MOMENTUM

European Momentum for Mainstreaming Telemedicine Deployment in Daily Practice

(Grant Agreement No 297320)

Deliverable 6.1

Report on **SIG 3** Legal, Regulatory and Security Issues

Legal, regulatory and security issues section of the Blueprint developed by practitioners

Version 13

Work Package:	WP6
Version & Date:	v13 12 August 2013
Deliverable type:	Report
Distribution Status:	Public
Authors:	Ellen K. Christiansen, Eva Henriksen, Leif Erik Nohr, Eva Skipenes
Reviewed by:	Montse Meya, Maria Jacobsson, Benn Molund, Kalliopi Liatou, George Gorgogetas, Athanasios Ballis, Constance Colin, Diane Whitehouse
Approved by:	EXCO
Filename:	D 6.1-SIG3 – v13_Momentum_SIG3_legal_report.docx

Abstract:
Since legal, regulatory and security issues are often mentioned as being among the main barriers for the establishment of sustainable telemedicine services, the SIG 3 team wanted to know how people in the field had experienced these issues. Some key issues that were addressed in the questionnaire related to the telemedicine services as described by the respondents: accreditation, conflicts of law, consent, data management procedures, the existence of national guidelines for responsibility and liability, ethical approval and concerns, the need for change in legislation, liability, privacy training for personnel, risk assessment, and selected security issues. The answers indicated that health care personnel involved in telemedicine services do not necessarily have an in-depth knowledge of legal and security requirements as their focus is elsewhere: it is on the patients and their well-being. It also appears that many of the respondents do not know who to ask when they have queries in these fields. One consequence of this finding might be that locally anchored and small projects cannot be scaled up, due to unsolved legal and security issues.

Keywords:

Accreditation, authentication, consent, data management, encryption, information security, legislation, liability, risk assessment, telemedicine guidelines.

Change History

Version History:

01	15 June 2012
02	19 March 2013
03	April-June 2013
04	18 June 2013
05	28 June 2013
06	28 June 2013
07	16 July 2013
08	17 July 2013
09	19 July 2013
10	20 July 2013
11	22 July 2013
12	24 July 2013
13	12 August 2013

Version Changes

01	First assessment of issues at hand
02	First review
03	Discussion with different national stakeholders, literature studies, writing, refining
04	Second review
05	Refining of blueprint
06	First draft completed. Draft sent for internal review
07	Commentaries received from the reviewers
08	Internal review by D. Whitehouse
09	Refining of blueprint by E.K. Christiansen
10	English language check by D. Whitehouse
11	Refining of blueprint by Ellen K. Christiansen
12	Review for formatting and consistency by M Strübin
13	Modifications made in response to editorial comments by M Strübin

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Momentum bears some similarities to the more general, and earlier, eHealth-related thematic network, CALLIOPE. It builds on some of the good practices developed in CALLIOPE. Where recognition is due to earlier principles, policies or operational processes developed and fine-tuned within CALLIOPE, due recognition is paid to this.

Table of Contents

Table of Figures

Abbreviations/Glossary

ATA	American Telemedicine Association
CPME	Comité Permanent des Médecins Européens
DH	Department of Health (UK)
EC	European Commission
EEA	European Economic Area
EHMA	European Health Management Association (http://www.ehma.org/)
EHR	Electronic Health Record
ENISA	European Network and Information Security Agency (http://www.enisa.europa.eu/)
EU	European Union
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	information technology
ITU	International Telecommunication Union
PIN	Personal Identification Number
PKI	Public Key Infrastructure
URL	Uniform Resource Locator
VPN	Virtual Private Network
WHO	World Health Organization

Executive summary

This section contains an overview of the issues investigated in the Momentum project survey when it comes to legal and security issues related to telemedicine services. Due to differences in the legislation concerning health services and data security in the Member States of the European Union (EU) and the European Economic Area (EEA), it is of great interest to investigate how these topics are dealt with in the various countries.

Special interest group 3 (SIG 3) has attempted to identify general features from the answers, as well as main differences. Based on these findings, study of the literature, input from stakeholders and the SIG's own members' experience, we have discussed a number of legal and security aspects and have developed some basic draft guidelines on law and data security to be used for implementation of telemedicine services.

Various issues of concern were included in the questionnaire survey. Topics for questions in the legal and regulatory fields included[1]: the need for change in legislation to facilitate for large-scale implementation of telemedicine, accreditation, responsibility and liability conditions, telemedicine crossing organisational and national borders and conflicts of law, national guidelines for clinical responsibility and liability in the telemedicine field, patient consent, and ethical approval and concerns.

The following topics were the subject of questions about information security: data management procedures and responsibility, information security risk assessment, various security issues and security measures in use, and privacy training for personnel.

Legal, regulatory, and security stakeholders were also mapped.

Some basic findings are the result:

- Some fundamental ethical, legal, and security principles for telemedicine should be discussed and outlined at an EU level,
- Basic principles for the use of telemedicine systems must be grounded at a national level,
- Some fundamental and overall principles must be worked out at a national level,
- When establishing and using a telemedicine service, both a "legal risk assessment" and a security risk assessment should be done repeatedly throughout the whole process,
- Financing/reimbursement is probably not a legal question as such, but the financing of the service must be taken into account from the very beginning of the development of the telemedicine services,
- As telemedicine is not a second-class service, the health personnel need to ask themselves: "Under what circumstances should it be considered either unjustified or not in accordance with best practice *not* to use telemedicine?" This assessment must be based on knowledge about best telemedicine practice adapted to different situations. To the extent such knowledge is not available, it reveals the need to explore this field.

Thus, a set of preliminary pieces of advice can be given on a general basis in relation to legal, regulatory and information security issues:

- As part of the "legal risk assessment", legal issues should be approached from the very beginning of the development process of a telemedicine service.
- Professionals should not be required to obtain any telemedicine-specific accreditation.
- Responsibility and legal liability issues must be clarified on the relevant level: national, regional or local. The "tele-patient" must be informed about who is responsible and who is

[1] These items are listed in the order in which they feature in the questionnaire.

liable for the service.

- Crossing of organisational, sectorial, regional and national borders should be sorted out, and dealt with, as a part of "the legal risk assessment".
- National guidelines are recommended, based on a common understanding of some basic principles of the use of telemedicine.
- Use of telemedicine services must be based on the patient's informed consent (as is the case with all health services).
- Patients' rights must be taken care of: examples include the right to information about the appropriate health care service, and the use of telemedicine. The institutions involved should have policies and guidelines that state clearly the legal and security requirements and responsibilities related to their telemedicine services.
- The health personnel should be given information about data management procedures and the identity of the data controller.
- Health institutions should have the necessary infrastructure for secure telemedicine services and access control and confidentiality matters need to be taken care of.
- For new telemedicine services, it is recommended to conduct an "overall risk assessment" in the early design phase of any initiative, and then to repeat the risk assessment towards the end of the development. In this way, information security will be embedded into the design process instead of being developed as an add-on to an implemented service.
- Health professionals working with telemedicine should be offered basic training about data security and legal issues, especially when it comes to the allocation of responsibilities inside their own organisation. Even more importantly, they should know whom to ask when they are in doubt about these issues.

From the data gathered, it appears that many of the routine services described involve only a few patients. On a general basis, the SIG 3 members have wondered whether legal impediments appear to be less important in small projects than in large-scale services. It is a possible explanation for this phenomenon that smaller projects are often anchored locally and either driven by enthusiasts from the health care sector with main focus on the well-being of the patients, whereas other driving forces concentrate on technology and gadgets. This might imply that the legal and security issues are not as thoroughly reviewed and solved at the outset of a telemedicine service as they could have been.

Related to the "Momentum from pilot to routine care" initial model, it is possible to imagine the following scenario. Dealing with legal and security issues from the beginning of the design process might contribute to bridge the gap between the third and the fourth stage of the initial model. This would ease the distance between the various stages e.g., development and pilot project, and implementation and deployment phase.

As well as information security, risk assessments should also be conducted regularly from the beginning of the telemedicine service process. The same should be done for legal issues. This could lead to an embedding of *both* information security and legislation in the telemedicine field. It would prevent any legal and security "surprises" that might occur (currently) when a service in question is intended to become a routine service that is fully integrated in the national health care system. To achieve this degree of embedding, expertise on legal and security issues should be involved in the telemedicine process from the very beginning.

1. Introduction

Legal and regulatory issues are often considered as among the main hindrances to the implementation of telemedicine. This has various reasons. One might be that the current laws and regulations that govern medical practice in most countries were worked out at a time when patients and physicians always met in the same location, face-to-face, and that the health legislation was never meant to apply to health care over distance (Rowthorne, 2010, p.3).

In the *eHealth action plan 2012-2020* published by the European Commission, legal barriers are mentioned in two of the seven listed main barriers for wider uptake of eHealth (COM(2012b) 736, p.5):

- "lack of legal clarity for health and wellbeing mobile applications and the lack of transparency regarding the utilisation of data collected by such applications;
- "inadequate or fragmented legal frameworks including the lack of reimbursement schemes for eHealth services;" [...]

This lack of legal clarity is also described in the "*Commission staff working document on the applicability of the existing EU legal framework to telemedicine services*" from 2012 (SWD(2012) 414, p.4):

> "Member States have long realised the potential of telemedicine and are supportive of its beneficial deployment. Nevertheless, despite widespread awareness of the benefits of telemedicine, its use in the provision of everyday health and care services is still relatively low and one of the reasons identified is the lack of legal clarity."[2]

This situation was already pointed out and made more specific in a Communication from the Commission to the European Parliament in 2008 (COM(2008) 689, p.8):

> "Although telemedicine may be an interesting option for many healthcare facilities, the lack of legal clarity has been repeatedly mentioned in the stakeholders' consultation as an obstacle to its wider use.
>
> The paramount objective in providing legal clarity in this area is to guarantee that telemedicine develops in such a manner that it benefits patient care while ensuring privacy and the highest standards of patient safety.
>
> The lack of legal clarity – in particular with regard to licensing, accreditation and registration of telemedicine services and professionals, liability, reimbursement, jurisdiction – is a major challenge for telemedicine and, in particular, for teleradiology. Cross border provision of telemedicine services also require legal clarification with regard to privacy.
>
> Only a few Member States have clear legal frameworks enabling telemedicine. In some Member States, for a medical act to be legally recognized as such, the physical presence of the patient and the health professional in the same place is required; this is a clear obstacle to the use of telemedicine. Moreover, there are often limitations in law or administrative practice on reimbursement of telemedicine services."

It might be said that, five years later on, we are still struggling with the same queries in this field. This is the reason why the Momentum questionnaire inter alia addresses topics

[2] A footnoted observation at the end of this quote refers back to a European Commission Staff Working Paper of 2009 (cf. SEC(2009)943 final).

associated with accreditation, licensing, professional liability, reimbursement, and the crossing of organisational and national borders in addition to privacy and security issues.

It is well-known in Europe that health care is regulated at a national level in the Member States of the EU. As a consequence, the EU has only a limited legal competency on health regulation matters. However, the EU does have competence on public health issues, a fact that might affect legal and security matters in the health care sector in the long run.

The situation is different when it comes to privacy. Despite the European Data Protection Directive (Directive 95/46/EC), there are considerable variations between the European countries:

> "The European Data Protection Directive is the EU level legislation on privacy to which all Member States in the EU must conform. It sets basic rights of privacy, but the exact interpretation of the practical exercise of those rights is decided in national legislation, which implements the Directive. Thus a certain level of legal certainty around health related privacy exists at EU level, but substantial variations still remain in the fine detail of the implementation of those rights in the Member States." (WHO, 2012, p.25)

It is therefore important to investigate how these issues are considered and handled in different European countries. The legislation governs who can handle sensitive information and restricts the purposes of use. Precautions must be taken so that the legal requirements are met. Security measures are part of these precautions.

Legal and regulatory tools are important when it comes to facilitating the implementation and use of telemedicine and eHealth. Use of telemedicine affects a wide range of relevant legislation and regulations in different fields, such as the protection of privacy, health legislation in general, any legislation concerning telemedicine in particular, and product liability rules (Commission Regulation (EU) No 207/2012). Cross-border health care regulations and specific sets of rules concern data security in general and the health care sector in particular.

It is important to bear in mind that there is a distinction between formal laws (comprehensive or sectorial laws) and complementary low-level legislation, informal rules, and self-regulation (WHO 2012, p.21). The last-mentioned categories act as a support for health professionals who have to comply with the legislation and regulation in force in their daily work "to translate their duty into action". Low-level legislation, informal rules, and self-regulation include so-called "soft law" such as ethical and practice guidelines, social customs, and the norms of various professions. Such sources of literature might be the main reference point or document for those who deliver telemedicine as a daily routine when they need to refer to legislation and regulations that have been adopted in practice. This is the reason why SIG 3 is not only focusing on legislation, but also on guidelines in the telemedicine field.

The aim of this report is therefore to identify the common trends as well as the main differences that occur in terms of the legal, regulatory and security aspects of telemedicine services. As can be seen from the interim 26 responses to the questionnaire, it might be difficult to be conclusive about all the findings in all the areas covered by the survey. It does appear to be difficult to find common trends and main differences in all the contexts. This is mainly due to the fact that several answers to the same question by different respondents turned out occasionally to be incoherent. For example, respondents from the same country responded differently to questions to which there was in fact only one "correct" answer. Nevertheless, SIG 3 found the actual answers to be very interesting indeed. They reveal that being involved in telemedicine services does not necessarily mean that the personnel concerned have a full overview of all the sets of rules relevant in the telemedicine field.

Several topics were considered crucial in the legal and security field by the members of SIG 3 from the very beginning; they were therefore pointed out as being relevant for the questionnaire content. The choice of relevant issues was based on the experience of the SIG 3 team members in general; literature studies; legal and security issues that were reported as causing problems in telemedicine projects; and, last but not least, problems that have been addressed in public and in public documents, both nationally and internationally.

On the basis of this background from the legal and regulatory field, the following subjects were chosen as core fields of interest for further investigation and elaboration[3]:

- Telemedicine legislation
- Accreditation
- Liability and responsibility issues
- Conflicts of law
- National guidelines for clinical responsibility and liability
- Consent
- Ethical approval and concerns
- Data management procedures
- Information security risk assessment
- Information security measures
- Privacy training/education for health professionals
- Mapping of legal, regulatory and security stakeholders.

Several of these topics are also recommended as needing to be highlighted by the World Health Organization (WHO) and the International Telecommunications Union (ITU) in their "National eHealth Strategy Toolkit" when an eHealth strategy is being developed (WHO-ITU 2012). In the first part of the toolkit that concerns how to establish a national eHealth vision, it is explicitly stated that legislation, policy, and compliance are eHealth components that are absolutely required in order to be able to develop an eHealth vision.

The WHO and the International Telecommunications Union (Ibid, 2012) consider it necessary, among other things, to focus on:

> "national legislation, policy and regulatory components that govern how health information is stored, accessed and shared across geographical and health-sector boundaries."

In addition, in eHealth specific policy, it is important to focus on:

> "Policies specifically governing eHealth services, including privacy of health-related data held in digitized format, its use and sharing for research and the public interest."

It is also pointed out that policies on medical jurisdiction, liability for eHealth services (e.g. telemedicine), data integrity, and quality of care, are all relevant topics of great importance. In addition, the respondents to the Momentum questionnaire considered reimbursement issues as vital.

In addition, it is interesting to note that, in other toolkits for implementation such as "Ready, Steady, Go" (Brownsell & Ellis, 2012) it is recommended that the clarification of legal matters should be taken care of in all phases of the implementation process. On a general basis, this 2012 report pointed out that there is much interest in telemedicine, but that few services have become mainstream. It is suggested that to achieve the up-scaling of telemedicine deployment, the complexities of implementing change at organisational, work force, and user levels need to be understood.

[3] These items are listed in accordance with the way in which they were categorised in the questionnaire.

In SIG 3's opinion, it is also important to be aware of the fact that the development, testing and implementation of telemedicine services involve a wide range of professionals who do not necessarily have an in-depth knowledge of the health care sector. In the legal area, it is of great significance for the application of the law to take into consideration that the use of telemedicine does not necessarily require a physical meeting between the patient and health care personnel. This is an important fact because many set of rules, e.g. on liability, were developed at a period when the patient and health personnel always met physically in medical consultations.

2. Telemedicine legislation [Question 23]

This section describes the possible need for change in health legislation in order to facilitate the implementation of telemedicine services. SIG 3 wanted to find out if the respondents' experience is that the legislation in force in the particular country or region allows for telemedicine solutions, or if amendments in the legislation have had to be made before the telemedicine services are implemented. The SIG 3 team also wondered if a change in legislation had been made as a *result* of experience with implementation and use of such services over time, and if people using telemedicine considered legal amendments necessary to ensure a wider implementation of these services. The background for asking these questions is described in the introductory part of this report. Legal hindrances are, and have been for many years, referred to as the main reasons for the lack of sustainable routine telemedicine services within and between institutions and countries and across organisational and geographic borders.

2.1 Synthesis of the answers to the questionnaire

Q23.1 Were changes to healthcare legislation a prerequisite for the implementation of telemedicine services in your country?

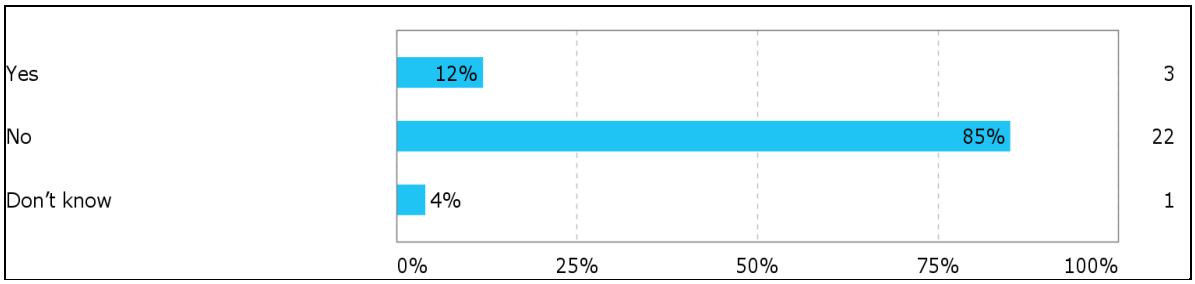

Figure 1: Responses to Q23.1: Were legal changes required for the service?

This is a general question that does not relate to the particular telemedicine service described.

It appears that 22 out of 26 of the respondents answered that changes to the healthcare legislation were *not* a prerequisite for implementation of telemedicine services in their own country. This is an interesting response since, as mentioned, legal barriers have often been cited as being the main reason for the lack of implementation of telemedicine.

However, aside from these 26 responses, two major issues are unknown. The first is if – or how many – services have not been implemented or have not succeeded due to legal hindrances (hence, they did not fulfil the criteria for inclusion in the Momentum questionnaire sample). The second is if the telemedicine services in operation always fulfil all the legal requirements in force. Based on the team members' own experience, and some input provided by questionnaire respondents, we have not excluded as an option that this is not always the case.

Three respondents from two different countries (one from Austria and two from Greece) answered that a change of legislation was a prerequisite for implementation of telemedicine services in their country. The third respondent from Greece intended otherwise, and answered "no" to this question. The third affirmative response is difficult to comment on, as it is one of the answers in an uncompleted questionnaire.

To take Greece as an example: it has a legal provision stating that telemedicine can only be used for advisory purposes. This has obviously been a hindrance for the delivery of health care via telemedicine (see Q23.1 subquestion - below).

Maybe the responses to question 23.1 indicate that due to legal obstacles, many telemedicine initiatives are not followed up in the first place. Hence, services that go against legislation and regulations that are in force are quite simply not piloted or implemented. When it comes to lack of large-scale implementation, it might also be of relevance that, independent of the financing system involved, the financing party will most likely require that the proposed services comply with the legislation in the field.

Q23.1 subquestion: If there is specific telemedicine legislation in your country, please outline its core elements and provide a reference to it.

No core elements were outlined by any of the respondents.

One country – Greece – provided an example of specific telemedicine legislation in the following fields: Minimum conditions met for applying telemedicine, and basic data protection requirements for applying telemedicine. Its core elements could be described as:

"A. Minimum conditions met for applying telemedicine. (ΦΕΚ 150/27-6-11, article 66, paragraph 16) .The specific article of the legislation allows telemedicine, after written consent only (as in the case of a surgery, unless the case of an emergency). In addition, it makes clear that telemedicine has specific limitation in diagnosis, so it is an advisory – additional method, serving the clinical practice. The legislation allows telemedicine services to run in Greece, but sets special minimum regulations.

B. Basic data protection requirements for applying telemedicine. (Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data Article 7a.) Although there is an exemption from the obligation to notify and receive a permit from the National Data Protection Authority when the processing involves medical data is carried out by doctors or other persons rendering medical service, provided that they are bound by medical confidentiality or other obligation of professional secrecy (provided for in Law or code of practice, and data are neither transferred nor disclosed to third parties), the present exemption does not apply to processing personal data within the framework of programs of telemedicine or provision of health care services via Internet. In the case of telemedicine, a special security plan has to be submitted to the National Data Protection Authority and a permit has to be received."[4]

Question 23.2 Have any changes to legislation or other legal rules been made as a result of your particular telemedicine service?

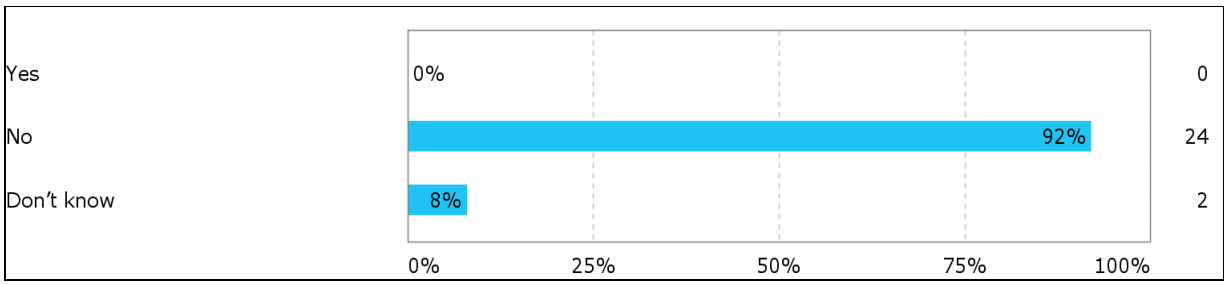

Figure 2: Responses to Q23.2: Have legal changes been made as a result of the service?

This question is related to the specific telemedicine service described.

As the figure shows, 24 out of the 26 respondents answered that no changes in legislation or legal rules had been made as a result of their telemedicine service. Two respondents did not know. This is not surprising, as one could argue that it is doubtful that countries would

[4] Thanks to George E. Dafoulas, of e-Trikala, Trikala, for describing this situation.

change their legislation based on information and experience with one or a few small projects taking place in that country.

However, it could be regarded as a possibility that a need for legislative amendments might be revealed in the wake of successful experience with a telemedicine service. However, this would presuppose the implementation of services that were not (completely) legal, which does not seem to be the case. As mentioned in relation to question 23.1, it may be that potentially useful telemedicine services are never tested or put into operation because of legal hindrances. However, it currently appears that such a supposition is purely speculative, and needs to be investigated further.

If either illegal or somewhat "dubious" services had been tested and had been assessed as useful, one could imagine that legal amendments would be initiated in order to modify the legislation so as to be in accordance with the practice at stake. However, this phenomenon is also not what SIG 3 found.

The input from the sample of 26 respondents has shown that a change of rules and regulations is not initiated, either before a service starts or as a result of a service revealing a need for change of the legislation in force. There is thus a possibility that, if the inclusion criteria for respondents to the Momentum had been somewhat different, the answers to the questionnaire would have shown more diversity.

Q23.2 subquestion: "If there is specific telemedicine legislation as a result of your telemedicine initiative, please outline its core elements and provide a reference to it."

As no respondent answered "yes" to the previous question (Q23.2), no-one pointed out that specific telemedicine legislation had arisen as a result of their telemedicine initiative.

However, there is one comment made to this question from one of the "no "respondents (from Norway). It was pointed out that the telemedicine service in question had fully demonstrated that there is a need for changes in the law. These changes could help to contribute to continuity of care and best quality treatment.

The particular Norwegian service had revealed that it should have been legal for cooperating health personnel employed in different health institutions to access the same electronic health records (EHRs). This is, however, not legal at present, inter alia, because it makes the liability conditions troublesome: Who precisely should act as the data controller with responsibility for determining "the purpose of the processing of personal data and which means are to be used" (LOV-2000-04-14-31, section 2, point 4) in the case of a system that is anchored in, and used by, employees in multiple health institutions? Hence, such access is not legitimate in Norway. The prohibition entails the need for more complicated, and less user-friendly, technical solutions than are considered desirable. A change in regulations could make the implementation of these kinds of tools smoother, easier and cheaper. These points of view have been communicated to the governmental authorities and can hopefully contribute to shed light on this and similar problems.

It is expected that changes in Norwegian regulations will be made in the near future as legal revisions in this field are expected in the country in the course of 2013. One of the main goals behind this revision of the law is to facilitate shared documentation systems for health professionals involved in the same patient trajectory[5], quite independent of where they are located. This will undoubtedly lead to a need for review and possible revision of regulations concerning both responsibility/liability and maybe also financing/reimbursement issues.

[5] A patient trajectory is viewed as "the sequence of encounters a patient has with the healthcare system" (e.g., Bigelow et al, 2005): http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG408.pdf (Accessed 2013-06-27)

Q23.3 Is it your opinion that further changes in legislation in your country are necessary for wider and easier implementation of sustainable telemedicine services?

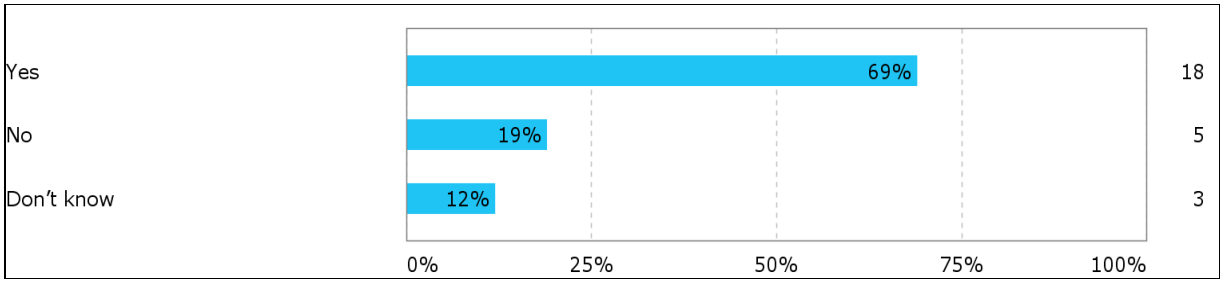

Figure 3: Responses to Q23.3: Are further legal changes needed?

This is a general question which was not related to the particular telemedicine service described.

As many as 18 of the 26 respondents from nine different countries, answered "yes" to this question. In the respondents' opinion, further changes in legislation are necessary for wider and easier implementation of sustainable telemedicine services.

Five respondents, however, answered "no". In their opinion, no change in legislation is necessary for wider and easier implementation of sustainable telemedicine services. It is worth mentioning that these respondents came from five different countries, and that all five countries described more than one service in the Momentum sample. This implies that respondents from five of the countries disagreed on this matter. In four of them, other respondents from the same country deemed a change of legislation necessary for implementation of telemedicine; in the fifth country the other respondent did not know.

A total of three respondents answered "don't know". One of them was combined with two "yes" and a "no" from the same country, one with a "no" and the third "don't know" was the sole answer from that country. This range of responses could be said to illustrate the fact that people hold different opinions, and the answers that the Momentum survey collected are not objective. They are, nevertheless, suitable as a basis for reflections.

Q23.3 Subquestion: If yes, please describe in what way

Different problems with financing were mentioned by several respondents. Several respondents communicated a need for sustainable financial systems on many levels.

It is obvious that people miss clarity with regard to the financing systems related to telemedicine services, and consider that in the long run this lack of clarity is an important barrier for implementation of such services and sustainable operation. Respondents have inter alia stated that there are problems with the financing of equipment in the home, and difficulties with the extent to which a patient fee should operate. Payment for second opinions was also mentioned as problematic by one respondent. Another respondent pointed out that current legislation does not support telemedical services (especially home care, home monitoring, etc.). Service providers are rewarded based on the number of patients that they treat: hence, they may want to treat as many patients as possible. Having good telemedicine home care available might reduce the need for medical treatment and therefore take some of the funding away from the providers of health services. As long as current legislation does not fund telemedicine services in particular, funding remains a big problem.

It might be discussed whether the organisation of financing and reimbursement systems is a legal issue as such. Nevertheless, it should be highlighted that people in the telemedicine

field consider a lack of good financing/reimbursement systems to be a problem that has to be addressed.

Other aspects mentioned for the wider and easier implementation of telemedicine services were the accreditation of health personnel, clarification of the security framework, legal aspects in general, liability issues, and the specification of legislation in general. The need for regulations concerning mobile devices was also mentioned.

2.2 Synthesis of the stakeholder feedback process

It is reported by other SIGs in the Momentum project that the findings in this part of the report seem to be consistent with responses to other parts of the questionnaire.

It seems necessary to define precisely what is meant by reimbursement, as stakeholder feedback revealed that the term can be understood in different ways. In some countries telemedicine is not considered as a medical act. People seem to be inclined to think that, at least in the Momentum project, reimbursement should be regarded as "financing by the healthcare system". Hence, the term "financing" is the most appropriate expression even though financing might be accompanied by different reimbursement models.

It has been suggested by some stakeholders that the significance of legal barriers might be exaggerated on a general basis. Maybe what is being observed is a learning curve with regard to legal matters. This is a controversial statement and could advantageously be investigated further.

It was also suggested that data security is gradually becoming more of a dilemma. If that is the case, the attention to data security in the context of the Momentum project could be occurring because this topic is currently very high on the political agenda throughout the EU.

2.3 Synthesis of the literature review

The aim of this sub-section was to shed further light on the significance of legislation when it comes to the deployment of telemedicine, as described by authors in the telemedicine area. The purpose of this literature review is to bring additional points of view into the discussion, and hopefully contribute with new perspectives. The SIG 3 team has therefore selected some items from the literature that it considered as relevant to this aspect of work on telemedicine legislation and regulation. It is beyond the scope of this project, and thus for this report, to carry out a complete literature study.

In the eHealth Strategies report (Stroetmann et al, 2011) it is pointed out that legal and regulatory issues are among the most challenging aspects of eHealth: privacy, confidentiality, data protection, and liability need to be addressed. It also appears that in most countries the use of eHealth is regulated by the general legal framework, "in particular by laws on patient rights and data protection, and by regulations on professional conduct (Stroetmann et al, 2011, p.IX)".

In the same report, the fact that the amount of legal and regulatory documents available on telehealth is considerably smaller than on electronic health record (EHR) implementations is also raised (Ibid, p. 30). The reasons for this are regarded to be more than one: on the one hand, telehealth applications are less complicated than EHR systems and, on the other hand, "there is a tendency to regard the use of telehealth services to be less problematic under current legal frameworks, so that the usefulness of legal provisions dealing with telehealth specifically is questioned".

However, the three most common issues underpinning regulations are listed as:

a) The requirement to treat a patient in person,

b) The question of accreditation,
c) Liability issues.

3. Legal issues including accreditation, liability, conflicts of law [Question 24]

In this section of the questionnaire, the respondents were asked specific questions relating to a set of concrete legal issues that are believed to be essential and generally challenging when developing, implementing and using a telemedicine service. The issues addressed here are especially relevant to services provided across national borders that use telemedicine applications. Three issues were identified as being of particular need for attention. They are: accreditation, liability, and conflicts of law. Each is described briefly here.

Accreditation

All European (and most other) countries require that health care personnel must obtain a specific authorisation, license or accreditation in order to work in their particular occupations or professions. The means of obtaining such accreditation, requirements and accreditation bodies vary from country to country. In some countries, states or regions with competences in healthcare within the country's borders have the authority to give accreditation to health care personnel.

In Europe, the Directive on the Recognition of Professional Qualifications (Directive 2005/36/EC) makes it more or less a formality for health care personnel in one EU (or EEA) country to obtain accreditation in another. It is necessary to apply for and get the relevant accreditation before being able to lawfully work as e.g. a doctor in the other country.

Accreditation or licensing for telemedicine is a big issue in the United States of America (USA) where medical licensing is issued on a state-by-state basis. According to the Federation of State Medical Boards (FSMB), ten states issue specific licences for telemedicine (FSMB, 2012).

Liability

Liability issues deal with the aspect of health care professionals being held accountable for their actions or conduct. What is the basis of liability? Who can be held liable and for what actions? What are the standards for responsible conduct? How does national and international legislation deal with telemedicine practices with respect to liability?

European legal systems deal differently with liability and responsibility issues. Under some forms of legislation the doctor-patient relationship is based on contractual obligations whereas others rely on codes of conduct and practice.

It is also worth mentioning that how liability and responsibility issues in telemedicine are dealt with under national legislations also affect payment and reimbursement issues. That is, in countries where telemedicine services are limited to e.g. doctor-doctor consultations, second opinion or general medical advice, professional responsibilities are limited and so are the possibilities of being paid for the provision of those services. A more comprehensive discussion of some aspects of responsibility and liability in telemedicine is given in Chapter 18 of the book "Telemedicine in Dermatology" (Nohr 2012).

This SIG thinks that it is important to advise national authorities not to adopt laws, regulations or guidelines that state that telemedicine services can only be used for "secondary services" and not for patient consultations. Dependent on the situation, patient consultations can take place either face-to-face or via means of telemedicine. Both types of consultations can be considered best practice in certain situations, and can supplement each other in a patient trajectory. However, the health professionals involved must always

consider when, and in what situations, face-to-face or telemedicine consultations are in accordance with the requirements for best practice. The consequence of regulations (as mentioned initially in this paragraph) could be that doctors refrain from holding telemedicine-mediated consultations because they are only reimbursed for face-to-face consultations.

Conflicts of Law

Telemedicine offers an opportunity to use various possibilities to provide health care across national borders. Patients and doctors can seek the best and/or the most accessible treatment or advice from health professionals in other countries.

Given the fact that health is regulated on a national basis, cross-border services raise real issues relating to conflicts of laws between nations. It is necessary to assess and clarify these issues before there is any hope of establishing routine telemedicine services across borders. The use of telemedicine and eHealth applications transcends traditional borders and frameworks with the obvious potential of challenging legislation.

Just as important, and as practical, is the challenge of crossing "internal" borders, whether these boundaries exist between organisations, sectors or regions.

3.1 Synthesis of the answers to the questionnaire

This section of the report examines the various issues covered by this section of the Momentum questionnaire in relation to accreditation, liability, and conflicts of law.

Q24.1 Was specific accreditation of health care personnel legally required to implement your service?

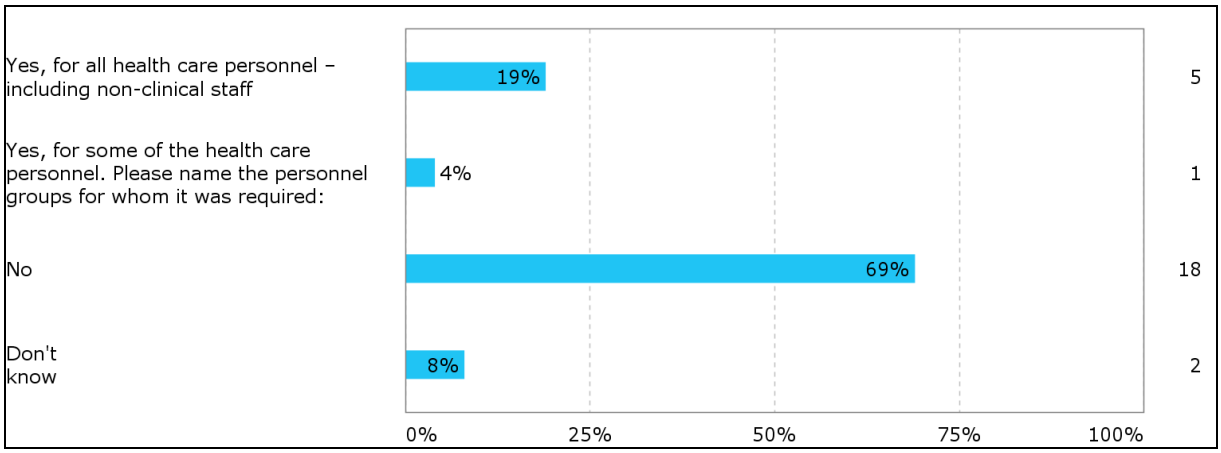

Figure 4: Responses to Q24.1: Did health care personnel require accreditation?

As the above figure shows, more than two-thirds of the respondents from ten of the eleven countries that answered this question showed that they either did not know of such requirements or that specific accreditation was not necessary for the service to be implemented.

The five respondents who answered "yes" represented the same country (Spain). One respondent specified that special accreditation was necessary for some of the health care personnel, namely physicians.

Q24.2 Is there a clear distribution of responsibility for legal liability among the healthcare providers that participate in the delivery of your telemedicine service?

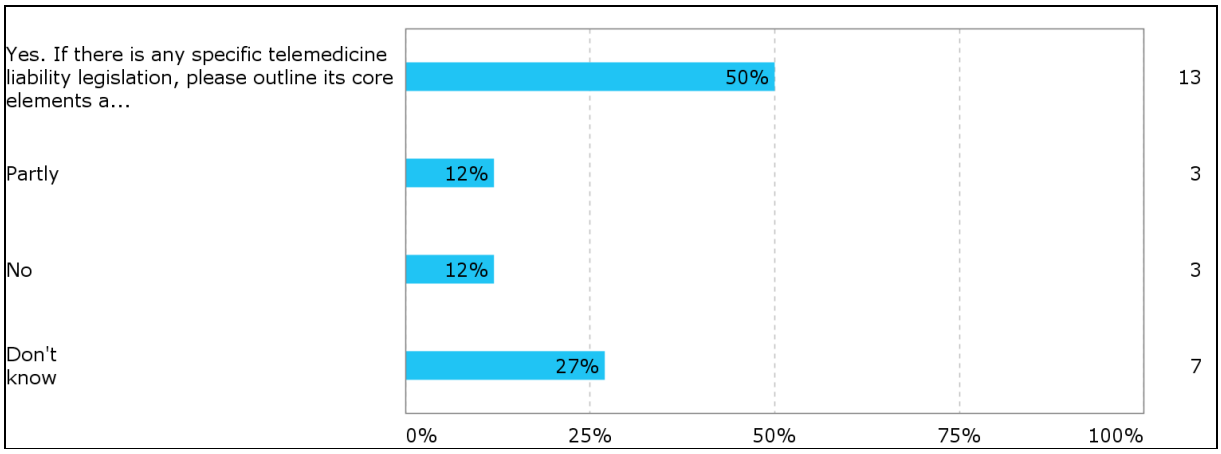

Figure 5: Responses to Q24.2: Are responsibility/liability clearly allocated?

Sixteen of the respondents indicated that there is either fully or partly a clear distribution of responsibility among the personnel involved in the delivery of telemedicine services.

As many as ten of the respondents either answered "no" or "don't" know to this question. In this SIG's opinion, there is little difference between not having a clear distribution of legal liability and not knowing about it. This confusion in status indicates that some positive policy action should be taken in this field.

Q24.2 subquestion (1) – If yes: "If there is any specific telemedicine liability legislation, please outline its core elements and provide a reference to it."

One respondent stated that s/he did not know where such legislation could be found. Another respondent specified that there are Stroke Guidelines in place that could/should adhere to European guidelines.

Q24.2 – subquestion (2) If yes: "If distribution of liability is only partly clear, or not clear, please describe your concerns about the lack of clarity."

One respondent pointed to the fact that there is no specific clarification on liability issues relating to telehealth. The service at stake would have to rely on existing rules on accountability in medicine and nursing.

Another respondent indicated that lack of clarity regarding legal liability leads to uncertainties relating to the delegation of tasks and priorities in action. If this is indeed the case, it shows that this is an important issue to clarify also for the day-to-day practice of the service.

A third response stated that it is often not clear who is responsible for what. More specifically it raised the problem of when responsibility is transferred from a doctor to a service provider or patient – if this is happening at all.

Q24.3 Are liability and/or responsibility issues barriers to the large-scale implementation of your telemedicine service?

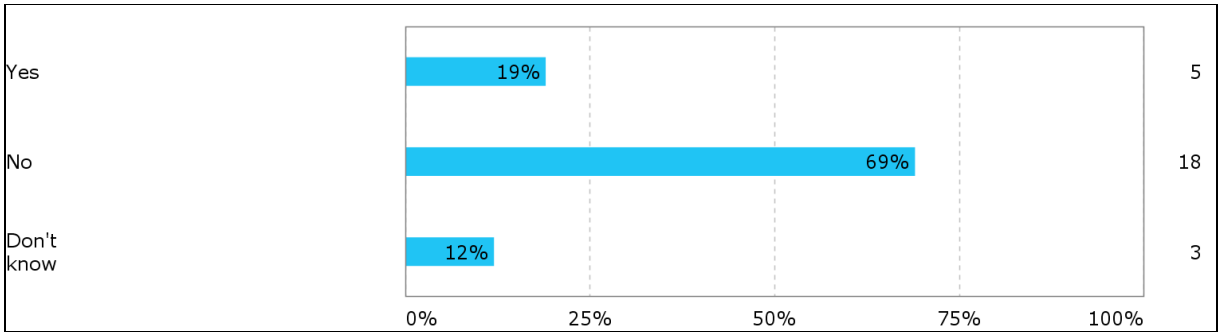

Figure 6: Responses to Q24.3: Do liability issues pose a barrier?

The most interesting, and probably also the most surprising, aspect of responses to this specific question is the fact that such a large majority of respondents found that liability/responsibility issues are *not* impeding the large-scale implementation of services.

The traditional notion is, or has been, that liability or responsibility issues represent real barriers to implementation, especially when one tries to take projects or pilots to the next – routine – level.

One possible explanation of these results is that both services and legal frameworks and what one might call legal conceptions have matured since such an explanation was first formulated. By this is meant that, even though there have been few actual changes to the legal systems in each country (according to previous answers to the Momentum questionnaire e.g., Q23.1/Q23.2), technology, services, performance, knowledge, trust and other factors have all improved. This, together with an increased knowledge of what is actually possible within the existing legal frameworks, has led to a move away from pure assumptions and notions towards assessments and clarifications of barriers and possibilities within the law.

Another explanation could be that this questionnaire was sent to, and replied by, people and organisations that have telemedicine services that are actually in place. It is therefore reasonable to assume that many of these operational services have been "tailored" in such a way that they meet the legal requirements functioning in their particular regions or countries.

Yet another possible explanation is that any illegal services were never realised on a routine basis and are therefore not included in the Momentum study sample.

With regard to this question (Q23.4), those who answered "yes" were asked to elucidate their answer by describing how liability/responsibility issues are considered barriers to large-scale implementation.

One respondent pointed out that these issues will be barriers when services are implemented across hospitals and sectors. Especially the latter point is one that could be anticipated: Increasing the actual scale of a service (in terms of the number of patients or doctors involved) is one challenge. However, in many cases it will be as challenging to increase the scale by making the service work between different hospitals, as well as between different health care levels or across national borders.

Another respondent pointed out what is probably a fact: Medical liability in telemedicine is not well defined. Liability, and especially medical liability, is a comprehensive and difficult issue to address. How one deals with it varies, based on the particular legal system, health care system, technologies, infrastructure, and a whole number of other factors.

Two respondents emphasised that this issue is critical because liability and responsibility issues are crucial for the health professionals themselves.

This matter is very important to bear in mind. Health professionals must meet requirements and legal duties. In those cases where they feel that there are uncertainties concerning these aspects, it is fair to believe that they might find it easier to keep out of the telemedicine realm or service, if nothing else so as to ensure that they remain "on the safe side".

In the Momentum guidelines, effort should be placed on giving advice as to how liability and/or responsibility issues can be assessed and dealt with.

Question 24.4 Does your service cross any borders relating to any legal authorities. Please tick all the relevant options

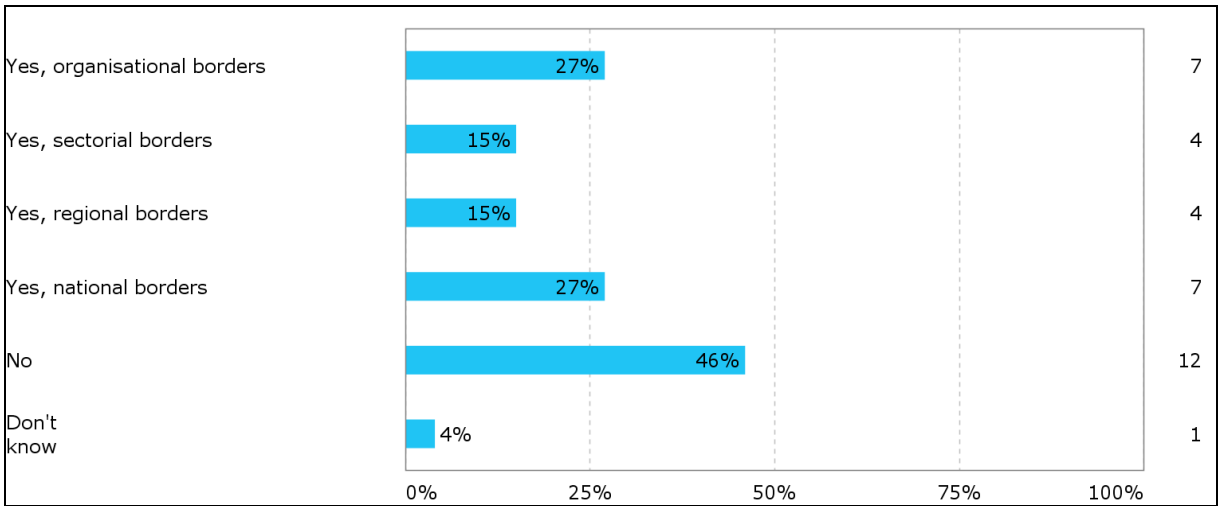

Figure 7: Responses to Q24.4: Does the service cross any legal borders?

This question allowed the respondents to tick more than one alternative response. Due to this fact, the total number of answers on this question is 35.

The figure above shows that twelve of the services in our sample cross no borders. One respondent does not know if borders are crossed. This implies that 13 or 14 of the services cross one "border" or another. The notion of border was sufficiently flexible to contain organisational and sectorial parameters. It is worth noting that an equal number of services cross national and organisational borders (7). Similar numbers cross sectorial and regional borders (4).

It is reasonable to believe that the answers to this question might be somewhat incomplete. One could, for example, expect that services crossing national borders also cross other borders such as organisational and regional ones. This does not seem to be the case, however: according to the respondents, four of the seven services only cross national borders.

As crossing of borders is of great interest and significance for implementation of telemedicine services, it is important to give more exact descriptions of which borders are being crossed and how this will be handled.

Q24.4(1) "If Yes, were any conflicts of law identified as a result of this crossing of borders?

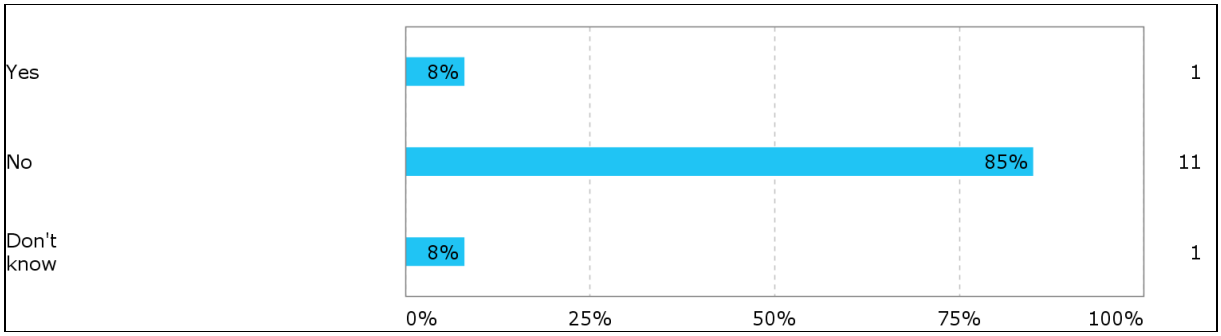

Figure 8: Responses to Q24.4(1): Were there any legal conflicts because of crossing borders?

The large majority of respondents answered that no conflicts of law were identified. This result is probably due to the characteristics of the Momentum sample. Many of the services crossed no borders, and the others are relatively small initiatives that are locally anchored. It is also not known how many telemedicine services was never realised because of legal hindrances related to crossing of borders.

The follow-up question was:

Q24.4(2) "If Yes, please describe the conflict(s) and how they were managed".

The only answer to this sub-question was related to solving a specific issue of data sharing.

3.2 Synthesis of the stakeholder feedback process

Work on stakeholder feedback is on-going during the course of the project.

3.3 Synthesis of the literature review

There is not much literature on these three issues (of accreditation, liability, and conflicts of law) in the form of scientific articles or books. The most relevant sources can be found in official documents, statements and guidelines (or similar) from professional associations. Most of these documents cover the various national levels, with the exception of EU-related documents.

An important European stakeholder is the Standing Committee of European Doctors.[6] The association has, among other activities, published Ethical Guidelines in Telemedicine. The University of Navarra in Spain has included these on its website[7].

To what extent these, and other, guidelines are being used, and how they are being used, is not known to the SIG, and could probably be an item worth investigating further. The literature review will be followed up on these matters through the project period.

[6] http://www.cpme.eu/ (Accessed 2013-06-27)
[7] http://www.unav.es/cdb/cpme97a.html (Accessed 2013-06-27)

4. National guidelines for clinical responsibility and liability [Question 25]

This section describes the situation with relation to frameworks or standards of professional responsibility for a doctor and/or other health personnel to treat patients without face-to-face contact. It also includes an investigation of national guidelines or recommendations regarding the allocation of clinical responsibility and legal liability among healthcare professionals and health care institutions when they use telemedicine services.

The respondents were asked to specify if it was considered to be in accordance with standards for professional responsibility for a doctor to treat patients without face-to-face contact in their country. The background for this question was that some national legal systems require face-to-face contact for a medical consultation to be legally valid. This is, for example, the case in Poland where the Polish Act on the Professions of Physicians and Dentists requires personal examination of a patient to make a diagnosis (SWD(2012) 414, p.5). The same principles apply to Austria and Malta. In Austria use of telemedicine might be accepted in emergency situations. In Malta, online interaction or use of telephone are not considered to be professional practice (Stroetmann et al, 2012).

The SIG also wanted to know if national recommendations and guidelines for distribution of clinical responsibility and legal liability are applicable in the respective countries.

As is presented initially in the Introduction to this report, guidelines are regarded as “soft-law”, and are meant to support good practice in daily work. The term “guidelines” is often used “loosely in the literature” and is “often [being] used interchangeably with standards” (Loane, 2002). However, the two terms of guidelines and standards should be clearly distinguished from each other. In this SIG's report, we have regarded guidelines as described in the sense used by Loane and Wotton (2002) who state that while standards “imply technical compliance with rigid and defined criteria; guidelines imply the following of recommended, and to some extent flexible practices”. The purpose of guidelines in general is described as being to facilitate best practice and to improve “the consistency and efficiency of health care, based on scientific and clinical research”.

The authors of the above-mentioned article pointed out, in 2002, that guidelines in the telemedicine area were scarce, which indicates that telemedicine is still not in routine use. It seems that, a decade or so later, this could still be the case. Loane and Wotton (Op. Cit., 2002) concluded that consensus on guidelines for telemedicine must be achieved, the approach should be international, and the guidelines should be worked out in cooperation between clinicians and what they call “telemedicine specialist[s]”.

In a review from 2008 (Jack & Mars, 2008), the authors searched for guidelines for the ethical practice of telemedicine all over the world. The aim was to find out the need for ethical guidelines for the use of telemedicine in South Africa. Twenty-one “telemedicine guidelines” were obtained as a result. They mainly focused on “clinical, operational or technical aspects” and tended to be specific to a sub-speciality in the medical field. Only three countries and one international association had developed ethical guidelines at that time. However, eight guidelines dealt with ethical issues, among them “codes of conduct for health websites, doctor-patient relationships, consent and communication, security and confidentiality”. In addition, several medical disciplines had established their own national guidelines. “Medical responsibility” is mentioned as one of the topics included in addition to “doctor-patient relationship, informed consent, confidentiality, data security, adequacy of records, data standards and quality, clinical competence, and licensure”.

It would be of great interest to re-investigate the situation today. It seems that non-English language sources were excluded in this 2008 mapping of guidelines (as Denmark, Norway, and Sweden all had guidelines at that time, but none of these are included in the review). However, the Finnish guidelines were included, probably due to the fact that they were issued in English.

The question of clinical responsibility and legal liability are recurring terms. The SIG has chosen to use the following definitions[8]:

Clinical responsibility: Any task or duty involving the professional component of medical practice, which requires the exercise of clinical judgement with respect to patient care.

Legal liability: A comprehensive legal term that describes the condition of being actually or potentially subject to a legal obligation.

Underpinning the majority of the services described in the Momentum project is the fact that it is considered not only to be possible to provide health care by means of telemedicine, but also that this is a responsible action to take. Health personnel and patients do not necessarily meet physically.

With telemedicine, a medical service is provided based on the information collected via a telemedicine service, such as video conferencing, images, text, and oral communication. It is up to the health personnel concerned to make sure that the quality of the received information is good enough to make a decision in accordance with the principles of best practice and standards for professional conduct.

Some countries, such as Denmark and Norway, have worked out guidelines in this field. The distribution of clinical responsibility among the health care professionals, and legal liability between the institutions involved, are important issues in these guidelines.

4.1 Synthesis of the answers to the questionnaire

The analysis of the questions and sub-questions that follow deal with issues of professional responsibility and legal liability.

Q25.1 Is it within the framework or standards of professional responsibility for a doctor to treat patients via telemedicine (without face-to-face contact) in your country?

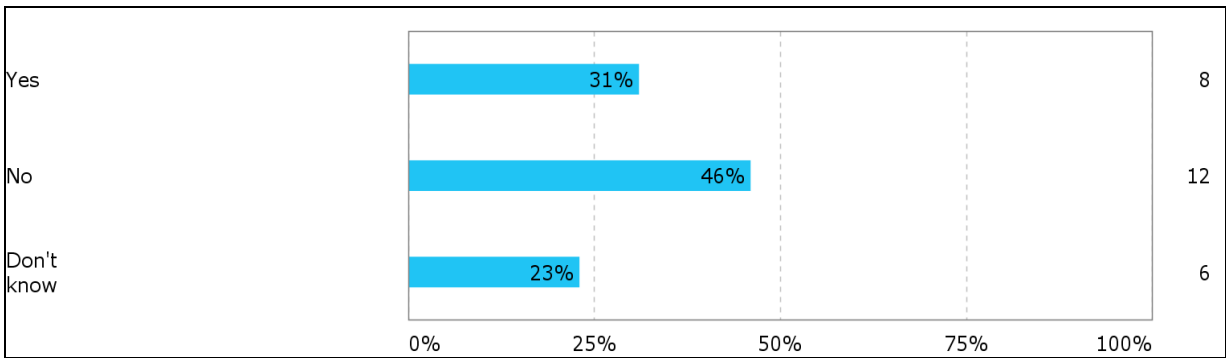

Figure 9: Responses to Q25.1: Does a doctor use telemedicine routinely?

An important barrier to the implementation and use of telemedicine is when national, professional or other legal standards prohibit doctors and other health care personnel from treating patients via telemedicine without face-to-face contact. Such regulations represent serious obstacles for the use of telemedicine for the diagnosis and medical treatment of

[8] http://legal-dictionary.thefreedictionary.com/liability (Accessed 2013-06-27)

patients. They imply that telemedicine can only be used for other health-related services, such as giving general advice, second opinion, and holding meetings. The SIG therefore wanted to know if such directions have been given to the survey respondents by their government, professional associations or others.

Twelve respondents from seven different countries answered that it is not within the framework or standards of professional responsibility for a doctor to treat patients via telemedicine. As a result of further investigation, it has turned out that several of the respondents were subject to a misunderstanding, and their answers were therefore not correct. This misunderstanding applies to at least four or five of the responses to this specific question.

Even if there are only a few incorrect answers to Q25.1, it is obvious that this is a fundamental question of great interest and importance in the telemedicine field, both within each country and related to cross-border services.

It is, however, important to bear in mind that, even if the national legal frameworks do prevent doctors from delivering medical treatment or consultations via telemedicine, there are numerous other telemedicine services that can be useful and serve both patients and the health care system well.

Question 25.2 Are there any national guidelines or recommendations regarding distribution of clinical responsibility between the health care professionals when they use telemedicine services?

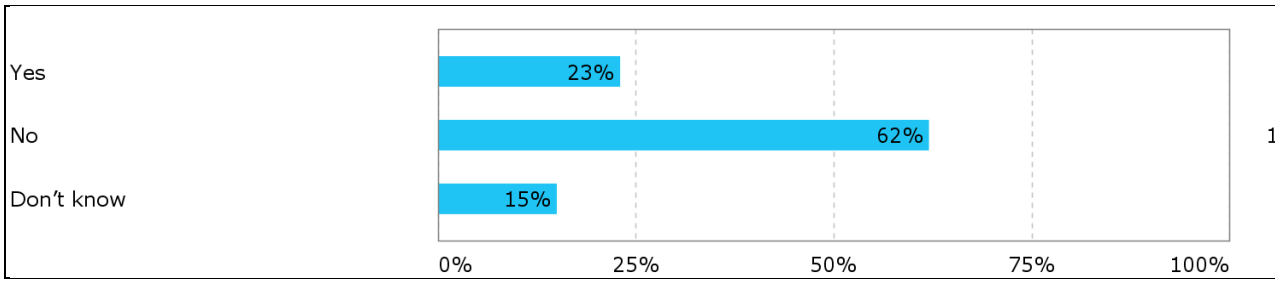

Figure 10: Responses to Q25.2: Are there guidelines for clinical responsibility?

This question focused on whether there are any *national* guidelines or recommendations that relate to the distribution of clinical responsibility.

Sixteen respondents answered "no" to this question and four did not know. Six respondents from three different countries reported that there are guidelines/recommendations concerning distribution of clinical responsibility when telemedicine services are delivered in their country. These answers had to be further investigated, as answers from the same countries were contradictory. After checking, it turned out that for two of the responses, the correct answer is in fact "yes". In addition, one of the negative answers should have been "yes". This means that three different countries have national guidelines after all. However, one of the set of guidelines turned out to be in fact regional in coverage.

The conclusion means that there are national guidelines regarding distribution of clinical responsibility in two countries: Denmark and Norway.

Q25.2(1) "If yes, which institution is responsible for the guidelines?

In Denmark and Norway, the Ministry of Health is the body that is responsible for the national telemedicine guidelines.

The third positive answer turned out actually to be either contract-based or only regionally applicable. In the case of contractors, the contractual partners are the regional health care

service provision insurer and the individual consortium of healthcare providers (hospitals or group of entities). However, each region is free to issue guidelines.

Q25.3 Are there any national guidelines or recommendations regarding distribution of legal liability between institutions involved in telemedicine services?

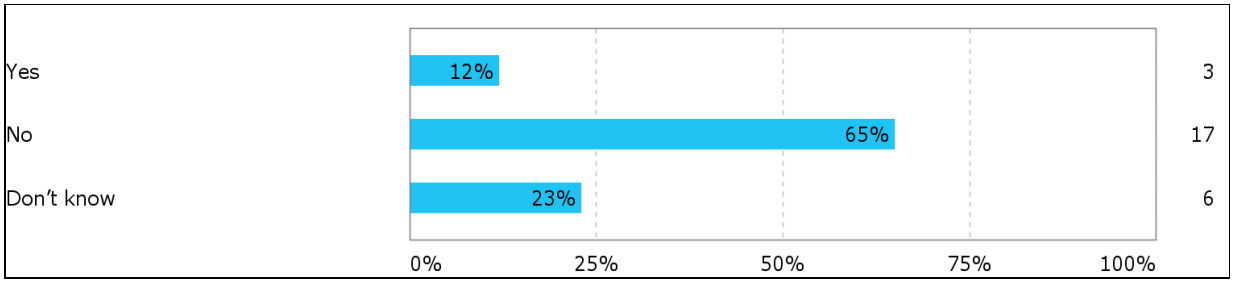

Figure 11: Responses to Q25.3: Are there guidelines for distribution of legal liability?

Three respondents from two countries (Norway and Sweden) reported that there are national guidelines or recommendations with regard to legal liability between institutions involved in telemedicine services.

Further investigation revealed that Denmark and Norway have such guidelines.

Q25.3(1): If Yes, which institution is responsible for the guidelines?

The responsible body was the Ministry of Health and Care Services.

4.2 Synthesis of the stakeholder feedback process

No stakeholder has so far commented on these issues. It could be of interest to discuss suggestions for possible guidelines in a focus group or in a workshop. It would, as a minimum, be of interest to shed light on the following subjects:

- Present the existing guidelines in Denmark and Norway, and the two countries' experiences.

Some questions could be posed, such as:

- Do we need (national) guidelines?
- Would guidelines make implementation of telemedicine services easier?
- If so, on what level should they be designed?
- More specifically: Is there a need for telemedicine guidelines in each country? If so: Should they be harmonised? In what way?
- Should there be guidelines available on an EU-level?
- On what ethical principles should possible guidelines be based?
- Which topics should be included in any guidelines?
- How should the chosen topics be handled and formulated?
- Is a suggested roadmap to guidelines needed?

4.3 Synthesis of the literature review

It is proposed that this sub-section draws on and describes any relevant literature with regard to framework or standards of professional responsibility for a doctor to treat patients without face-to-face contact. This could serve as a starting point for reflections around telemedicine services and responsibility/liability.

This SIG will, however, search for some input on good literature concerning the allocation of clinical and legal responsibility and liability for health personnel involved in delivering

telemedicine services. The team will also look for literature concerning the need for face-to-face contact between health professionals and patients.

5. Consent, ethical approval and concerns [Question 26]

Consent is a basic and fundamental condition for any examination or treatment of a patient as well as a basis for the processing of medical information. Over the years, various aspects of consent have been widely discussed in the telemedicine world. This is not surprising, given the fact that many telemedicine services represent new ways of both examining and treating patients, and telemedicine and eHealth process patient information electronically.

Having said this, it should, however, be noted that many telemedicine services are in routine practice today. Electronic patient records and electronic sharing of information are more the rule than the exception in many countries. Bearing this development in mind, it is relevant to ask how necessary or relevant it is to emphasise the need for *explicit* and/or *written* consent to underpin the use of electronic tools in the delivery of health services. As medical practice by means of such tools becomes more and more routine, known and common, the need for specific patient consent to this practice may no longer be relevant. The most well-known example of this change in the practice of consent is teleradiology. Digital radiology is nowadays standard in most hospitals, and not subject to explicit consent from the patient.

There are a few necessary background observations that can be made.

The patient should still be informed about the procedures in question, and the patient shall always have the possibility to opt out of any suggested service, including the telemedicine service. (Consent can be presumed.)

Telemedicine is still developed in research projects. In research, consent is a prerequisite when a project includes patients. Projects usually need approval from ethical committees, and patient consent must be gathered in this process.

The right to consent (and not to consent) is a *right* for the patient. Legislation on patients' rights is more and more common in many countries. Two years ago, the EU passed the so-called Patients' Rights Directive which includes articles on telemedicine and cross-border health care (Directive 2011/24/EU).

5.1 Synthesis of the answers to the questionnaire

This section describes issues relating to consent, ethical approval and concerns about telemedicine deployment.

Q26.1 Do patients need to give their explicit and informed consent in order to receive the telemedicine service?

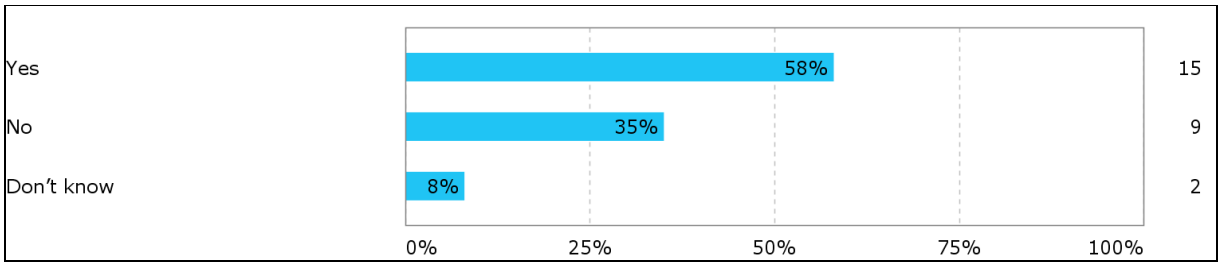

Figure 12: Responses to Q26.1: Do patients need to give consent?

Question 26.1 deals with the all-important issue of consent. Consent is a fundamental basis for care in three aspects: with few exceptions, all treatment must be based on the patient's consent; so too, must the processing of medical information about the patient, including sharing of this data.

It could be of interest to investigate how the 35% of negative answers give their consent when receiving a telemedicine service.

The table above shows that more than half of the services included in this study are based on explicit (and in one aspect, specific) consent from the patient before the service is provided.

Q26.1(1): In the event that patients have to give their informed consent, how do they do it?

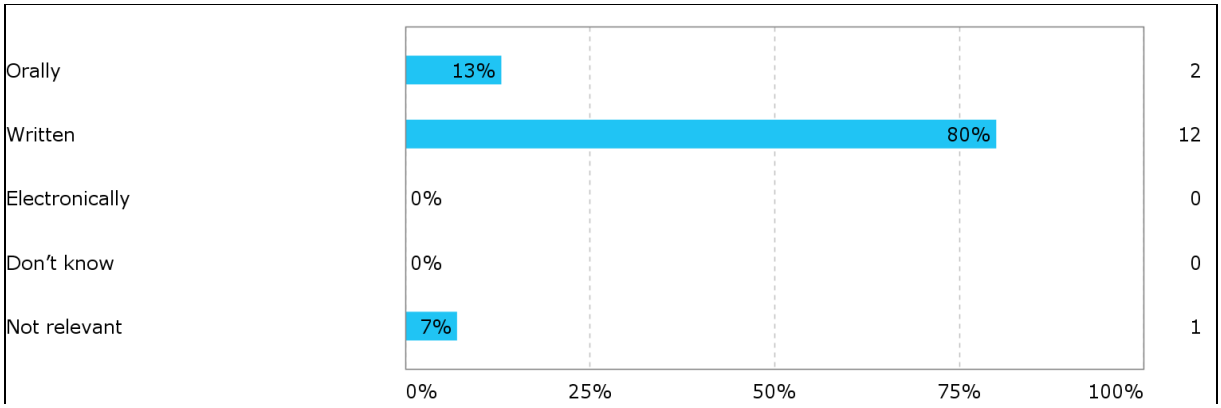

Figure 13: Responses to Q26.1(1): If yes, how do they give consent?

This figure speaks for itself. Most services ask for consent and the vast majority of these formalise the consent in written form (12 respondents from seven different countries).

Q26.1(2): How is information about the telemedicine service provided to the patients?

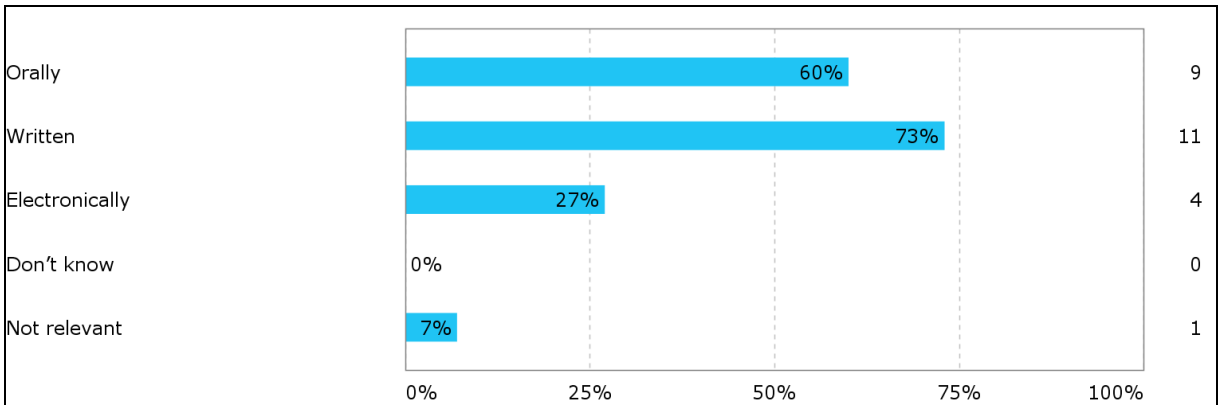

Figure 14: Responses to Q26.1(2): How are patients informed?

Given the responses to the previous question (Q26.1) and sub-question, this is not a surprising result. One should consider that it is likely that patients are actually informed in more than one way, maybe by written material, information given directly by the health care personnel, and via information e.g. on websites or sent via email.

Question 26.2 Has the telemedicine service been assessed by an ethical committee at any time?

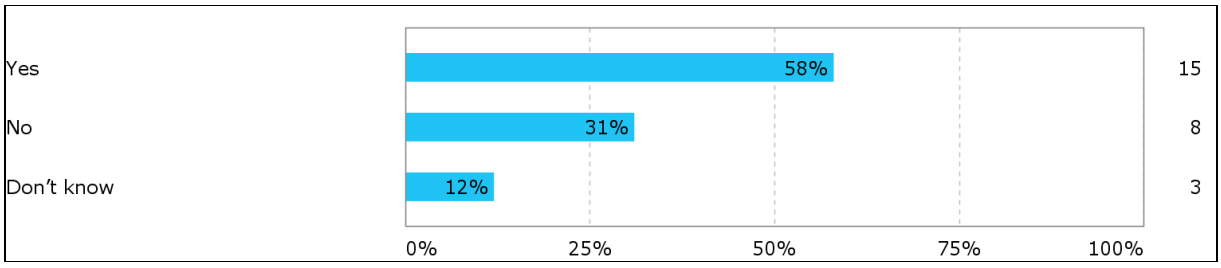

Figure 15: Responses to Q26.2: Was there an ethical assessment?

Most services in the sample (15) have been assessed by an ethical committee. In general, many of the telemedicine services are either research projects or are based on quite recent research projects. That might also be the case in the Momentum sample, but this matter was not investigated. The moment a service emerges from the research realm, it is no longer subject to assessment by a research ethical committee. It might, however, need to be given an ethical assessment by other ethical committees on a national, regional, local or institutional level.

Q26.2(1) If yes, did the ethical committee have any comments or reservations related to legal, regulatory or security issues.

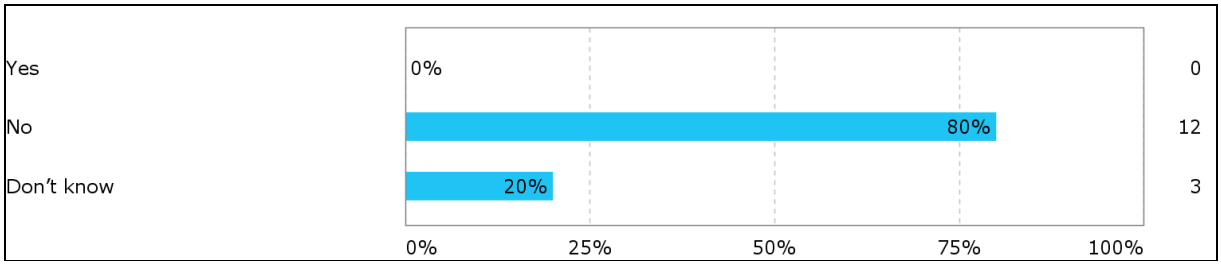

Figure 16: Responses to Q26.2(1): If yes, were there legal, regulatory or security concerns?

No one answered yes to this question.

Q26.2(2) If any ethical issues have been raised in relation to the telemedicine service by anybody, please describe which they were and by whom they were raised

There was one concrete answer to this sub-question:

> "The transmission of personal data between patient's home and hospital should be protected in a highest achievable level."

5.2 Synthesis of the stakeholder feedback process

Work on this issue is on-going during the project period.

5.3 Synthesis of the literature review

In the legal literature, consent is a big issue. There are probably hundreds of articles and books on this topic. For a very comprehensive presentation on this issue, the SIG can recommend the works of Professor Elisabeth Rynning of University of Uppsala, Sweden (see for example (Rynning, 1994)).

The above-mentioned guidelines from CPME (see Q24) also include the issue of consent, as do many other guidelines and recommendations. The American Telemedicine Association (ATA) has issued a number of practice guidelines on different aspects of telehealth. The importance of basing practices on consent is emphasised in all of these guidelines.

A quick search on the word "consent" on the website of the Journal of Telemedicine and Telecare[9] returned no fewer than 456 results. It is not within the scope of this project to go through such a large amount of literature, but this illustrates the importance of, and the interest in, this issue.

[9] http://jtt.sagepub.com/ (Accessed 2013-06-27)

In the United Kingdom (UK), the findings of the Whole System Demonstrator programme[10] are worth exploring. As the programme claims to be the world's largest randomised control trial of telehealth and telecare, its findings should produce valuable input to the telemedicine community not only on efficiency but also on patients' rights and consent issues.

Earlier this year (2013), Springer-Verlag issued a book entitled "eHealth: Legal, Ethical and Governance Challenges" (George et al, 2013). The book includes articles on a number of aspects of telemedicine and eHealth with a special focus on law and ethics.

[10] https://www.gov.uk/government/news/whole-system-demonstrator-programme-headline-findings-december-2011 (Accessed 2013-06-27)

6. Data management procedures [Question 27]

This section describes data management procedures involved in telemedicine deployment.

The entity who determines the purpose of the data processing is the *data controller* in the organisation. Personal data may only be processed according to requirements in national provisions adopted pursuant to Directive 95/46/EC on the protection of the personal data of individuals. The data controller is responsible for ensuring that this data processing is taken care of. A *data processor* is a body which processes personal data on behalf of the controller.

In Article 17 of the Directive, regarding the security of processing, the following is stated: "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." (Directive 95/46/EC)

Data management procedures include clarifications of responsibilities regarding the processing of personal data, and necessary agreements between the data controller and the data processor.

6.1 Synthesis of the answers to the questionnaire

Important questions related to data management procedures are whether the organisational responsibility for security and legal standards is known to the users of the telemedicine service; whether a data controller has been identified; and whether any changes to the usual data management procedures had to be modified before the telemedicine service could be used and, if so, what changes were made.

Q27.1 Is it obvious to you which organisation or individual is responsible for the security and legal standards of your telemedicine service?

The reason for asking this question is that it is important for those responsible for telemedicine services to know who to consult in order to sort out which requirements are applicable, to what degree they are implemented, and to whom they should report any breach of security and legal requirements.

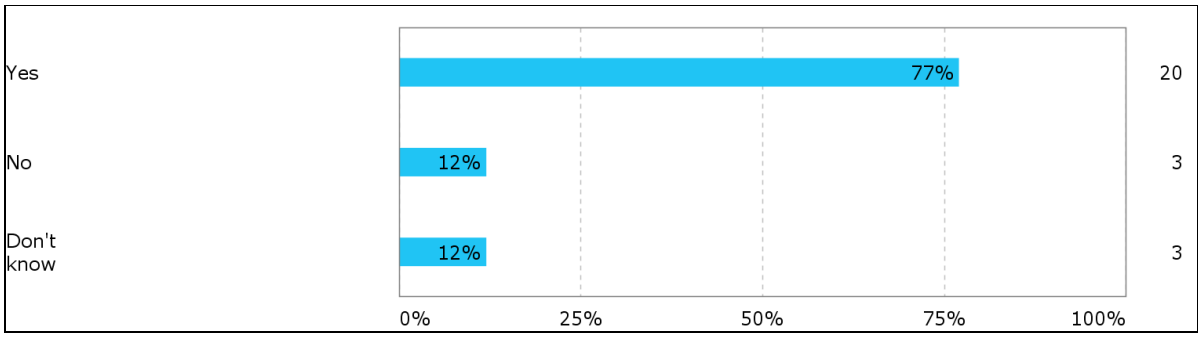

Figure 17: Responses to Q27.1: Is it clear who is responsible?

As the responses show, it seems to be obvious for the majority of the respondents *who* is the responsible body for the security and legal standards of the telemedicine service. Note, however, that nearly one-quarter (6 out of 26) of the respondents do not know who is responsible for security and legal standards.

Question 27.2 Has a data controller been identified?

This question is related to the previous question in the way that, if it is obvious who is the responsible body for security and legal requirements of the service, it should also be evident who the data controller is.

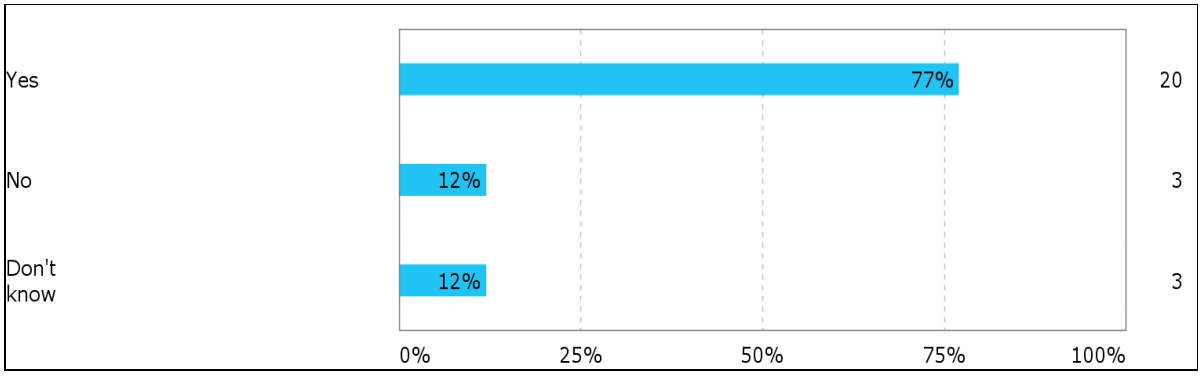

Figure 18: Responses to Q27.2: Has a data controller been identified?

Even if the numbers of yes/no answers are equal in volume in response to Q27.1 and Q27.2, two respondents answered *no* to the first question (Q27.1) and *yes* to the second (Q27.2), and two other respondents answered the opposite. This indicates that these respondents misunderstood one of the questions. It might be that the respondents are unfamiliar with the term "data controller" or that they do not know about the data controller's responsibility for information security.

Q27.3 Did you have to make any changes to your normal data management procedures to implement your telemedicine service?

By "data management procedures" was meant policies and procedures related to the management of data in the organisation, including definitions of responsibilities.

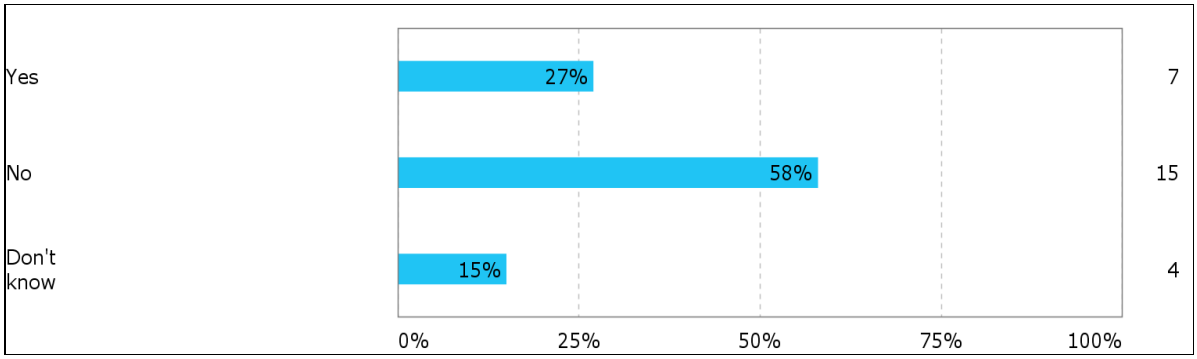

Figure 19: Responses to Q27.3: Were there changes to data management?

More than half of the respondents (15 out of 26) stated that they did not have to make any changes to their normal data management procedures. One change mentioned by some of those who had to make such changes was the establishment or improvement of security policies, including responsibilities and an authorisation regime for access to certain data. This is precisely the type of answers that this SIG was looking for. Some of the respondents reported that they had to establish a new infrastructure for gathering and exchange of personal health information – which is not exactly to what the question was referring.

6.2 Synthesis of the stakeholder feedback process

Work on stakeholder feedback is on-going during the project period.

6.3 Synthesis of the literature review

In a study on Legal and Regulatory Aspects of eHealth, the European Health Management Association (EHMA) describes the duties of a data controller as follows:

> "Among the duties imposed on the data controller, he or she has the responsibility to protect the personal data he or she holds, and therefore to take technical and organisational measures ensuring their security and confidentiality. A data controller may pass data to a third party to act as a data processor to process the data on his or her behalf, but the data controller will have to comply with some requirements in order to be allowed to do so. In a medical setting one of the key legal issues affecting the data processor is that he or she must have a legal or a contractual duty to maintain data confidentiality. This means in practice that the contract between the data controller and the data processor must include a clause that the data processor shall act only on instruction of the data controller and that he or she is also legally responsible in case of any breach of data confidentiality." (EHMA, 2006)

In telemedicine services where two or more organisations are involved, it must be clarified who is the responsible data controller(s). In the UK, the Department of Health (DH) has proposed Guidance for shared records. This states that:

> "There is no single data controller responsible for the shared environment - participating organisations are therefore data controllers in common for the information within the shared environment."

The guidance says that organisations need to ensure that all data protection requirements are being satisfied.[11]

Data protection issues in Europe, especially those that focus on EHR information, are discussed in a paper from 2008 (Sellars, 2008), in which the role of data controller is also briefly discussed.

[11] http://www.ehi.co.uk/news/ehi/8146/dh-guidance-for-shared-records (Accessed 2013-06-27)

7. Information security risk assessment [Question 28]

This section describes information security risk assessment pertinent to telemedicine deployment.

Assessment of risks is important in order to reveal vulnerabilities and possible threats to information security, and to be aware of which security measures should be implemented.

In the EU Directive on protection of personal data (Directive 95/46/EC), assessment of risk is (indirectly) mentioned in Article 17: *"- shall ensure a level of security appropriate to the risks".*

It is, however, unclear to what extent the requirements from the directive are implemented in the different countries. Indeed, plans are underway to introduce a new regulation on data protection that will replace the terms and conditions of the 1995 directive. As a background for the proposal for a new EU regulation on protection of personal data (COM(2012) 11), the European Commission states that:

> "The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the way data protection is implemented across the Union. (...) This difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC."

The proposed new regulation refers to risk assessment in Article 33, which introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations.

7.1 Synthesis of the answers to the questionnaire

This sub-section investigates whether an information security risk assessment of the telemedicine service has been performed i.e., assessment of risks to confidentiality, information integrity or availability. In addition, question 35 in the questionnaire asks whether there are methods in place for risk management of devices and/or systems of the telemedicine service (e.g. to ensure effectiveness, security and safety). (See also Del 7.1 undertaken by SIG 4 on Technical Infrastructure and Market Relations.)

Q28.1 Has an assessment of risks to the information security been performed, i.e. risks to confidentiality, information integrity or availability?

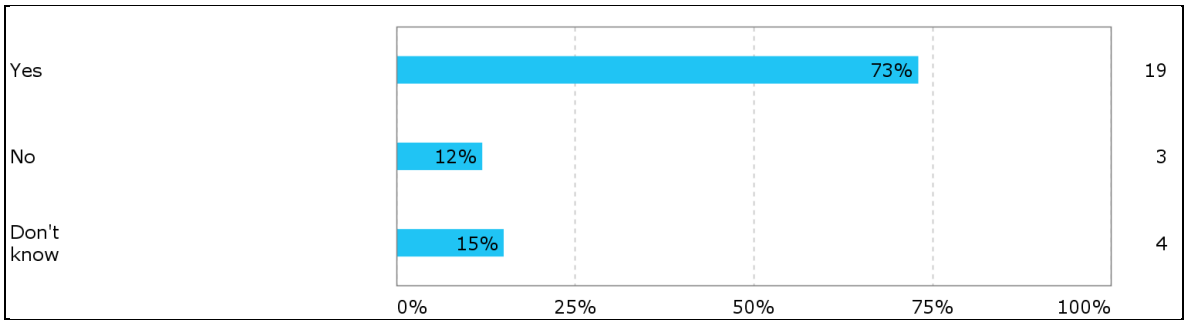

Figure 20: Responses to Q28.1: Was there a risk assessment?

Nearly three-quarters of the survey respondents (19 out of 26) know that a risk assessment of information security has been performed for their telemedicine service. This indicates that there may be a requirement for risk assessment in most of the regions or countries answering the questionnaire. It remains to be investigated whether that is the case.

For seven out of the 26 respondents, the answer is different in question 35 of the survey. Of these seven, 3 answer *yes* that a risk assessment has been performed (question 28), but they do not know if there are any methods in place for risk management (question 35). Most of those who answer *no* or *don't know* to this question also answer *no* or *don't know* to question 35.

7.2 Synthesis of the stakeholder feedback process

Work on stakeholder feedback is on-going during the project period.

7.3 Synthesis of the literature review

Security risk analysis is a basic requirement of ISO 27002 (ISO/IEC 27002:2005), which is internationally recognised as the generic information security standard.

ISO 27799, "Information security management in health" (ISO 27799:2008), specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines.

The standard points at the importance of information governance: "As health organisations become ever more critically dependent on information systems to support care delivery (...), it becomes increasingly evident that events in which losses of integrity, availability and confidentiality occur may have a significant clinical impact. ... All countries and jurisdictions will undoubtedly have case studies where such breaches have led to misdiagnoses, deaths or protracted recoveries. Clinical governance frameworks therefore need to treat effective information security risk management as equal in importance to care treatment plans, infection management strategies and other "core" clinical management matters."

Methods for risk assessment

The International Organization for Standardization (ISO) has one generic standard for risk assessment (ISO 31000:2009), and a specific standard for information security risk management (ISO/IEC 27005:2011).

There are many methods and guidelines for how to conduct risk analysis, and organisations often adapt existing risk management methods to their own environment and culture, thus creating their own method. But all include the three central tasks of:

- identifying threats and possible unwanted incidents,
- analysing impacts and likelihood of the identified threats,
- evaluating risks with respect to acceptance criteria.

A number of papers from the Norwegian Centre for Integrated Care and Telemedicine (NST) describe one way to do risk assessment (Bønes et al, 2007; Henriksen et al, 2009; Bolle, 2011).

The European Network and Information Security Agency (ENISA) has a site which is a central hub of information about risk management / risk assessment[12]. The site encompasses a variety of information pertinent to risk management and risk assessment.

[12] http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms (Accessed 2013-06-27)

8. Security issues [Question 29]

This section describes some specific security issues involved in telemedicine deployment.

8.1 Synthesis of the answers to the questionnaire

This sub-section describes the methods of authentication used to obtain access to the telemedicine service by healthcare professionals or other health service employees; whether the user is logged out after a certain idle time; whether data transfer is encrypted; whether communication is performed via a VPN connection; and whether all access to the system or service is logged and whether anyone inspects the logs. All these aspects of security are important in order to ensure an adequate level of information security for the telemedicine service.

Q29.1 Does the telemedicine service give a healthcare professional or other health service employees access to patients' health information?

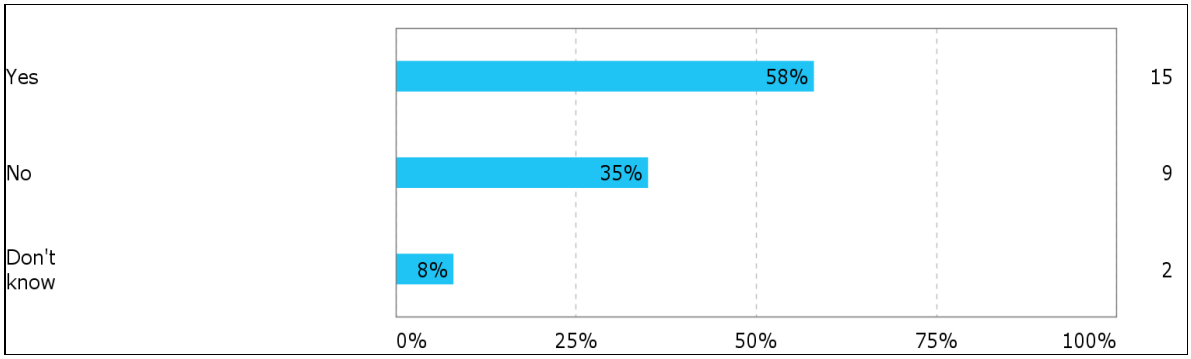

Figure 21: Responses to Q29.1: Can health service employees access patient information?

More than half of the respondents (15 out of 26) answered *yes* to this question. However, more than one-third (9 out of 26) of the respondents, stated that their service does not give access to patients' health information.

To this SIG, this indicates that the term "access to patient's health information" is not interpreted in the same way by all respondents. Health information does not have to be written or readable electronic information. Listening to and viewing patients via video conference systems also implies having access to patients' health information. It seems, from the answers to these questions, that several of those who answered *no* to this question, are dealing with services that are based on video conferencing.

When looking at the 26 telemedicine services dealt with by the Momentum survey, we would assume that nearly all of them would imply that there is access to patients' health information.

Q29.1(1) If Yes, which methods of authentication are used to obtain access to the telemedicine service, including the patients' health information?

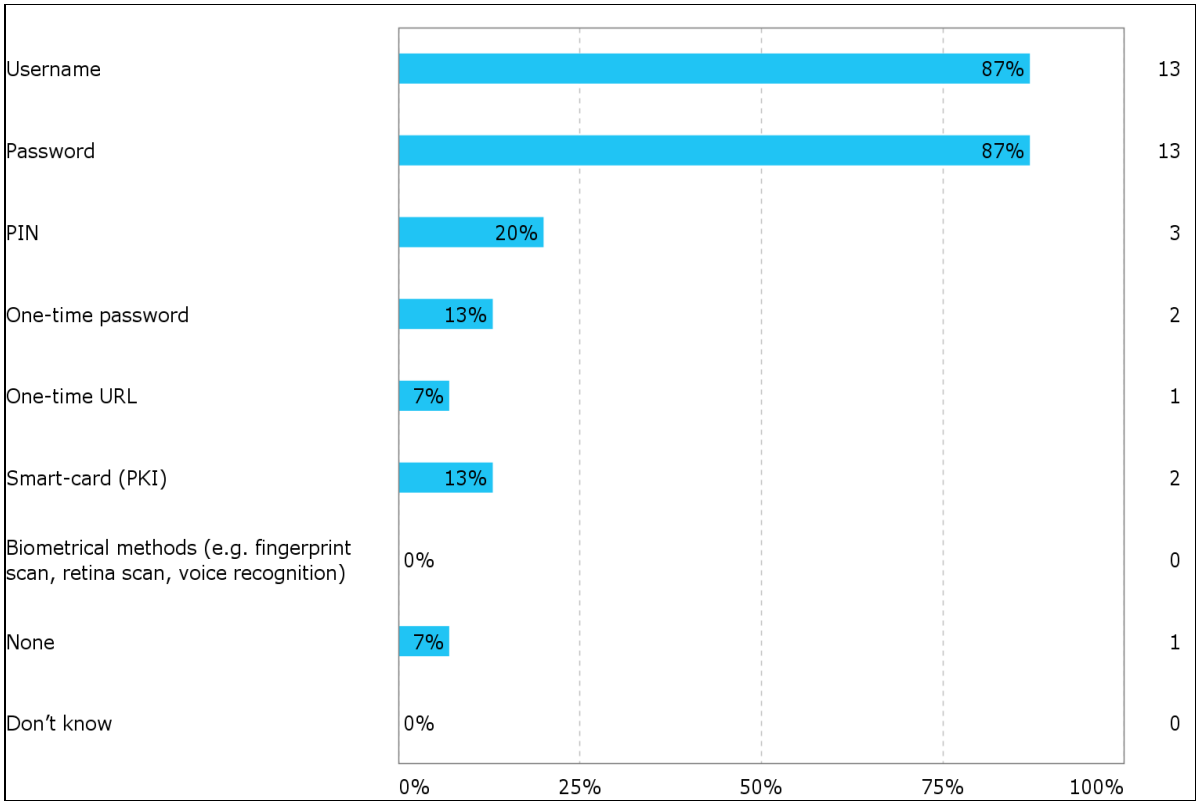

Figure 22: Responses to Q29.1(1): What method of authentication do they use?

This additional question was answered only by those 15 respondents who answered *yes* to the first question (Q29.1).

Username and password is by far the most widespread authentication method, as this answer was given by 13 of the 15 respondents. Nearly half of those who gave this response (6 of the 13) said that the method combined a username and password with an additional authentication method, like a one-time password or URL (3), PIN (3) or Smartcard/PKI (1).

Only one of the 15 respondents has answered that a smartcard/PKI is used, i.e. not together with username and password.

One respondent answered that no authentication is performed. The telemedicine service in this case is a video conference service. Video conference services have no direct authentication method. First, authentication of the caller is achieved by recognising the number/address of the caller. Second, recognising the person that appears in the video image is also an implicit authentication method. Authorisation for access can be achieved by answering known calls and avoiding answering unknown calls.

Q29.2 Is the user automatically logged out from the system/service after a certain idle time (i.e., does the application time out)?

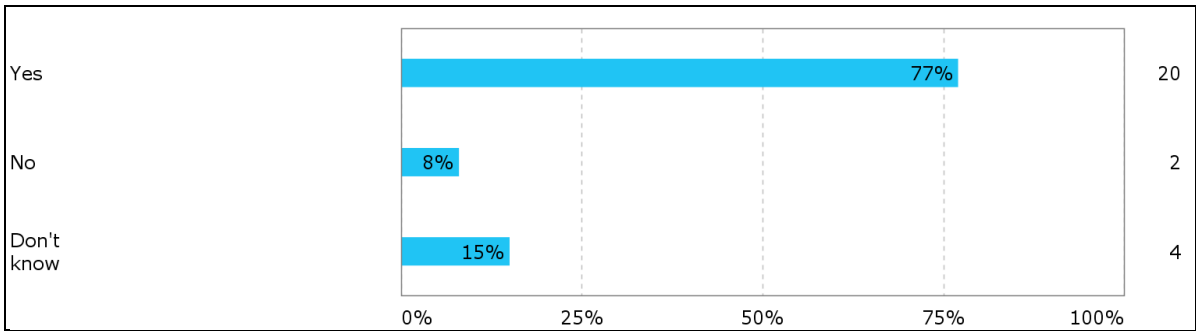

Figure 23: Responses to Q29.2: Does the application time out?

Timeout is one of several precautions to prevent access from unauthorised persons. It is used in the services described by three-quarters of the respondents (20 out of 26). However, this is not suitable for all types of services. For infrastructure services like a health network or a call centre, it is not obvious that one should close down the service in periods of no traffic.

Q29.3 Is the data transfer (i.e. communication) encrypted?

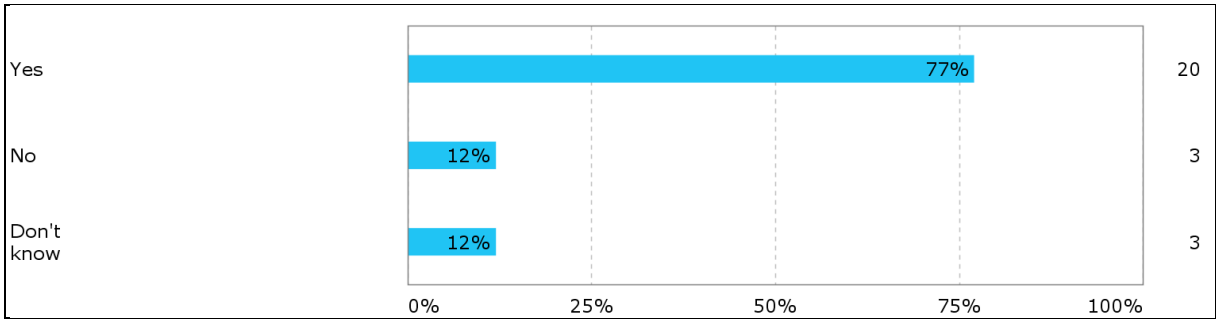

Figure 24: Responses to Q29.3: Is the data transfer (i.e. communication) encrypted?

Encrypted communication seems to be the usual way to transfer data, as indicated by more than three-quarters of the respondents (20 out of 26). The response to this question may be related to the next question (the use of VPN).

It should be noted that one of those who responded *no* to this question said in the response to question 6.3 (Description of the telemedicine service) that "secure http" is used, which in fact means SSL or TLS, i.e. encryption at the transport level.

It is unclear whether encryption is a requirement in all countries. In Norway, encryption is required when communicating sensitive information outside local/internal network. It is not, however, mentioned as a requirement in the personal data protection directive (Directive 95/46/EC).

Q29.4 Is the communication performed via a VPN connection?

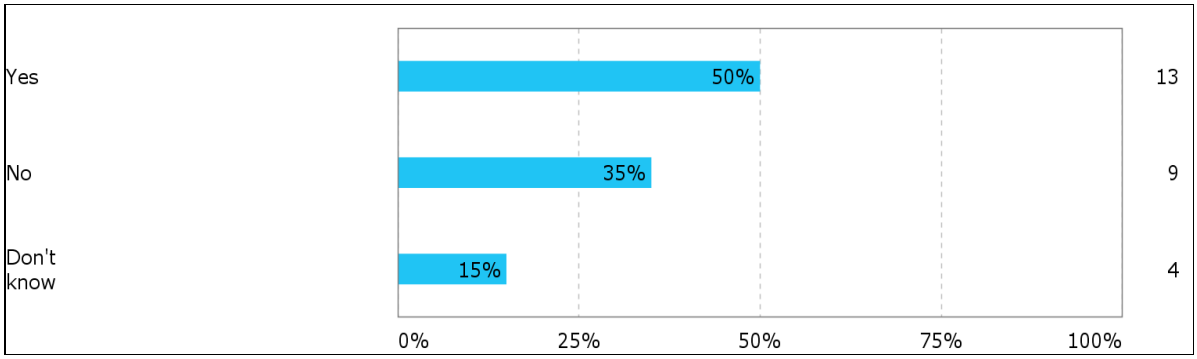

Figure 25: Responses to Q29.4: Is the communication performed via a VPN connection?

Half of the respondents (13 out of 26) have answered *yes* to the use of a Virtual Private Network (VPN).

VPN is most often an encrypted connection. Two respondents have answered *no* to the previous question about encrypted communication (Q29.3) and *don't know* to this question about the use of VPN (Q29.4), and one respondent has answered *don't know* to both questions. This means that most of the respondents, 23 out of 26, have answered *yes* to either "encrypted communication" or "use of VPN" or both[13]. This indicates that most of the telemedicine services use encrypted connections.

Q29.5 Is all access to the system/service logged?

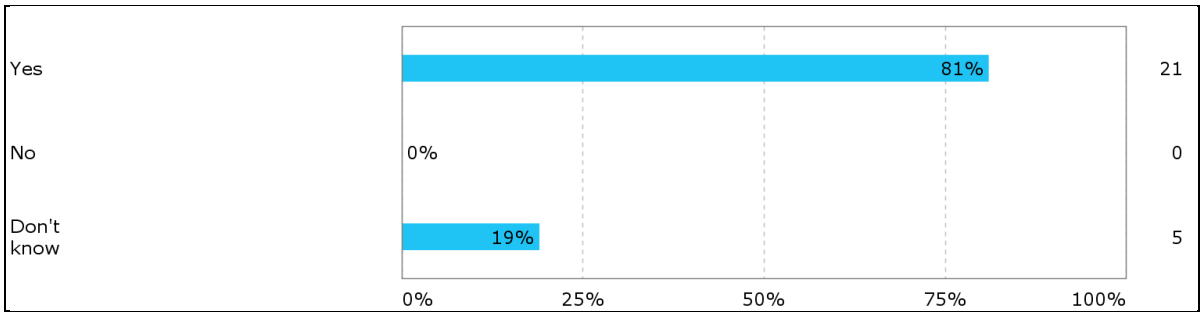

Figure 26: Responses to Q29.5: Is all access to the system/service logged?

Q29.5(1) If Yes, does anyone inspect the logs?

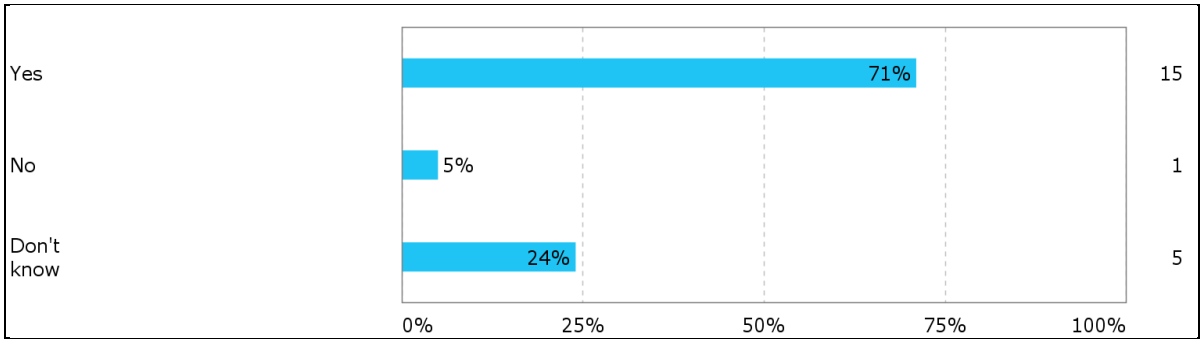

Figure 27: Responses to Q29.5(1): If Yes, does anyone inspect the logs?

[13] It is probably 24 of 26, since one of those who responded *no* to encryption in question 29.3, says in the response to question 6.3 (Description of the telemedicine service) that "secure http" is used.

Most of the respondents (21 out of 26) reported that all access to the service is logged, but it is not obvious to everyone who responded that the logs are investigated, as can be seen from the responses to the follow-up question. The usefulness of having logs can be questioned, if they are not inspected.

Logging is important for discovering unauthorised access – in retrospect. Inspection of logs is important in order to reveal misuse, and punitive measures can be taken. However, when data is disclosed, it is too late to reverse the act: as it were, "the cat is out of the bag." Logging helps indirectly, as a warning or a kind of "scarecrow", but it does not prevent unauthorised access.

8.2 Synthesis of the stakeholder feedback process

Work on this topic is on-going during the course of the project. Comments made by stakeholders at the Momentum Workshop in Berlin on 8 April 2013 included:

- Slowly and incrementally solutions and "get-rounds" are found to be issues that were critical in telemedicine some five to seven years ago, such as legal matters. Now, perhaps, issues relating to privacy and information security are higher on the list of potential barriers.
- Security could be described as "today's issue": it is now at the core of many policy issues related to information technology in general as well as eHealth and/or telemedicine specifically.

8.3 Synthesis of the literature review

The European eHealth benchmarking III study (SMART 2009/0022) provides an overview of how Europe's acute hospitals use eHealth. Its results regarding data protection and security (section 3.4 of the report) are similar to the findings from the Momentum questionnaire. The following points are extracted from the summary of the appropriate section of the benchmarking study:

- Among the different security measures that are taken to protect the patient data stored and transmitted by the hospitals' [information technology] IT systems, the most commonly used measure is the use of passwords to access workstations. Passwords are used across all the types of hospitals considered.
- The more sophisticated systems, such as encryption of transmitted data and data entry certified by a digital signature, are more likely to be found in large hospitals or those which belong to groups of hospitals or care institutions.
- In more than eight out of ten hospitals, the access to electronic patient records is logged.

In a briefing paper from EHTEL in 2008, "Sustainable Telemedicine: paradigms for future-proof healthcare" (EHTEL, 2008), footnote 2 on page 12 says: "Medical Associations in Germany refuse medical treatment over the Internet without cryptographic security measures."

A systematic review of information security in telemedicine has been conducted by Vaibhav and Brewer (2011).

9. Privacy training for personnel [Question 30]

This section describes privacy training for personnel involved in telemedicine deployment.

9.1 Synthesis of the answers to the questionnaire

This sub-section describes whether personnel have received any privacy training, and how often the training is repeated. The section also discusses whether staff contracts or insurance in the organisation is adequate for covering the staff's use of telemedicine systems.

Q30.1 Have all personnel had privacy training?

Education and training is a part of awareness-raising for the privacy aspects of telemedicine. It acts as a basis for motivating the use of implemented security measures. The users can often perceive such measures as cumbersome and unnecessary precautions.

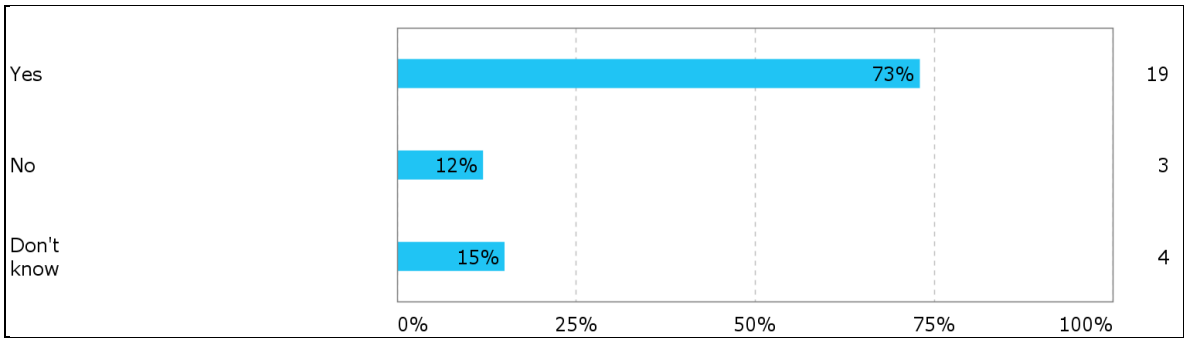

Figure 28: Responses to Q30.1: Have all personnel had privacy training?

Q30.1(1) If Yes, how often is this training repeated?

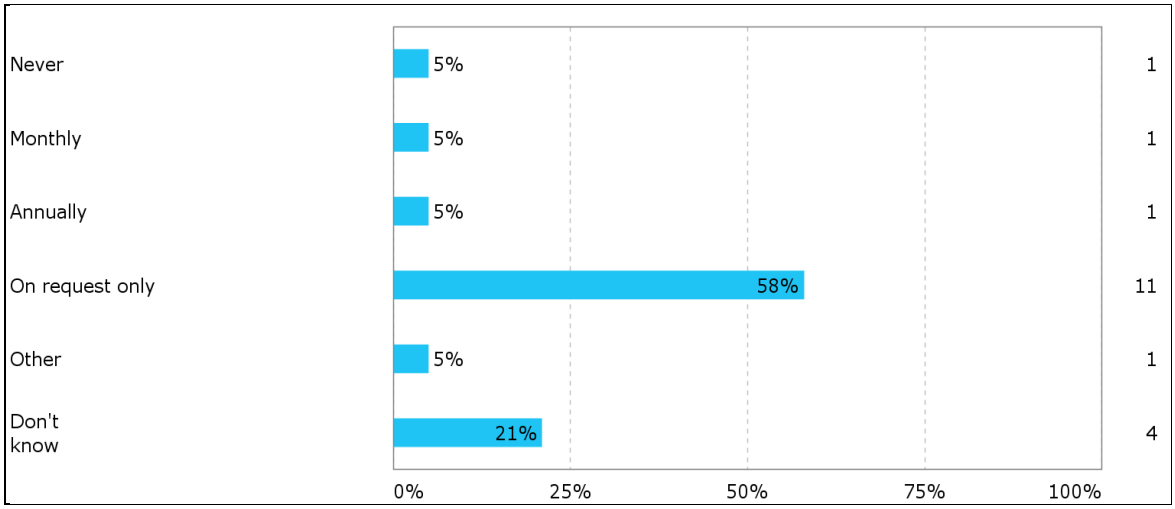

Figure 29: Responses to Q30.1(1): If Yes, how often is this training repeated?

Nearly three-quarters of the respondents (19 out of 26) have answered *yes* to the question about such training, and most of them (15 out of 19) also report some routine for repeating this training.

Q30.2 Are staff contracts and insurance in your organisation adequate for covering their use of your telemedicine system(s)?

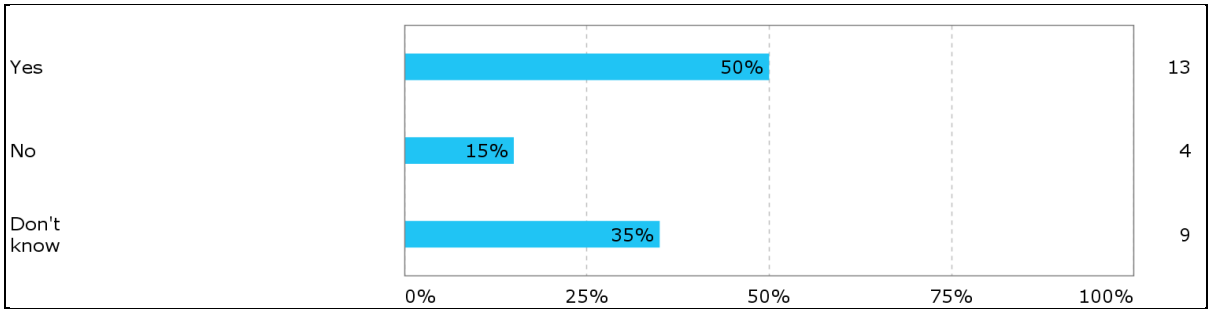

Figure 30: Responses to Q30.2: Do staff contracts and insurance cover telemedicine?

This may be a relevant question in some countries/regions, but not everywhere. The relative high number of *don't know* answers to this (9 out of 26) may reflect the degree of relevance; both the *yes* and the *no* answers may be used by those who do not find this question relevant.

9.2 Synthesis of the stakeholder feedback process

Work on this topic is on-going during the course of the project. Comments made by stakeholders at the Momentum workshop in Berlin on 8 April 2013 included:

- Everyone needs to have knowledge about security,
- Users do not need to know everything about security,
- It is crucial to know who needs to know what about the security of telemedicine systems.

9.3 Synthesis of the literature review

As an example of what should be included in privacy awareness training, a presentation made by the US Department of Health and Human Services offers some ideas.[14]

- Books and training programmes are available[15], as well as eLearning courses on privacy awareness.[16]

[14] http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/privacyawarenesstraining.pdf

[15] http://www.amazon.com/Managing-Information-Security-Awareness-Training/dp/1439815453

[16] http://irtsectraining.nih.gov/

10. Mapping of legal, regulatory and security stakeholders [Question 31]

It might be useful to develop an overview of stakeholders in the telemedicine field in the participating countries, both for network building and for further investigating of certain areas in the questionnaire. It is also of interest to find out if health professionals actually know of relevant stakeholders. This is why the respondents were asked about their knowledge about other stakeholders in the country working on security, regulation, and/or legal aspects of telemedicine.

10.1 Synthesis of the answers to the questionnaire

Q31.1 Do you know of authorities, organisations, or others working to clarify security, regulation, and/or legal aspects of telemedicine in your country?

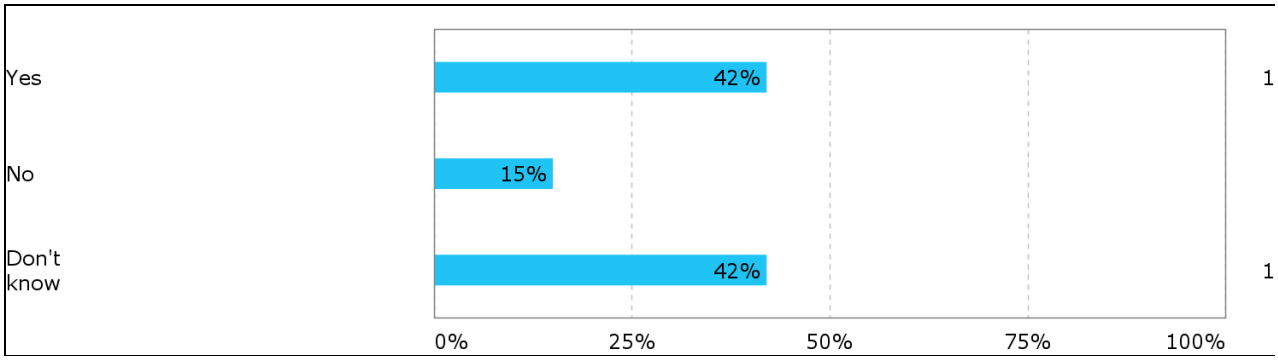

Figure 31: Responses to Q31.1: Do you know bodies that clarify security and legal issues?

It is worth mentioning that as many as 11 of the respondents from eight different countries did not know of authorities or organisations in their country working to clarify security and/or legal aspects. In addition, four respondents from three different countries answered "no".

This finding may indicate that, if and when health care personnel in the telemedicine field are unsure of legal, regulatory and security issues, they simply do not know whom to ask. The respondents in the six different countries who were able to name other authorities or organisations named the following. Many of them were also able to cite suitable websites:

Q31.1(1) If "Yes", please specify and offer URLs or documentation where feasible:

- *Denmark*: MedCom, Denmark: http://www.medcom.dk/wm109991
- *Denmark*: NSI, Governmental organisations
- *Estonia*: Health Board; The Data Protection Inspectorate
- *Greece*: Data Protection Authority of Greece, DPA www.dpa.gr
- *Greece*: Greek Research Center for Biomaterials, EKEVYL S.A http://www.ekevyl.gr/?lang=en&secid=52
- *Greece*: Greek Ministry of Health and Social Welfare http://www.yyka.gov.gr/page/english
- *Norway*: The Health Directorate, included the Department of Standardisation, *E-helse og IT*: http://www.helsedirektoratet.no/english/Sider/default.aspx
- *Norway*: Ministry of Health and Care Services: http://www.regjeringen.no/en/dep/hod.html?id=421

- *Norway*: The Norwegian Data Protection Authority: http://www.datatilsynet.no/English/
- *Norway*: the Norwegian Centre for Integrated Care and Telemedicine: http://www.Telemed.no/home.81328.en.html
- *Slovenia*: http://www.uradni-list.si/1/objava.jsp?stevilka=455&urlid=200815
- *Spain*: CATCERT: http://www.catcert.cat/CATCERT and http://www.apd.cat/en

10.2 Synthesis of the stakeholder feedback process

SIG 3 members' experience from the telemedicine field is that health personnel tend to be concerned with and anxious about certain topics in the legal and security field associated with the use of technology. This applies in particular to topics associated with data security and the duty of professional secrecy, responsibility issues and documentation routines.

10.3 Synthesis of the literature review

Work on the literature related to stakeholders in the legal, regulatory, and security field is still on-going.

11. Observations or concerns

There are a limited number of observations or concerns relating to the findings of SIG 3.

The advice given, resulting from the current status of the Momentum survey, could obviously have been based on more detailed and broader data from more, and more representative, countries. However, this SIG's considerations of the survey results are built on an amalgamation of literature studies, input from stakeholders, and our own members' experiences. We therefore think that we are able to give some well-founded advice and add value to the on-going discussions about the implementation of telemedicine services. We look at the data collected as offering a good starting point for reflections that might lead to new approaches on the implementation of telemedicine services.

How to collect good input from the various stakeholders in the telemedicine field might need some attention in the near future. Workshops can be a useful mechanism, and so too can focus groups. It is also possible to imagine smaller activities or arrangements that would be organised locally, regionally or nationally by each SIG.

References

Bigelow JH, Fonkych K, Fung C, Wang J (2005), *Analysis of Healthcare Interventions that Change Patient Trajectories*, Santa Monica CA: Rand Corporation http://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG408.pdf (Accessed 2013-06-2013)

Bolle SR, Hasvold P, Henriksen E (2011), "Video calls from lay bystanders to dispatch centers - risk assessment of information security", *BMC Health Services Research*, 11:244, http://www.biomedcentral.com/1472-6963/11/244 (Accessed 2013-06-27)

Bønes E, Hasvold P, Henriksen E, Strandenæs T (2007), "Risk analysis of information security in a mobile instant messaging and presence system for healthcare", *International Journal of Medical Informatics*, 76(9):677-687, http://www.ijmijournal.com/article/S1386-5056%2806%2900162-6/abstract (Accessed 2013-06-27)

Brownsell S, Ellis T (2012), *Ready, Steady, Go: A telehealth implementation toolkit,* The University of Sheffield, NHS National Institute for Health research, Version 1, September 2012, http://clahrc-sy.nihr.ac.uk/images/resources/Ready%20Steady%20Go%20toolkit.pdf (Accessed 2013-06-27)

Carlisle G, Whitehouse D, Duquenoy P (eds) (2013), "eHealth: Legal, Ethical and Governance Challenges." Heidelberg: Springer Verlag.

Cavoukian A, Hoffman DA., Killen S (2009), "Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design", *Information and Privacy Commissioner of Ontario, Canada,* http://www.ipc.on.ca/images/Resources/pbd-remotehomehealthcarew_Intel_GE.pdf (Accessed 2013-06-27)

COM(2008) 689 final, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on Telemedicine for the benefit of patients, healthcare systems and society,* Brussels, 4.11.2008.

COM(2012a) 11 final, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF (Accessed 2013-06-27)

COM(2012b) 736 final, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions on eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century,* Brussels, 6.12.2012.

Commission Regulation (EU) No 207/2012 of 9 March 2012 *on electronic instructions for use of medical devices*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:072:0028:0031:en:PDF (Accessed 2013-06-27)

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* **,** The European Parliament and the Council of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (Accessed 2013-06-27)

Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 *on the recognition of professional qualifications,*

http://ec.europa.eu/internal_market/qualifications/policy_developments/legislation/index_en.htm (Accessed 2013-06-27)

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 *on the application of patients' rights in cross-border healthcare,* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF (Accessed 2013-06-27)

EHMA (2006), *Study on Legal and Regulatory Aspects of eHealth,* "Legally eHealth", Deliverable 2, Processing Medical Data: Data Protection, Confidentiality and Security, EC Contract # 30-CE-0041734/00-55, http://www.ehma.org/files/Legally_eHealth-Del_02-Data_Protection.pdf (Accessed 2013-06-27)

EHTEL (2008), "Sustainable Telemedicine: paradigms for future-proof healthcare", A Briefing Paper Version 1.0 Date: 20 February 2008 http://www.ehtel.org/references-files/task-force-telemedicine/ehtel-briefing-paper-sustainable-telemedicine.pdf (Accessed 2013-06-27)

FSMB (2012), "Telemedicine Overview, Board-by-Board Approach", Federation of State Medical Boards, August 2012, http://www.fsmb.org/pdf/grpol_telemedicine_licensure.pdf (Accessed 2013-06-27)

Henriksen E, Johansen MA, Baardsgaard A, Bellika JG (2009), "Threats to Information Security of Realtime Disease Surveillance Systems." *22nd International Conference on Medical Informatics Europe MIE 2009,* Sarajevo, Bosnia – Herzegovina, IOS Press, volume 150, p. 710-714. http://ebooks.iospress.nl/publication/12754 (Accessed 2013-06-27)

ISO 27799:2008, *Health Informatics — Information security management in health using ISO/IEC 27002,* International Organization for Standardization (ISO), http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41298 (Accessed 2013-06-27)

ISO 31000:2009, *Risk management — Principles and guidelines,* International Organization for Standardization (ISO), http://www.iso.org/iso/catalogue_detail?csnumber=43170 (Accessed 2013-06-27)

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security controls,* International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), http://www.iso.org/iso/catalogue_detail?csnumber=50297 (Accessed 2013-06-27)

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management,* International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742 (Accessed 2013-06-27)

Jack C, Mars M (2008), "Telemedicine: A need for ethical and legal guidelines in South Africa", *South African Family Practice*, Vol 50, Issue 2.

Loane M., Wootton R. (2002), "A review of guidelines and standards for telemedicine", *Journal of Telemedicine and Telecare,* 2002; 8; p. 63-71 http://jtt.sagepub.com/content/8/2/63.full.pdf (Accessed 2013-06-27)

LOV-2000-04-14-31, *Norwegian Act of 14 April 2000 no. 31 relating to the processing of personal data (Personal Data Act),* Norway's Ministry of Justice and Public Security, http://www.lovdata.no/all/hl-20000414-031.html (English version: http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf) (Accessed 2013-06-27)

Nohr, LE. (2012). "Legal Issues", In: Soyer, HP et.al *Telemedicine in Dermatology,* Heidelberg: Springer Verlag, p. 157-165.

Rowthorne, V., Hoffmann, D. (2010), "Legal impediments to the Diffusion of Telemedicine", *White Paper*, Law & Health Care Program, University of Maryland School of Law, held on April 16, 2010.

Rynning, E. (1994), *Samtycke till medicinsk vård och behandling*, Uppsala: Iustus Förlag AB (in Swedish only).

SEC(2009)943 final (2009) Commission Staff Working Paper. Telemedicine for the benefit of patients, healthcare systems and society. European Commission. Brussels. 30.6.2009. http://www.uni-mannheim.de/edz/pdf/sek/2009/sek-2009-0943-en.pdfAccessed 2013-06-27)

Sellars C, Easey A. (2008), "Electronic health records: data protection issues in Europe." *BNA International World Data Protection Report,* McDermott, Will & Emery, http://www.mwe.com/info/pubs/worlddata0508.pdf (Accessed 2013-06-27)

SMART 2009/0022, *eHealth Benchmarking III,* Final report, Deloitte & Ipsos Belgium, 13th April 2011 http://www.ehealthnews.eu/images/stories/pdf/ehealth_benchmarking_3_final_report.pdf (Accessed 2013-06-27)

Stroetmann, Karl A, et al (2011), "European Countries in their journey towards national eHealth infrastructures", *Final European progress report*, January 2011, European Commission Information Society, Brussels, empirica, Bonn, and eHealth Strategies, Bonn

Stroetmann, Karl A, et al (2012), "United in Diversity: Legal Challenges on the Road Towards Interoperable eHealth Solutions in Europe", *European Journal for Biomedical Informatics*, Volume 8, Issue 2, pp.3-10 http://www.empirica.com/publikationen/documents/2012/EJBI_2012%282%29_Stroetmann_et_al.pdf (Accessed 2013-06-27)

SWD (2012) 414 final (2012). Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services. Brussels 6.12.2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0414:FIN:EN:PDF (Accessed 2013-06-27)

Vaibhav G, Brewer J (2011), "Telemedicine Security: A Systematic Review", *Journal of Diabetes Science and Technology,* 2011 May; 5(3): p.768–777, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3192643/ (Accessed 2013-06-27)

WHO (2012), "Legal frameworks for eHealth", *Global Observatory for eHealth series*, Volume 5, World Health Organization.

WHO-ITU (2012), *National eHealth Strategy Toolkit*, World Health Organization, ITU, ISBN 978 92 4 154846 5 (WHO), ISBN 978 92 61 14051 9 (ITU), http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf (Accessed 2013-06-27)