solutions that meet the legal requirements.

One should not, however, underestimate the fact that existing legislation on this area does not fully encompass changes in perception with regards to health care, treatment, patient focus and processing and sharing of information. Legislation regulating confidentiality, sharing of information and patient records in the public health care sector derives from a time when health care was an isolated phenomenon, a final visit, and there were no imposed need for the GP to share his or hers medical records with other health care providers. Health care have been considered a static activity, not process oriented as it is today, often with several health care providers sharing their part (and obviously needing to share the same medical information) in the treatment of the patient. Furthermore, current legislation often does not take in to account the increased mobility of both patients and health care personnel. Legislation is based on paper medical records. It is not fit for electronic information processing and the great amount of information that needs to be stored, received, handled and communicated without being at the same time an obstacle for the health care.

These legislative challenges are a concern for health- and juridical authorities in many countries. One need to establish technical, organisational and legal measures that both ensure confidentiality and privacy and at the same time make sharing and distribution of information possible. One can say that there is a need to “synchronise” legislation with information technology.

To illustrate some of the ongoing discussions, we will here give two examples, from Sweden and Norway.

In Sweden we have seen that the counties, which have an obligation to provide public health care, implement information security models based on a Right-to-Know concept. The legislator, though, demands a standard of information security that is more based on a Need-to-Know concept. So why does not the counties follow the law? Well, a model based on e.g. Bell-LaPadula model would be very rigorous, demanding a lot of administration concerning every user in the network. A Right-to-Know model is more adapted to the modern way of health care needs, and the access rights are based on a role, e.g. “doctor”. Should the legislator ignore the counties “lawbreaking” and fight back in the name of integrity, or should the legislator adapt the legislation and make the best of the situation, with respect for both patient integrity and the health care provider’s needs? The latter solution is probably the one most in step with information processing in modern health care. Through this solution one can use IT both for making the medical records more accessible for health care personnel and safer from non-privileged users.

In Norway there is an on-going discussion on exchange of and access to medical-/patient information. Current legislation limits the possibility to share information by granting access to information stored at one site for an external requesting party, e.g. another hospital or a general practitioner. The Norwegian Health Register Act² draws a “line” or border around each institution and places clear responsibilities on different parties within the institution. Access to information is largely granted within each institution (naturally based on a “need-to-know” principle), but externally initiated access, e.g. from other institutions or doctors, is as a general rule prohibited.

It should be mentioned here that the limitation on external access to information does not (and should not) change the duty and right to share information through exchange and transmission that is initiated “internally” from the party hosting the relevant information database. On a technological level, this has the implication that systems must prevent external access to the data-systems and instead be set up to communicate by exchange of messages.

One reason for this difference is that from a security and risk-analyses/risk-management point of view it is inherently more “risky” to grant access from external “sources”. This is a statement or understanding fully shared and argued by the Norwegian Data Inspectorate (Datatilsynet), and a framework within which also health institutions and professionals must act.

In assessing the usability and safety/security of given systems, a key process is to perform thorough risk-assessment analyses.

What is utterly important, however, is to have a clear and precise understanding of what the legal requirements are and how these are interpreted under different legislations with regards to the use of IC technologies. Both health authorities and public bodies that supervise data processing legislation³ play important roles in the process of finding solutions all parties – patients, professionals, authorities – can live with.

In our work both within the Baltic eHealth project in general and the legal group in particular, we should also advocate – strongly – the fact that the use of electronic means and solutions in fact can enhance security, privacy and confidentiality. As an example, the use of electronic health records gives new possibilities when it comes to secure storing, better access when needed, possibilities to change/correct/erase and logging. Furthermore, the use of electronic patient records can contribute to the reduction of medical errors.⁴

Taking health services to a cross border level adds another challenge when it comes to security and confidentiality issues. Within the EU and EEA, legislation on data processing has been harmonized in accordance with the mentioned EU Directive on such processing. This does not by any means exclude institutions and/or personnel from establishing a high level of security and safety, especially when it comes to sensitive information. The directive and national legislation furthermore simplify transmission of information in the sense that these regulations establish a principle of acknowledging each country’s security regimes. But still one need to have established an acceptable level of security within each institution and the transmission itself must be sufficiently safe and secure.

2.3 On health networks

The establishment and increasing use of national health networks have proven to be a way to boost use of many telemedicine and eHealth services. Although there are some differences in terms of technological and organisational regimes, a common denominator is that these networks are closed (more or less) and aim at facilitate communication between many (all) parties of the health care system. Most health networks are in one way or another internet-based.⁵

Health networks are often mentioned in the same sentence as terms like “secure” or “safe”. The networks aim at providing a safer and more “organised” infrastructure for medical information exchange.

Using these networks no doubt can contribute to making the communication safer and more secure. As important as the technology is the fact that these networks means the establishment of organisations that to some extent take responsibility for connections and most importantly the traffic between the connected parties.

But in terms of security and safety it is important to be aware of the limitations of the networks duties and responsibilities. These networks does not by any means remove or take over these responsibilities from personnel or institutions. The end-users are still fully responsible for establishing security and safety regimes. It is the end users that must answer to the national supervising authorities, regardless of the use of health networks. Connecting to and using a health network is something that must be considered together with other aspects of the whole security regime of the end-user. The potential risk of this connection must be made part of the risk assessment study that all users must carry out.

This applies to a national level, and connecting national networks to create regional networks obviously does not change this.

2.4 Project specific issues

Confidentiality, security and safety issues are important for both pilots in the Baltic eHealth Project. Both services rely on safe and secure exchange of potentially very sensitive information and must establish strict and credible security regimes. As mentioned, the adaptation of the EU Directive on processing of personal data (see above) has lead to a harmonised and quite uniform legislation within the EU and EEA states. This does not, however, limit the national authorities’ powers and responsibilities and the end-users must relate to and act according to the provisions of these authorities. Among other things, this usually means that proper risk assessments study must be carried out, taking into account the cross national/cross border aspects of these services.

When used as a routine service, eRadiology can make the establishment of a so-called virtual radiology department possible. This can be graphically described as this:

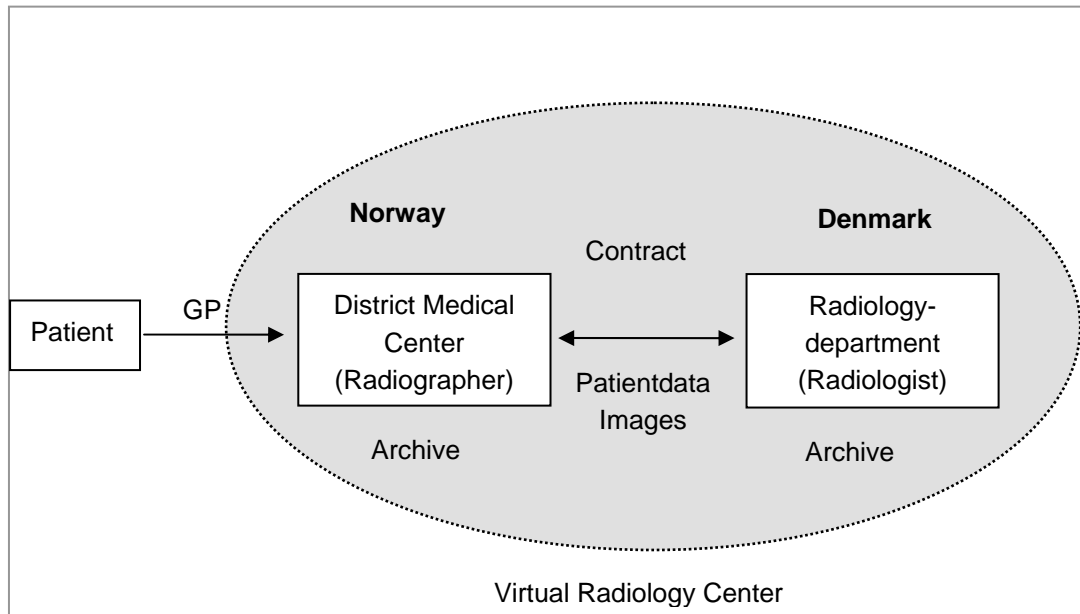


Figure 1⁶

Having such a centre or department working in according to national legislation is a multifaceted challenge, but obviously security and safety is utterly important. In an ideal setting, information shall flow between the parties constituting the department, secure and at the same time easy and effortless/seamless. We believe this is obtainable and the relatively small scale pilot should give us valuable knowledge that can be used when moving to large scale routine services.

2.5 Further actions

The more detailed and concrete requirements that have to be met in order to act within the national legislations must be clarified in due cause and in cooperation with the project partners from the participating countries, the national health- and data processing authorities.

In a more long-term perspective, it would be very useful to be able to do a more comprehensive study on differences, similarities and barriers between the legislation of the participating countries, but this will probably be to big a task to perform within the limits of this project.

In order to fulfil the aims of the project and this work package, we will produce a set of guidelines on this issue. These guidelines will primarily be aimed at the pilots and services in this project, but can hopefully have relevance beyond and for further development and expansion of the project. These will be generic and pragmatic guidelines on good and useful routines for secure and safe information exchange in the pilots. The guidelines will also include recommendations on record keeping.

3. Responsibility

3.1 The issue

The term “*responsibility*” is multi-faceted. There is at least three aspects of it:

- Being responsible
 - For instance when we are dealing with issues like assigning a doctor who is responsible for the treatment of the patient when she/he is at the hospital. In our setting: Who is responsible for the patient in a telemedicine setting?
- Acting responsibly
 - This refers to the ethical-legal norm put on all health care personnel to conduct their practice in accordance with the best standards, and to be “measured” against these standards. This is the aspect of responsibility as a so-called legal standard.
- Being held responsible.
 - Refers to the fact that a doctor (or any/many other health care personnel) can be met with sanctions if the legal requirements (or ethical requirements) are not met or not satisfactory fulfilled.

Responsibility is a “legal standard”. In terms of law-making, this means that the legislator in the relevant act and article refers to the standard as a legal requirement. The law or article itself does not further detail the content of the standard (or do this only to some extent). What is “in” the standard is based on a judgement of what is the state-of-the-art performance of (e.g.) a procedure at a given time. As research, practice and competence changes, so will the requirements under the standard. Ultimately, the level will be set by courts or disciplinary boards in cases where a procedure is disputed.

Estonian legislation is a bit different than the Nordic in the sense that there is no specific legislation concerning the medical profession. The legal situation between doctors (and other health care personnel) and hospitals is regulated through contracts. One chapter of the Estonian Law of Contracts is dedicated to regulating the activities of medical personnel. At the moment of writing this report it is not entirely clear if this system is open for variations in these contracts or if there is a great deal of standardisation. This might be important for the legal basis of telemedicine and eHealth, especially with regards to responsibility and responsible practice.

As we see, these are different *aspects* of the issue and not different issues. The aspects are intertwined in each other. If not anything else, this shows that responsibility is a difficult issue. It is difficult to define and limit, and difficult to discuss. In our group it is therefore important that we from the start have a more or less common understanding of what we mean by the term “responsibility”. I will here present it as I see it and as I have dealt with it over the years.

From the very start of telemedicine in Norway, health care personnel and especially doctors have raised questions concerning responsibility. Naturally, both personnel and patients feel uncomfortable with uncertainty in this issue, and it is every reason to assume that this is a feeling shared with colleagues and patients world-wide. In a simple form, the question has been who the responsible practitioner is where the patient meets with his GP and the specialist is present via videoconferencing. As services and solutions have evolved, the question has been expanded to encompass all settings where the patient – doctor contact goes through some kind of interface, online or offline.

Distance is the core of the issue. And in relation to the three aspects of responsibility mentioned above, the following questions can be asked:

- Can a doctor be the responsible (treating) doctor for a patient that she or he does not see face to face?
- Can a doctor treat a patient that is not physically present and still meet requirements of responsible conduct? Can only some kinds of tele-treatment be considered responsible?
- Can a doctor be held responsible for misconduct or malpractice when treating a patient via a telemedicine/eHealth service?

3.2 Official legal interpretations

We mentioned earlier the concern on this issue shared by medical- and other professionals in Norway from the early start of telemedicine. This concern led to the issuing of a so-called “Circular letter” (rundskriv) from the Norwegian Ministry of Health as early as in 1996, and in 2001 this was replaced with an updated circular letter, I-12/2001 entitled “Telemedicine and responsibility” (Our translation. Original: “Telemedisin og ansvarsforhold”).⁷ A circular letter is an official interpretation of laws or other regulations on specific topics. The interpretation is not law itself, but holds a high “status” for instance in courts or other casework. These letters also serve a preventive function in the sense that they aim at clarifying difficult or debated issues before they (e.g.) go to the courts.

The Norwegian Circular Letter (hereafter: CL), sets out by stating that with regards to responsibility, the use of telemedicine does not change established principles. This is an important statement in the sense that it emphasises that from the Ministry’s point of view, telemedicine practice must perform within existing legislation. The CL then goes on to define responsibility, and does so by saying that it will be too extensive to give a full definition. In this context, the term is used on “*breach of legislative duties that can have compensation, punishment or administrative reactions as a consequence.*” (Our translation).

In the CL, responsibility is closely connected to the duty of *acting* responsible as it is expressed especially in the Norwegian Health Personnel Act,⁸ article 4 (§ 4). This article puts a strong duty on health care personnel to act within their competence in a manner that meets high standards in terms of responsibility and care.

It has been asked whether responsibility should be judged differently based on what kind of telemedicine means that are in use. The Norwegian CL answers this by stating

something one can call an information principle: This principle states that health care personnel is responsible for the treatment given, based on the information it gets about the case at hand. *How* the information is received, being it by a face-to-face meeting, through video conferencing or by sound and/or pictures sent to the patient, is irrelevant. The receiver of the information must consider if the information is good enough – in terms of both quality and quantity – to start treatment, give advice or other actions. In a telemedicine setting; if the doctor finds that the received information is not good or sufficient enough, she or he must get more information or ask the patient to meet for a face-to-face consultation.

This principle implies that from the view of Norwegian Health authorities the use of telemedicine (or eHealth) is not considered irresponsible at the outset. This is different than what we have seen elsewhere. There are examples that under some legislations⁹, the health authorities and/or the legislators have found it “necessary” to state, more or less explicitly, that no treatment can be based on information received by any other means than traditional face-to-face contact.

To finalize going through the Norwegian circular letter, it is worth mentioning that the letter ends by emphasising the importance of having systems and routines in place, and that this to a large extent is a management issue. In a telemedicine setting, it is important to clarify the situation. What kind of consultation is it? Who is doing what? Is everyone at the same “level” in terms of who is doing what, etc. Some examples of routine questions are given:

- What is the situation at hand; a *referral* from a GP to a specialist, or advise from specialist to GP?
- Is the received information sufficient for a responsible medical judgement?
- Who will keep and be responsible for health records?

The Swedish Board of Health (Socialstyrelsen) issued a similar interpretation some years ago and the statements and principles laid out by Norwegian authorities is believed to be in full accordance with Swedish legislation.

At the time of this report being made, the Danish health authorities have issued a draft for a guideline or circular letter very much in line with the Norwegian CL. This document have been assessed by (among others) the Danish Medical Association and their statement is very positive.

Naturally, there is no definitive answer to the question “who is responsible”. The answer might not be that one person and/or body is responsible. Different parties can be responsible for different situations, at different stages and based on differences in competence. From a telemedicine/eHealth viewpoint, the important issue is to make sure that the use of these services is not excluded as irresponsible from the start. A way of preventing this from happening is to establish good routines and guidelines on practice as well as making sure that this practice is in accordance with national regulations and governmental interpretations.

Apart from the obvious value and necessity of sorting out these issues in order to clarify the situation for the patient, the personnel and other parties, it is important to be

aware of the fact that how we judge the service in terms of responsibility is in fact decisive for the service itself:

If the legislation (or the interpretation of it) states that a doctor can not in a responsible manner treat patients via telemedicine/eHealth interfaces, then the services themselves are “reduced” to advisory services/doctor-to-doctor second opinion. A consequence of this is that the service is not subject to payment, at least not in full.

3.3 Project specific issues

In our project, the answer and solutions to this “problem” will decide/determine if a teleradiology or teleultrasound service between hospitals (nationally or cross border) can really replace/substitute such services where a hospital or a medical centre does not have radiologists in house or where the existing radiologists’ workload is too heavy. (See figure 1 above). With a restrictive approach/attitude from health authorities (and/or legislators), teleradiology or –ultrasound will be used merely for second opinion and doctor-doctor advice or education purposes.

These can of course be useful and powerful services, but eHealth can be so much more. It should be a goal for this project to argue before our health authorities (and others) that responsibility issues should not stop services from develop into real telemedicine treatment services.

With regards to responsibility, the eUltrasound pilot causes fewer problems. The pilot, at least at this stage, exchange information between doctors, between known (and few) parties and for advisory/consultation purposes. In this setting the responsibility will remain with the principal doctor – the one asking for advice from the specialist in Trondheim. The latter is of course not completely released from all duties of responsibility, but she/he will not be considered responsible for the treatment of the patient.

3.4 Further actions

As mentioned above, clarifying responsibility issues is decisive for how the services can be performed. It will therefore be an important task for this project to make sure that national legislations do not prohibit our services due to a strict interpretation of responsibility issues. It will probably be necessary at some stage to contact the health authorities in at least some of the participating countries to clarify this issue.

Furthermore we will produce specific guidelines on responsibility. These will be made in accordance with the mentioned principles of the Norwegian, Swedish and Danish recommendations and we will draw on existing guidelines on e-radiology to the extent they are relevant for our pilot.

4. Licensure

4.1 The issue

Doctors and other health care personnel need to be licensed to practice. National licensure bodies¹⁰ issues general licenses as well as specialist accreditations to doctors and other health care personnel. A license shall be based on the applicants formal competence, first and foremost her or his diploma(s). In addition, and depending on the license in question, other skills might be relevant, like practice, specialisation, etc.

Since understanding and being understood is important in a health care setting, the national bodies can establish requirements with regards to language skills for out-of-state applicants.

Since all participants in this project is either EU members or part of the EEA, the EU Directive of 5 April 1993 on mutual recognition of diplomas¹¹ is relevant and important. The provisions of this Directive have been made Norwegian law under article 52 of the health personnel act and the EEA regulations. The same legal adaptation have been made by most (all?) other member states.

The purpose of this Directive and subsequent adaptation of member state laws is to facilitate free movement of doctors (and other health care personnel), by establish a regime where diplomas from medical schools in the area are recognized mutually between the states. This harmonisation makes it much easier to obtain a license in another EU/EEA country, and to some extent it is a *right* for the professional to get such a license.

However, the process is not entirely summary in the sense that national authorities shall consider the application and that additional courses and skills (e.g. language) can be required. And the directive and legislation does not imply that there is a common European license for all medical professionals. To practice in another country, a doctor (and other) must still send an application and obtain license from the national authorities.

In this chapter, we use the term "accreditation" for the authorisation given to specialists.

4.2 Questions

The following are some of the questions we have seen being asked or raised concerning licensure/accreditation. This is not a prioritised list, and the list is not exhaustive. When the term "doctor" is used, it usually also applies to other health care professionals, as for example those listed in the mentioned EU directive on mutual recognition of diplomas.

4.2.1 *Is there a need for a special license in telemedicine/eHealth?*

In the early days of telemedicine (some ten years ago) this was a more important and more discussed issue than it is today. At the time many believed that telemedicine should be looked upon as another speciality of medicine, and as such it should at least be subject to specialist accreditation. Some argued that this was an important aspect of the whole issue of quality assuring the services. Malaysia was one of the first countries (if not *the* first) to pass a Telemedicine Bill, as early as 1997.¹² In this bill, the Malaysian health authorities establish a regime where professionals that want to practice in Malaysia can apply for and get a certificate to practice telemedicine from another state. The impact and use of this bill is not known to us, but might be something to look into as part of our project.

It is probably safe to say that the attitude towards telemedicine and eHealth have changed over the years. The main conception nowadays is that telemedicine and eHealth solutions is “blending in” into traditional medicine and are tools for enhancing these services and making them more accessible and more equally accessible. As a consequence, few believe that it is necessary to require specific licensing for telemedicine. The issue is more how to make use of telemedicine/eHealth part of education and competence of medical professionals.

4.2.2 *In what country must a doctor be licensed?*

Obviously, this question is relevant for services where telemedicine is provided across borders – where the professional and the patient reside in different countries and under different legislations.

The question can be divided into at least three sub-questions:

a) Who is “travelling” – the patient or the doctor?

The traditional perception is that in a cross-border telemedicine setting, the doctor is “travelling” by electronic means to patients in another country. The situation could, however, be the opposite: It could be that it is in fact the patient who is travelling to a doctor in another state/country. In the latter example, the issue of licensing is of less importance, and the question is more whether or not the patient can reimburse national (local) insurers for costs. If we apply the traditional perception, we are lead to sub-question b).

b) Must an out of state doctor have an in-state license to practice?

If a doctor is offering treatment from another country, the question is whether she or he needs a license to practice medicine in the country where the patients reside. The principal or traditional answer is yes. In order to practice, a doctor must be licensed in the country where she or he is practicing. It does not matter if the doctor is fully licensed in another country. This is the case where the doctor physically moves from the country where she/he is licensed, to another country. Within the EU/EEA region, obtaining license in another member country is, as mentioned, almost a formality. Nonetheless, a license must be obtained.

If this is a requirement also when the doctor continues to practice from the licensing state, solely providing services through telemedicine to another, is still unclear. (see below under “c”)

An alternative solution could be to establish a solution like the one proposed in the mentioned Malaysian Telemedicine Bill where a out-of-state license is combined with a in-state telemedicine certificate.

Or maybe this problem could be solved through contracts or treaties between countries and/or individual doctors.

c) Can a licensed doctor practice from another country?

This question refers to a situation where a doctor is licensed in one country and offers services via/by telemedicine to patients in this country, but the doctor resides in another country.

Under Norwegian and Swedish law, this still is an unclear situation. We have put the question before Norwegian health authorities, but have not yet received a definitive answer.

Questions concerning this have been asked to the Swedish Board of Health and their preliminary point of view is that the out of state doctor must hold a license in her home-country only, and that Swedish patients seeking this doctors treatment, by telemedicine or by travelling, must raise maltreatment complaints under the licensing state’s legislation. A Spanish doctor treating Swedish patients through telemedicine can never be held responsible under Swedish legislation.

This standpoint is fully understandable and in line with the situation in most countries. But it still raises two questions: Can the Spanish doctor be liable for practicing without a proper license (quack doctor) by offering her/his services to Swedish patients? And: What if the doctor applies for, and gets, a Swedish license. Can she/he then practice in Sweden, from Spain, via Telemedicine and then fall under the supervision of Swedish health authorities and be allowed to enter the Swedish reimbursement/health insurance scheme for her/his services?

With regards to radiology it has been stated that these are services where it is of little relevance, from a patient point of view, who is in fact interpreting the pictures. (Given that this person is qualified). Following this argument, obtaining a license from the out of state radiologist might not be necessary. The responsibility towards the patient will remain at the radiology department where the examination/treatment is carried out.

For services like radiology, this might be a fruitful approach. One potential drawback of this arrangement is that the interpreting radiologist (who is in fact *treating*), will be excluded from supervision and any sanctions from the health authorities of the state where the patient resides. The question of quality assessment and judging the radiologists’ qualifications will be handed over to the hospital and it will be up to the hospital to supervise and follow up, probably through contracts. This arrangement also means that there must be a responsible radiologist at the patient’s institution. It will probably hinder the use of real virtual radiology departments where one side can be staffed with radiographers only.

4.3 Further actions

This project is a cross-border project, and it is of great importance to clarify the situation on this issue. I think we first of all need to look at the different legislations, but we believe that we will find that they have much in common.

We need to find out if it is acceptable for national health authorities that out-of-state radiologists and ultra-sound specialists “treat” patients without being licensed to practice in the state where the patient resides and where the examination is performed.

This issue was discussed at the e-radiology workshop in Trondheim in early March 2005¹³, and the general opinion seemed to be that it was probably necessary for the radiologists to obtain national license(s). This would be the most orderly way of sorting this matter, however not solving all problems. There seems to be differences between the national authorities with regards to how such applications are processed and the question of whether or not a doctor in fact can practice into a state from another is still not clarified. These issues must be addressed in our project, probably by contacting the different health authorities and asking for clarifications.

Licensure issues will also be made part of the guidelines on responsibility since this is one important issue to clarify before, or as part of, entering into a treatment situation.

5. Patients' Rights

5.1 The issue

Granting people legal rights is a strong force in many states. The importance of rights and the notion that it is the national legislator's duty to grant and protect these rights is a thinking that really found its foothold after World War II. The perception of human rights manifested itself in the United Nations Universal Declaration on Human Rights.¹⁴ This declaration establishes a foundation, a set of minimal rights for every human being that it should be a duty for both the global society and the individual states to secure and protect.

Legal rights have become part of health care legislation as well. One is talking about the individual citizen's right to health care and rights towards the health care system. Over the years we have seen patients' rights act put in force in many countries. It is worth mentioning that Finland passed the first patients' rights act in the world. And even without a specific act or regulation on patients' rights, it is widely recognised that patients have some rights with regards to health care that are secured by law. We have already mentioned that confidentiality is not only a professional duty, but also a patient right. Another important right is the patient's right to access and see her/his own medical records. Up until quite recently this was a discussed and debated issue in many countries and not something all patients could consider a right. The extent of this access right was also widely discussed, and in Norway this was not entirely clarified before the passing of the Patients' Rights Act of 1999.

In Estonia there is no specific legislation on patient rights. This does not, however mean that Estonian legislation does not acknowledge patients as having rights towards the health care system. These rights must be claimed using the traditional measures according to Law of Contract and criminal law.

Patients' rights can be divided into three aspects:

- The right to *become* a patient (entry rights)
- Rights as a patient (e.g. right to information, consent and access to medical records)
- Formal/procedural rights (e.g. right of appeal)

How and to what extent these rights are granted varies under different legislations. The most controversial of these, is probably the right to become a patient. This implies a right to treatment, often specified in terms of level of treatment and a timeframe within which treatment must be granted. This is a right that must be met with clear obligations from the authorities and it has obvious economic consequences.

5.2 Patients' rights in the Baltic eHealth project

Pilots and services in this project should obviously meet national requirements with regards to patients' rights. We believe that it is especially important to uphold rights in terms of information and consent. At this stage we do not see that the services of this project have a direct relevance for possible rights regarding the right to treatment. It

can, however, be argued that both the e-radiology and the e-ultrasound pilot can contribute to faster response/treatment and that advice and treatment is given at a higher level. In any case, we should be aware of these issues and make clear the state of patients' rights in the participating countries and make sure that our pilots perform in accordance with these rights.

5.3 Further actions

To create awareness of patients' rights and ensure such rights in this project, we will produce a set of guidelines on this issue. These guidelines will especially focus on information and consent issues as these have been pointed out as especially important by many of the participants in the project.

6. Reimbursement/payment

6.1 The issue

Reimbursement/payment is perhaps the most important issue when we are talking about barriers for implementation of telemedicine/eHealth – both on a national and an international level. It is probably a more political than legal issue, but has some legal implications and basis.

The total merging of eHealth into the health care system is still a bit ahead, and as a consequence, these solutions and services are treated very differently by health authorities' world wide. The solution to all these problems lies partly (a major part) in how these services are considered in each state. Is telemedicine/eHealth recognised as full medical services, or “merely” as support-solutions? Can patients be treated via telemedicine, or can telemedicine be used only for second-opinion? (cf. the discussion on responsibility above). Can out-of-state doctors be paid or patients seek reimbursement for treatment received from out-of-state telemedicine doctors?

To further complicate the situation, payment-/reimbursement-/insurance systems are different in different countries. In the Nordic (and probably the Baltic) countries, however, the systems are mainly public with a limited element of private participation.

6.2 Further actions

Working with these issues easily drain out all energy from a good idea and project, and often lead to a rapid decrease of speed. In order to avoid this, we suggest a parallel approach:

At the same time as we try to find solutions to this issue on a more superior and “legal” level, we should try to solve this issue within this project through contracts between the parties. This work obviously will have to be done in close cooperation with the work on economics.

We believe that contracts can be both a powerful and dynamic tool to solve this issue in this project, but we fully recognise that contracts only to limited extent solve the reimbursement/payment issue. We should aim at discussing this issue with national authorities at some stage. To the extent that this project leads to findings in this issue we should document them and disseminate the results on a wider level, both regional and international.

7. Contract issues

Contracts have been mentioned several times both in this report and in our meetings in the project. We have argued that many of the issues raised here can and probably should be solved through agreements and contracts. We believe that contracts are versatile, dynamic and give the necessary precision. Through contracts we also identify the relevant parties and commit them to their duties in the project.

One limitation of using contracts is of course that they are specific to the situation and parties involved in it. In principle they have no power or relevance outside this framework.

There are some issues that need to be clarified before negotiating and working out the contracts:

- Contracting parties

One needs to point out the person/persons that have in fact the power to commit the institution. In most cases the situation will be that the contract is entered between two or more institutions. If the case is that the contract is entered between individuals, this should be clarified by the management of the institution (usually a hospital).

- What can be subject to contracts?

Even if national legislation in principle upholds a large extent of contractual freedom, health care is an area where there probably are some limitations. For instance, the mentioned rights of patients can not be violated by contract. It will probably be necessary to quality assess our contracts with both hospital owners/managers and health authorities.

7.1 Further actions

In order to secure quality and to have as uniform contracts as possible, we will issue a set of guidelines on contracts: How to make them, what should be part of them, who should be parties of them, etc.

We will look into this further, but it is probably a good idea to produce some standard contracts or at least some standard contract fragments.

8. Informed Consent

8.1 The issue

Consent can be defined as an unrestricted, unilateral statement, action or disposition based on sufficient information, given by a competent person. It is a specific legal term relevant in many situations where a person commits her-/himself to something. Consent is an issue that is being widely discussed both in general and in relation to specific topics, as for instance health care. Within the scope and the limits of this report we will just give a brief description of this issue, pointing only at the most important aspects relevant to health care.

8.2 Requirements for valid consent

We will here present some of the most important requirements for valid consent. This presentation is not very detailed, but we believe it covers the most important aspects.

8.2.1 *Personal competence*

Consent is an individual commitment, and the consenting party must be competent to consent. In general competence to consent coincides with a person being of age, in the Nordic countries this happens at the age of 18.

With regards to health care, there are, at least under some legislation, some exceptions from the general rule. According to the Norwegian Patients' rights Act, article 4-3, a person has the power to consent from the age of 16. This was also the case before this act came in force.

But even if a person is of age, she or he can be considered incompetent to consent. This is especially relevant for elderly people and people with reduced mental capabilities. This can be a permanent or a temporary condition. It is the duty of the receiver of consent – the health care personnel in our case – to make sure that the consenting party is competent.

8.2.2 *Unrestrained*

It is an absolute requirement that the consent is given without any kind of pressure or restraint. A forced consent will not under any circumstance be valid.

This may sound like an obvious and unproblematic issue, but in practice one can easily find situations where the line between persuasion and pressure gets blurred. This can for instance be the case where the patient is in doubt about whether or not to enter into a suggested treatment and the doctor strongly recommends that she or he does.

8.2.3 *Information*

The phrase informed consent is very commonly used. It is in fact somewhat of a tautology, since there is no such thing as consent without information. And some have even pointed out that it is not the consent that should be informed, but the patient.¹⁵

The phrase does however emphasise the importance of information as a requirement for consent.

The patient shall be given enough information to be able to judge the situation and to make a reflected decision. In English case law this has been stated as follows:

“The health care provider must provide the patient with sufficient information about the proposed treatment and its attendant risks to conform to customary practice of members of the same profession with similar training and experience situated in the same or similar communities. In addition, the health care provider must impart enough information to permit a reasonable person to gain a “general understanding” of both the treatment or procedure and the “usual and most frequent risks and hazards” associated with the treatment”¹⁶

This quotation points out a very important aspect of information: As well as information about the treatment in question, the patient must be informed of potential risks. There have been some discussions, both in literature and court cases if the health care provider must inform the patient about *all* risks, however distant. This is probably not necessary.

As important as providing the patient with information is it to make sure that she or he has really understood it. The health care provider might fulfil his information duties by giving the patient a handout or something like that, but in many cases it is necessary to sit down with the patient and explain treatment and procedures and risks in detail. This is probably especially important with elderly or very young patients.

8.3 Formal requirements. Consent forms and documentation

As a general rule there are no formal requirements for consent. In everyday life, a patient consent to be examined and treated by the doctor just by showing up at the doctor's office or at the hospital. The doctor will not have to specifically ask for consent.

In most cases there is no requirement for written consent. Consent can be implied, it can be stated based on the patient's behaviour (like above) and it can be oral. In cases where it is important to be sure that the patient has given consent and what she or he has consented to, some kind of written consent can be a good idea. This is especially the case where such documentation can be useful for later audit.

In any case, the doctor should enter information about consent issues into the patient's journals, if this has been discussed with the patients.

One should be aware of that the use of some kind of consent form does not in any way amend consent that contains some kind of errors. The use of forms does, for instance, not relieve the health care personnel from its information duties.

8.4 Withdrawal

A very important aspect of consent is that it can be withdrawn. This is a privilege for the consenting party and it can be withdrawn at any stage, without any limitations.

This is underlined in the mentioned Norwegian Patients' rights act, which states that if the patient withdraw her or his consent, she or he shall be informed about the implications of the fact that health care can not be given.

8.5 Consent is not a contract

Consent is fundamentally different than a contract. A contract is entered between more or less equal parties, putting specific obligations on them and giving them instruments and measures if one of the parties does not fulfil her/his obligations. A contract is in force for the agreed time and can be terminated or prolonged only by agreement between the parties.

Consent lacks this duality and equality. As mentioned, consent is unilateral. By giving consent, a person is using a right she or he has as an autonomous human being. And the consenting party can at any time withdraw this disposition. Consent is limited to the situation at hand and it has a limited lifetime.

These limitations to consent are important to be aware of. We see that consent in some cases is being used in a way that at least looks like a contract, and in some cases forms and written consent is used to make things a bit more "contract'ish". We strongly advise against it.

8.6 Project specific issues

The pilots in this project raise some particular issues with regards to consent. In most cases, neither radiology nor ultrasound raises problems with regards to consent. The services are well known and the patients are familiar with the procedures.

Radiology services have also been called "back-room services". This describes the fact that from the patients' point of view, the medical treatment is done by someone they do not meet or see. This at least applies to the simple forms of radiology. But most patients in most cases have no idea about who is interpreting the pictures, and most probably do not care. And to a large extent, the patient's consent to treatment also implies consent to processing of personal data, including pictures.

In our project this has raised the question whether we should establish a routine for asking consent from the patient – a routine that is not used in traditional services. If a patient has her pictures taken in Odense (Denmark) and the pictures are transmitted to Estonia and interpreted by a doctor there, should this be based on her consent?

We do not have a definitive answer to this question. It is a point, and a good point, that patients as mentioned usually do not get information on who is interpreting the pictures, and they are not being asked to consent.

However, to be on the safe side, we suggest that we establish a routine where consent from the patients is obtained.

One argument supporting this approach is the fact that this way of having the pictures interpreted is relatively new for most patients. As a general rule, more emphasis should be given to information and clear consent when dealing with untraditional and

new procedures. The patient should be informed that the pictures might be transmitted to radiologist/radiology department in another country for interpretation. She or he should be informed about the means of transmission, including safety and security measures. Following the nature of consent, this means that the patient can protest and deny the doctor or radiographer to send the image. This must be respected, and the images must then be dealt with in a traditional matter.

The way the consent issue has been dealt with should be reported in each patient's journal.

To the extent this routine is suitable for the eUltrasound pilot we suggest the same approach here. This issue might not be as relevant for this pilot since it only deals with doctor-to-doctor consultations and not actual treatment. It will probably, however, be in accordance with good medical practice to inform the patient that the ultrasound examination will be transmitted to an external expert for second opinion.

8.7 Further actions

Consent issues will be made part of the guidelines on patients' rights. At this stage we are not convinced that a specific consent form is necessary, but if it turns out to be so or if this is something the practitioners ask for, we will reconsider this.

¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

² Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) LOV-2001-05-18-24

³ See www.dp.gov.ee, <http://www.datatilsynet.dk>, www.datatilsynet.no, www.datainspektionen.se, www.ada.lt

⁴ See the report "CPR Generation Effectiveness in Reducing Medical Errors", issued by the Gartner Group at www.gartner.com.

⁵ For more information, see for example www.carelink.se (Swedish health network), www.medcom.dk (Danish health network), www.nhn.no (Norwegian health Network).

⁶ The figure is taken from the minutes of the eRadiology workshop held in Trondheim on March 10 2005. Minutes taken by Morten Jakobsen and Henning Voss. Used by permission.

⁷ Full text of the circular letter can be found (in Norwegian only) at http://www.dep.no/hod/norsk/dok/andre_dok/rundskriv/030071-250016/dok-bn.html

⁸ Lov om Helsepersonell m.v., LOV-1999-07-02-64. See: www.lovdata.no

⁹ A German guide for medial conduct from 1997 stated that *"The medical practitioner may supply individual medical treatment, especially advice, neither exclusively by letter nor in newspapers or magazines nor exclusively by means of communication media or computer communication networks."* This quotation is taken from "Green Paper. Legal aspects of health telematics" issued by the European Health Telematics Association (EHTEL), www.ehtel.org

¹⁰ See for example <http://www.safh.no/> which is the website for "Statens autorisasjonskontor for helsepersonell" or "The Norwegian Registration Authority for Health Personnel". (web site partially in English).

¹¹ Full title: *"Council Directive of 93/16/EEC of 5 April 1993 to facilitate the free movement of doctors and the mutual recognition of their diplomas, certificates and other evidence of formal qualifications."*

¹² See: <http://mcsl.mampu.gov.my/english/telemedicBI.html> (last accessed 14.12.2004)

¹³ See "Minutes of eRadiology Workshop in Trondheim 10th of March 2005", available at <http://www.baltic-ehealth.org/>.

¹⁴ See <http://www.un.org/Overview/rights.html>

¹⁵ Rynning E, Samtycke till medicinsk vård och behandling, Lustus Förlag, Uppsala, 1994

¹⁶ Ford v. Jarman