ICT PSP – Empowering patients and supporting widespread deployment of telemedicine services

MOMENTUM

European Momentum for Mainstreaming Telemedicine Deployment in Daily Practice
(Grant Agreement No 297320)

Deliverable *D6.2*

Report on ***SIG 3*** – "Legal, regulatory and security issues"

"*Legal, regulatory and security issues* report for the blueprint
validated by 'doers' and stakeholders"

Version 12

Work Package:	WP6 SIG on legal, regulatory and security issues
Version & Date:	*v12 / 10 September 2014*
Deliverable type:	Report
Distribution Status:	Public
Authors:	Ellen K. Christiansen, Eva Henriksen
Reviewed by:	Silvia Bottaro, Rachelle Kaye, Marc Lange, Tino Marti, Leif Erik Nohr, Peeter Ross, Stephan Schug, Eva Skipenes, Veronica Strotbaum, Diane Whitehouse (including reviews of case descriptions)
Approved by:	Marc Lange, Michael Strübin
Filename:	D6 2_MOMENTUM_SIG3_v12

Abstract

Legal and security issues are important issues throughout the whole process, whenever a new telemedicine service is developed, implemented, scaled-up, and put into operation. Taking such issues into consideration is for the best of both patients and telemedicine doers. Four critical success factors regarding the legal and security aspects of telemedicine deployment have been identified and discussed: Assess the conditions under which the service is legal; identify and apply relevant legal and security guidelines; involve legal and security experts; and ensure that telemedicine doers and users are "privacy aware". The analysis of legal and security issues is based on the 26 telemedicine services investigated in the Momentum project in 2012-2013 and the results of Deliverable 6.1. The critical success factors have been examined in terms of 4-7 use cases. The conclusion is that telemedicine doers must keep an eye on legal and security issues throughout the whole telemedicine

deployment process. The first three critical success factors are closely related and might be said to partly overlap with each other. However, offering this level of detail about legal and security issues can help telemedicine doers to take all relevant legal, regulatory and security aspects into consideration.

Key Word List

Legal and security experts, legal and security guidelines, legal and security risk assessment, privacy awareness, telemedicine.

Note on the seven telemedicine cases

Six of the telemedicine cases described in this deliverable can be located on the MOMENTUM website, called service descriptions, under six countries (Israel, Italy, the Netherlands, Norway, Sweden, and Spain): http://telemedicine-momentum.eu/europe/. A short description of each of the cases (including the Germany Patientenhilfe case) is also included in deliverable D3.2.

Change History

Version History:

01	27 June 2014
02	11 July 2014
03	21 July 2014
04	26 August 2014
05	27 August 2014
06	30 and 31 August 2014
07	1 September 2014
08	2 September 2014
09	3 September 2014
10	4 September 2014
11	6 September 2014
12	10 September 2014

Version Changes

01	Initial version subject to first review.
02	Version subject to limited review among SIG team members.
03	Version subject to wider review among SIG team members and Veronika Strotbaum.
04	Version subject to review: Marc Lange, Diane Whitehouse, SIG team members, and SIG leaders.
05	Modifications made based on review: Silvia Bottaro, Leif Erik Nohr, Stephan Schug, Eva Skipenes, Veronica Strotbaum, Diane Whitehouse, and Executive Summary and Abstract added, by Ellen K. Christiansen and Eva Henriksen.
06	Modifications based on review from Diane Whitehouse by Ellen K. Christiansen.
07	Modifications based on review from Diane Whitehouse by Eva Henriksen.
08	Version with text from the various reviewers accepted.
09	Modifications based on input from Diane Whitehouse.
10	Further minor amendments offered by Marc Lange.
11	Final minor changes made by Diane Whitehouse following commentary by Ellen Christiansen.
12	Quality review, with formatting and other edits, by Michael 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.

Table of Contents

EXECUTIVE SUMMARY III

1. INTRODUCTION 1

2. ASSESS THE CONDITIONS UNDER WHICH THE SERVICE IS LEGAL 2

3. IDENTIFY AND APPLY RELEVANT LEGAL AND SECURITY GUIDELINES 8

4. INVOLVE LEGAL AND SECURITY EXPERTS 14

5. ENSURE THAT TELEMEDICINE DOERS AND USERS ARE "PRIVACY AWARE" 19

6. OBSERVATIONS OR CONCERNS 25

7. CONCLUSIONS 27

8. BIBLIOGRAPHY 29

Executive summary

It is critical for those involved in the successful deployment of a telemedicine service to pay attention to legal and security issues throughout the whole telemedicine deployment process, whenever a new telemedicine service is developed, implemented, scaled-up, and put into operation. When telemedicine projects fail, it is not necessarily because of legal hindrances but because the legal situation was not taken into account and assessed at the right time. It is important to bear in mind that the reason for initiatives in the legal and security area are for the benefit of both telemedicine doers and patients.

Through the analysis of 26 telemedicine services which have been integrated into routine care in Europe, and an in-depth analysis of seven use-cases, four critical success factors in the legal and security field have been identified: They are: assess the conditions under which the service is legal; identify and apply relevant legal and security guidelines; involve legal and security experts; and ensure that telemedicine doers and users are "privacy aware".

- **Assess the conditions under which the service is legal**

The initial step in telemedicine deployment is to find out whether telemedicine in general is regarded by the public authorities as an appropriate way to offer healthcare services, and under which circumstances the specific telemedicine service can be regarded both as legal and in accordance with general requirements for best practice in medicine. The objective is to ensure that the personnel involved in the telemedicine development process are heading towards setting up a legal telemedicine solution and do not waste their resources on a service which turns out to be illegal.

- **Identify and apply relevant legal and security guidelines**

This critical success factor reminds the telemedicine doers to identify and apply existing guidelines for telemedicine. The main objective for using such guidelines is to make it easier for telemedicine doers to establish a telemedicine service in accordance with basic and accepted principles in the legal and security field. Identification of available guidelines might also inspire the telemedicine doers to ask for national guidelines.

- **Involve legal and security experts**

Telemedicine doers should ask advice from legal and security experts, when needed. The experts must be available throughout the whole process of planning, developing, and implementing a telemedicine service. They must handle legal and security subjects whenever the telemedicine doers ask for it. One part of their task is to conduct risk assessments in both the legal and the security field. The objective is to make sure that the telemedicine service under development is ultimately legally and securely implemented. As a result, legal and security obstacles should not emerge unexpectedly for the telemedicine doer and should not influence – in a negative way – the willingness to deploy and use telemedicine services.

- **Ensure that telemedicine doers and users are "privacy aware"**

Knowledge about appropriate practice when it comes to privacy and security behaviours may be termed "privacy awareness". Such knowledge is based on current ethical and legal principles and applies to developers during the phase of system design and implementation, as well as to end-users during operational use. "Privacy awareness" can be achieved through education, training, strategic attitudes formed in the organisation, and the development of a privacy awareness "company culture" or organisational culture. In this way, privacy awareness can contribute to strengthen peoples' confidence in and willingness to use telemedicine, whether they are healthcare professionals or patients.

These critical success factors have been validated against four to seven different telemedicine use cases which were selected to create a representative set of telemedicine diversity. All these use cases have reported that the circumstances under which the service could be legally established have been investigated at different stages of deployment. All the reported use cases have taken some sort of guidelines into account; both clinical guidelines and legal and security guidelines are mentioned. Legal and security expertise has been used in at least four of the use cases for different purposes and at different stages of the development and implementation process, illustrating that experts should be available throughout the whole telemedicine deployment process so that the telemedicine doers can involve them when needed. The case owners have provided little information about training in "privacy awareness". Several of the case owners mentioned "patient consent" as an example of privacy awareness. Privacy awareness and patient consent are not the same, but there is a relationship between them.

The first three critical success factors are closely related and might be said to partly overlap with each other. Despite this overlap, they have been kept independent and separate, mainly due to the content of the responses given to the MOMENTUM 2012 questionnaire and an in-depth analysis of the seven services. Based on this background, it is anticipated that this level of detail could help telemedicine doers to take all the relevant legal and security aspects into consideration.

1. Introduction

Different groups of people may undertake a range of initiatives in the telemedicine field. These groups of people can include clinicians, hospital managers, entrepreneurs, vendors, and public administrators. Competence in legal and security matters is not always available to these people when it is needed during the process of setting up and deploying a telemedicine service.

It is, however, absolutely important to address legal, ethical and regulatory issues in telemedicine deployment. When telemedicine initiatives fail, it is not necessarily because of legal hindrances, but because the legal situation was not taken into account and assessed at the right time.

When it comes to legal and security issues, it is important to bear in mind that the reason for initiatives in this area is for the benefit of both patients and telemedicine doers. Consequently, sound legal services founded on the legislation and regulations in the field, is a pre-requisite for the development of best quality medical services fit for large-scale implementation. This also implies that the patients' right to privacy must be taken care of, even though practitioners in the healthcare sector might sometimes experience it as a hindrance in their daily work.

In order to initiate and scale up telemedicine services successfully, the following success factors need to be paid attention to in the legal and security field:

- Assess the conditions under which the service is legal.
- Identify and apply relevant legal and security guidelines.
- Involve legal and security experts.
- Ensure that telemedicine doers and users are "privacy aware".

Considerations in the legal and security field will no doubt involve discussions about codes of professional conduct and about ethical principles. The privacy of patients is always within the focus of health professionals and, hence, is discussed when legal and security matters are on the agenda.

In the following four sections of the report, four critical success factors in the legal and security field are presented. The presentation is built on the description of use cases, this special interest group's members' own experience, its understanding of the findings of the Momentum questionnaire results and of literature describing the development, implementation and use of telemedicine services.

The four critical success factors are closely related. Together they contribute to create sound and sustainable telemedicine services and offer guidance on making sure that services under development are legal, also with regard to both information security and privacy aspects.

2. Assess the conditions under which the service is legal

This section of the report describes the issues surrounding assessment of the conditions under which a particular telemedicine service is legal.

2.1 What this critical success factor is

This critical success factor gives telemedicine doers an understanding of the degree of latitude under which they can operate when developing a new telemedicine service.

Assessing the conditions under which the specific telemedicine service is legal is about finding out:

- Whether the telemedicine service is regarded by the authorities1 as an appropriate way to offer healthcare services.
- Under which circumstances the telemedicine service is regarded as legal, by carrying out a "legal risk assessment"2.
- Whether the telemedicine service is covered by law and whether it is not inhibited by law or by bodies with competence in the telemedicine field.
- Whether the telemedicine service is in accordance with general requirements for best practice in medicine.

It is also important to understand the objectives that underpin this critical success factor.

2.2 Objectives

There are two main objectives supporting this critical success factor.

- The first objective is to ensure that any personnel involved in the telemedicine development process can be assured of providing a legal telemedicine solution.
- The second objective is to avoid any waste of resources and any risk of decreased enthusiasm among the telemedicine doers and users, for example if it were to turn out that the proposed telemedicine service were proven to be illegal.

Both are important objectives.

[1] These authorities can be of different sorts and levels in the European Union and countries geographically close to the Union, and/or countries that are involved in such contractual arrangements with the Union as the European Economic Area. Examples of these authorities include healthcare authorities and social care authorities.

[2] A legal risk assessment can be described as a process that runs parallel to an information security risk assessment. In it, possible legal hindrances ("risks") are identified and measures are planned and carried out to avoid risks and/or mitigate them, cf. section 4 on the critical success factor related to the involvement of legal and security experts.

2.3 Context

Different assessments of the conditions under which the precise telemedicine service is legal must be made depending on the surrounding context of the planned service.

There are two main contextual elements to be explored. The first refers to whether the telemedicine service being run is a medical act or not; the second relates to the sharing of patient information. Both are explained in more detail below.

1. Is the telemedicine service a medical act or not?

It is of great relevance whether the service is regarded as a medical act[3] (eHSG 2014) or not. Currently, considerations differ from country to country depending on the definition of medical act described in the various national health legislations. If the telemedicine service is recognised as a medical act, legislation applicable to medical acts will apply to the service in addition to other relevant legislation. Of particular relevance for this legal assessment is this non-exhaustive list of questions:

- What kind of health professions delivers the service?
- What is the purpose of the service (cf. how does it fit with the definition of a medical act)?
- Who are the participants/parties involved in the service (e.g. is it a doctor-to-doctor (D2D) service or is it a doctor-to-patient (D2P) service)?

2. Is there relevant legislation related to the sharing of patient information?

There may be legislation that refers to the sharing of patient information that relates to at least three topographical, geographical or organisational levels.

- Across national borders.
- Across regional borders.
- Across organisational borders.

2.4 First thoughts on pre-requisites

It is a pre-requisite that the telemedicine service is legally authorised. With regard to this pre-requisite, the notion of legal authorisation has three aspects:

- Legislation and regulations in the field must make it clear that telemedicine is a legitimate way to deliver healthcare.4

[3] "The medical act encompasses all the professional actions, e.g. scientific, teaching, training and educational, organisational, clinical and medico-technical steps, performed to promote health and functioning, prevent diseases, provide diagnostic or therapeutic and rehabilitative care to patients, individuals, groups or communities in the framework of the respect of ethical and deontological values. It is the responsibility of, and must always be performed by a registered medical doctor/ physician or under his or her direct supervision and/or prescription." (UEMS 2009)

[4] The service should be organised in a way that is also in accord with requirements for responsible conduct and/or best practice.

- Legislation and regulations in the service provision field must avoid provisions that prohibit or inhibit the delivery of healthcare via telemedicine in general, either directly or indirectly.
- The general attitude of the relevant authorities must state and imply that telemedicine is accepted and wanted.

This initial notion of pre-requisites will be explored further in deliverable D3.2, and the validation process of the critical success factors (e.g., also D3.3 and D3.4).

2.5 Illustration of this critical success factor from the Maccabi case

The Maccabi case illustrates a situation in which the legality of telemedicine provided by the company was never questioned. All the relevant ethical, privacy and security issues had already been dealt with in earlier versions of Maccabi's telemedicine services.

2.6 Illustration of this critical success factor from the RxEye case

The legal framework was considered very important for RxEye. It was expected that the service complied with all the relevant provisions set out by the legal framework on teleradiology services.[5] Hence, the RxEye service operates within the current legal framework for such services.

Contracts are the main enablers that ensure the provision of this brokerage service for medical image reporting. One of the components of the service is to provide customers with contract drafts. These drafts are prepared according to the appropriate legal framework. In this case, especially in case of the provision of cross-border services, accordance with the relevant legal framework is critical.

2.7 Illustration of this critical success factor from the Teledialysis case

The circumstances, under which the Norwegian Teledialysis service was or could be legal, were questioned and elucidated at several stages of the development and deployment of the service. Liability and responsibility issues were focused on and had to be defined and described. The fact that the roles and the work-related tasks of the staff changed due to the changes in the way dialysis was organised were also assessed in the light of the legal framework for such services[6].

2.8 Illustration of this critical success factor from the ITHACA case

ITHACA is run in Badalona in Catalonia. In general in Spain, telemedicine is an undisputed and legally approved service; it is not perceived as an inferior service or "second-class medicine". As a complement to traditional healthcare, it is seen as posing little threat.

[5] See Legido-Quigley et al (2014) for an up-to-date view on legal frameworks relative to teleradiology.

[6] Health legislation, legislation and regulation concerning privacy, statements and guidelines from public authorities.

The circumstances under which the ITHACA service could be organised in a legal way were assessed. The service operates in strict compliance with the Spanish Personal Data Protection Act (Ley Orgánica 1999). The Spanish law complies with the Data Protection 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 (EC 1995).

No concerns arose regarding the legality of the services included in the ITHACA initiative. Collaboration agreements were set out between all three organisations involved (BSA, Novartis and Indra, which are all independent companies). The three organisations signed bilateral and multilateral agreements to carry on the project and to give ITHACA a binding strength.

2.9 Illustration of this critical success factor from the Patientenhilfe case

Legal and security issues were not mentioned at all in relation to this case; the background to this is still under investigation and appears to relate more to security compliance.

2.10 Illustration of this critical success factor from the KSYOS case

As far as the founder of KSYOS was concerned, the handling of legal and security issues was taken care of late in the development process of the service in order for the service to get well underway as soon as possible and without experiencing too many delays.

2.11 Illustration of this critical success factor from the Cardio Online Europe case

Great efforts were made to ensure the quality, security and legality of this cardiology service in accordance with the legal framework in force in Italy. The device and software is certified by the Food and Drug Administration (FDA) and the Italian Ministry of Health. The application is manufactured in Israel, and has licenses for its use and sale.

Every electrocardiogram (ECG) is signed by a specialist cardiologist. The system has an integrated certification for information security management system, ISO/IEC 27001, in telemedicine (ISO/IEC 27001 2013). It is also certified in terms of its quality, ISO 9001 (ISO 9001 2008). All the system’s software and all its devices are certified as medical devices.

2.12 Lessons learned on assessing whether the telemedicine service is legal from the cases

In the six cases where this topic was elaborated, it was reported that the circumstances under which the service could be legally established were assessed. This has been done at different stages in the development and implementation process for the various services. In the Maccabi case this investigation had already been undertaken by the time the service was established (i.e., it was done for an earlier Maccabi service). In the KSYOS case, legal issues were taken care of relatively late in the development process, namely in what KSYOS calls the scale-up phase. In the other cases in which legal issues were described, it was reported that these aspects were investigated at the outset. In the Teledialysis case, legal and security matters had been handled from the outset and, beyond that, whenever it was needed in the development and implementation phase.

2.13 Overall analysis on assessing whether the telemedicine service is legal from the cases

It appears that the timing of the investigation of the circumstances, under which the service is legal, has differed. As described, it varied from being clarified prior to the implementation of the service (Maccabi) to relatively late in the process (KSYOS). In the other cases legal and security clarifications took place initially and when needed.

In none of the cases were legal and security issues reported to cause problems, even though all respondents agreed that such issues had to be discussed. Hence, it seems to be agreed that it is important to handle these issues, but that the right time for them to be handled can vary from case to case.

2.14 Further relevant discussion

Three issues have particularly emerged as a result of materials provided either by reading of the literature and through observations provided by members of the MOMENTUM consortium: the degree of constraints relating to the implementation and use of telemedicine; how public authorities can be influenced positively so that they eliminate any legal constraints; and the timing at which the legal assessment should take place.

1. Does the relevant legislation in practice imply various constraints for implementation and use of telemedicine?

The legal situation in certain countries might imply that there are restrictions when it comes to the use of certain tele-services in the healthcare sector. Among the example countries suggested are Germany, Poland, Malta and France. For example, "In Germany, a professional code of conduct – enforced by court rulings – exists that does not allow [one] to [undertake] a standard patient encounter in ambulatory care over distance – thus preventing certain types of tele-services to operate within Germany"[7]. Poland and Malta are also placed under extensive constraints when it comes to use of tele-services in the healthcare sector. In other countries, such as France, previous face-to-face contact between physician and patient is recommended for all telemedicine use cases (eHSG 2014), i.e., the first contact between the two should not take place via telemedicine. The same is the case in Norway.

A study on the existence and degree of such limitations, at least within the countries in the European Union, should be produced.

[7] Dr Stephan Schug, EHTEL in an e-mail dated 22 July 2014 to Ellen K Christiansen

2. How to influence the public authorities positively so that they eliminate any legal constraints?

Possible ways to influence the public authorities, so as to eliminate legal constraints, could include:

- The provision of documentation about the sustainability of running telemedicine services.
- The communication of research results that address the advantages of the use of telemedicine in international organisations for different health professional groups.
- Lobbying of potential telemedicine doers.
- One could also imagine that the on-going work within the European Union, among them, the eHealth Action plan published in 2012, and the green paper on mobile health (EC 2014), might be useful in bringing the process forward. This could in due time be supplemented by provision of either policy guidance and/or an appropriate green papers for member states in the European Union.

The importance of these various possibilities could be further explored.

3. What can be observed about the "timing" of legal assessments of telemedicine services?

It would be of great interest to investigate further whether the handling of legal conditions early or late in the telemedicine deployment process has certain consequences that might be formulated in a more generic way for the benefit of telemedicine doers.

This assessment should also be related to the type of telemedicine service under development, cf. the Introduction to D4.2, where three types of telemedicine services (telediagnosis, telemonitoring and teleconsultation) are classified.

It could perhaps also be of interest to investigate more thoroughly whether the right "timing" of the legal investigation is linked to certain characteristics of the service, for example whether it is a private or public service, a doctor-to-doctor or a doctor-to-patient service, a service crossing borders, or if there are other circumstances of significance for the appropriate timing of the legal considerations.

3. Identify and apply relevant legal and security guidelines

This section of the report describes the issues surrounding the identification and application of relevant legal and security guidelines.

3.1 What this critical success factor is

This critical success factor reminds the telemedicine doers to look for the existence and possible usefulness of relevant guidelines on legal and security matters. Guidelines can be defined as "low level legislation", informal rules, and self-regulation that can guide telemedicine doers about the process of telemedicine deployment and help them to "translate their duties into action" (WHO 2012). These guidelines can also be described as "soft law" as well as social customs and norms of professions. Typical guidelines are also interpreted as a set of non-binding recommendations (EC 2013). One could say that guidelines imply compliance with practices that are recommended, and are therefore to some extent flexible (Loane & Wootton 2002). Finally, guidelines might ease the development process of sustainable telemedicine services and assist the telemedicine doers in the development and maintenance of a service.

There are at least three different types of guidelines. They include:

- Non-binding international codes of practice.
- Operational national guidelines related to application of relevant legislation and regulations.
- Codes of conduct (which also emerge from professional organisations).

Guidelines on the legal and security aspects of the use of telemedicine have been published in several countries, both in Europe and in other areas, especially in Australia and the United States of America (Loane & Wootton 2002, Jack & Mars 2008). One European example is the guidelines concerning telemedicine and responsibility/liability in Norway (HOD 2001).

There are also guidelines available for professional groups – such as doctors and psychologists – that codify legislative and security measures as well as ethical and policy considerations. Examples include guidelines for medical doctors' use of telemedicine in Denmark (Sundhedsstyrelsen 2005) and Finland (Finlands Läkarförbund 2004) and guidelines for psychologists in Norway (Norsk Psykologforening 2002). Another example is the ethical guidelines in telemedicine worked out by the Standing Committee of European Doctors (CPME) in 1997 (CPME 1997). Even though existing guidelines might be aimed directly at different professional groups, a specific country, a region, or even a particular service, they might provide useful baselines or examples for other telemedicine doers who are working to set up telemedicine services. More information, with examples of guidelines, can be found in an article issued in South Africa (Jack & Mars 2008).

One should, of course, not forget to mention also quality guidelines for deploying and running ICT systems.

3.2 Objectives

For the telemedicine doer, the objective of this critical success factor is to facilitate the establishment of a telemedicine service in accordance with the basic and accepted principles in the legal and security fields. These principles need to be applied throughout the whole telemedicine development and deployment process.

Use of different guidelines, accommodated to the various groups of telemedicine doers, can help doers to sort out the most important legal and security issues to be taken into consideration when telemedicine services are developed, run, scaled-up and made routine.

These types of guidelines can also serve as a good starting-point for doers who want to work out their own guidelines. For instance, the availability of guidelines in only particular countries or regions suggests that the translation of these guidelines into other languages might offer useful background information and understanding to doers in other nations with other languages.

3.3 Context

If a service is defined as a medical act (see section 2.3), relevant general legislation in the field has to be applied when the telemedicine service is established. Original health legislation was passed in most countries when it was traditional delivery of healthcare that was the norm, not telemedicine. Today, health legislation also governs telemedicine, which is not always easy to handle in practice.

Bearing this background in mind, relevant legal and security guidelines might represent a useful support and interpretation of, and supplement to, the available national legislation and regulations for telemedicine doers.

Use of guidelines will be particularly important for telemedicine doers who have little experience of telemedicine and limited resources, which might be the case when initiatives emerge in either small institutions or municipalities, or when the service is only useful for small groups of patients, or both.

3.4 First thoughts on pre-requisites

The legal and security rules must not restrict the use of telemedicine or state that delivery of any healthcare via telemedicine is inadvisable, not recommended, or illegal, directly or indirectly. The guidelines should focus on how to facilitate the provision of telemedicine – as a legal service – so as to provide the best outcomes for patients and for the healthcare system.

These guidelines must be issued by trusted bodies, such as public authorities, telemedicine advisory groups, telemedicine provider business services, or combinations of telemedicine providers represented throughout Europe.[8] These guidelines must be known and considered important and useful by the relevant target groups and be adapted to their needs. The target groups include, among others, medical staff, technologists and vendors. Since laws are changing and people gather new knowledge on their way, continuous annotations from telemedicine doers in general, and legal experts in particular, should be welcomed. Guidelines need to be up-to-date to be trusted and used.

It is also important that the guidelines are communicated in a clear and understandable language and are adapted to the various target groups from the outset.

3.5 Illustration of this critical success factor from the Maccabi case

Legal and security guidelines were applied during the process of working on the Maccabi case. Guidelines for the central electronic medical record were clear to both the medical personnel and the patients. Since ethical, privacy and security issues had already been dealt with in earlier Maccabi-developed telemedicine services, these guidelines were available and the system has been confirmed as being compliant with them.

3.6 Illustration of this critical success factor from the RxEye case

The reliability of the RxEye radiological service was discussed at an early stage of the service development. The conclusion was that RxEye provides a proper way to conduct such a radiological service, as long as the patients' rights are taken into account.

Both the European (ESR 2014) and North American (ACR 2013) Societies of Radiology have issued white papers which address the principles of good teleradiology practice. It was beneficial for the RxEye service to follow the principles outlined in these white papers.

3.7 Illustration of this critical success factor from the Teledialysis case

Appliance of legal and security guidance was of great importance in terms of the implementation of the Norwegian Teledialysis service. Guidelines for telemedicine and responsibility/liability matters issued by the Norwegian government (HOD 2001) were taken into account. Based on these guidelines, the service was described, the roles and responsibilities of the healthcare personnel were defined, and the protection of the patients' rights was secured.

The Norwegian *Code of Conduct for information security in the healthcare, care, and social services sector* (Hdir 2014), issued by the Norwegian national health authorities, was applied[9]. This code of conduct was developed by representatives from the health and social services sector, and comprises the sectors' view of how to ensure information security. In addition to developing the code of conduct, the health authorities have produced a set of

[8] Examples that are worth further reading, include those emerging from, e.g., the European co-financed project, TELEscope (http://www.telehealthcode.eu) or national telemedicine advisory service / competence centres such as the Telecare Service Association in the United Kingdom (http://www.telecare.org.uk).

[9] The Code itself and a selection of fact sheets and appendices have been translated into English.

short practical guidelines and several fact sheets on how to meet the individual requirements in the code.

The code represents a holistic approach to an information security policy for all organisations within the sector. Since 2006, this code has turned out to be a very important tool in the process of deploying telemedicine.

3.8 Illustration of this critical success factor from the ITHACA case

Guidelines were considered useful and important in the ITHACA case. The service builds on the Catalan clinical guideline (Guirado 2003), which is based on international guidelines for treatment of hypertension (Chobanian et al 2003, Chalmers et al 1999). It is assumed that security advisors follow appropriate technical guidelines. No specific legal guidelines were used, apart from procurement guidelines.

3.9 Illustration of this critical success factor from the Patientenhilfe case

Deutsche Gesellschaft für Patientenhilfe (DGP) is certified for data security, based on an audit according to the ISO 27001[10] standard. This includes a confirmation that Patientenhilfe obeys the specific regulations for health and social data. Furthermore, since it is a legal requirement for every company's website in Germany, the service has declared its conformance to the general German federal law on data protection (there are two German regulations that apply here).

3.10 Illustration of this critical success factor from the KSYOS case

Appliance of relevant legal and security guidelines were indicated as having been important in what is called "the scale-up phase" of this service by the founder of KSYOS.

It seems that, in the KSYOS case, the application of legal and security guidelines were handled relatively late in the process of the development and dissemination/scaling-up of this commercial service.

3.11 Illustration of this critical success factor from the Cardio Online Europe case

In terms of Puglia's Cardio On Line Europe case, great efforts were made to ensure that the adopted service was approved by the relevant bodies.

[10] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (last accessed 5 September 2014).

3.12 Lessons learned on identifying and applying relevant legal and security guidelines from the cases

In the six cases where the topic of legal and security guidelines was elaborated, it was reported that some sort of guidelines have either been taken into account or it was at least ensured that the adopted telemedicine service was approved by the relevant bodies (as in the Cardio Online Europe Case). In the other cases, both legal and security guidelines (e.g. in Maccabi, Teledialysis, and KSYOS) and clinical guidelines (e.g. in RxEye and ITHACA) were applied.

Some particular important topics are mentioned in addition to legal and security guidelines in general: reliability, good practice (RxEye), codes of conduct for information security in the healthcare sector, and responsibility and liability matters (Teledialysis).

3.13 Overall analysis on identifying and applying relevant legal and security guidelines from the cases

Since all the six cases reported on have used some sort of guidelines, one must assume that they have considered it useful. It is of interest that different types of guidelines have been applied. These guidelines concern different aspects that are discussed in connection with health services. Both clinical, and legal and security, guidelines related to telemedicine services and health services in general have been used. Since the experience with telemedicine is relatively limited compared with more traditional health services, the need for various guidelines in the telemedicine field should probably be further analysed and met.

One could assume that good guidelines could inspire the telemedicine doers to produce new telemedicine services. Such guidelines, taking into account legal, security and clinical aspects, can guide doers in the right direction and make them feel more confident about the process of developing and implementing new and sustainable services.

The focus of the analysis of this critical success factor, however, was guidelines concerning legal and security issues. Clinical guidelines are related, but have not been further elaborated in this section of the deliverable.

3.14 Further relevant discussion

Based on the previous considerations, the Momentum project will recommend further work to create a basis, and a possible template, for guidelines for telemedicine services.

Ideally, each country should work out guidelines for telemedicine doers, based on European regulations and relevant national legislation. What could be discussed further is how to create an incentive for the production of such telemedicine guidelines. One could suggest:

- In order to support each country in its endeavour to work out telemedicine guidelines in the legal and security fields, fundamental ethical, legal, and security principles for telemedicine services should be further elaborated and outlined at the level of the European Union.

- Already existing guidelines in the legal and security fields should be mapped, systematically collated, translated, and made available, i. e., on the internet.
- An overview of the crucial topics that need to be addressed in legal and security guidelines for telemedicine should be worked out.
- A simple template for such guidelines should be suggested and recommended.

By working on these activities, one could make sure that the various existing guidelines are understood, known, and available, and can be appropriately applied throughout the European Union. Guidance on relevant topics, and a template, could make this work easier overall, and facilitate the writing of similar guidelines in the 28 countries within the Union, even though healthcare is a national responsibility and is therefore governed by the national legislation in each country.

It is of special importance that the language and the approach used in the guidelines are carefully accommodated to the various stakeholder target groups.

General guidelines cannot substitute for advice that is specifically adapted to specific legal and security issues that may emerge in the telemedicine deployment process. That challenge is the topic of the next section of this deliverable.

4. Involve legal and security experts

This section of the report describes the issues surrounding involving and asking advice from legal and security experts in the development and implementation process of the telemedicine service. New legal and security issues may arise at any time during the telemedicine service's life span, and must be taken care of as they emerge.

4.1 What this critical success factor is

This critical success factor incorporates involving and asking advice from legal and security experts when needed, to minimise the risk of experiencing legal and security problems when deploying the telemedicine service. Usually, telemedicine doers are not experts in these matters. Legal and security assessments will also include pertinent ethical and privacy considerations, among the telemedicine experts, the telemedicine doers and the healthcare personnel involved.

It is important to be aware of the skills and expertise that the legal and security experts must have, and the tasks that they will undertake. Legal and security experts must be knowledgeable about regulations relevant to telemedicine at all levels, internationally, nationally, and locally, and must be aware that different queries may emerge at different stages of a development and implementation process. These experts are not necessarily experts on medicine. However, they do need to know the healthcare system intimately and be aware that telemedicine can provide healthcare in new and innovative ways. They must be informed that, as a rule, the general legislation in this field constitutes the basis for traditional health services being delivered in new ways.

The experts must be able to handle legal and security subjects as they arise during the whole process of planning, developing, and implementing a telemedicine service. Their tasks may comprise:

- Identifying, exploring and applying current legislation and regulations that are relevant to the telemedicine service under development.
- Undertaking "legal risk assessments" throughout the whole process, as indicated in section 2.1 in this deliverable[11].
- Undertaking information security risk assessments, where risks to confidentiality/privacy, integrity, and availability are identified and security measures are planned. By running such assessments at an early stage of the service development, "privacy by design"[12] can be achieved for the service. Risk assessment

[11] And again (cf. footnote 2): A legal risk assessment can be described as a process that runs parallel to an information security risk assessment. In it, possible legal hindrances ("risks") are identified and measures are planned and carried out to avoid risks and/or mitigate them.

[12] Privacy by design originated in the mid-1990s, and has been much promoted particularly by the Canadian authorities ever since. See especially (Cavoukian 2009).

should be repeated whenever changes are made which could influence the information security of the service.

It is also important to understand the objective(s) of this critical success factor.

4.2 Objectives

This success factor has one main objective for the telemedicine doer, which is to make sure that the telemedicine service under development ultimately is legally and securely implemented. This implies that any legal and security issues, including any ethical and privacy matters, must be scrutinised and taken care of when relevant.

Involving legal and security experts throughout the whole process will facilitate as smooth a development process as possible, and ensure that any legal and security obstacles are identified and handled at an early stage of the telemedicine deployment process.

As a result, legal and security challenges should not emerge unexpectedly. The handling of legal and security issues will be tackled as an integral part of the development process and will therefore not postpone or obstruct any on-going telemedicine development or deployment. If unexpected legal and security uncertainties emerge in relation to a telemedicine service in operation, it might influence – in a negative way – the employees' and users' willingness to disseminate and use the service, both among health professionals and patients.

4.3 Context

Significant matters to be applied by legal and security experts involve categorisation of the telemedicine service and exploration of any cross-border elements, while also bearing in mind the relevant socio-political or economic system(s):

- The initial activity should be to categorise the service e.g., as a medical act or not.
- If the telemedicine service crosses any borders – national, regional, or organisational – there will be more complex legal matters to solve, than if the service takes place within one organisation. It will also entail taking more complex technical security measures. One type of "cross-border"-service is the delivery of health services to patients performed cooperatively among healthcare institutions that are located either in the same region/country or in different regions/countries. In these situations, the following non-exhaustive list of subjects should be addressed:
    - Description of the roles and responsibility/liability of the health personnel involved.
    - Investigation of the need for legal agreements and/or contracts.
- The socio-political or economic system in which the telemedicine service operates will influence the legal requirements (i.e. laws) that have to be complied with. This implies that the legality of the service, the legislation and reimbursement rules, have

to be investigated when a service is shifted to another region or country, i.e., from one socio-political/-economic system to another.

The need for experts in the legal and security field is especially connected with the fact that the roles and the organisational tasks of the healthcare personnel alter once telemedicine is used.[13] The role of the patient will also change as a result of the introduction and use of telemedicine services.

4.4 First thoughts on pre-requisites

Adequate resources must be allocated for the involvement of legal and security expertise. Since legal and security assurance should not be regarded as a minor matter, this implies a willingness to allot appropriate financial and personnel resources for as long as they are needed. This success factor is thus related to the aggregation of resources (i.e., the pulling together of the resources needed for telemedicine deployment – see deliverable D4.2).

When resources are allocated, legal and security experts must be *available* for the telemedicine doers, the doers must know *who the experts are and where to find them* and the experts must then be *used*.

4.5 Illustration of this critical success factor from the Maccabi case

Ethical, privacy and security issues had already been dealt with in earlier Maccabi-related telemedicine services. Therefore, legal, ethical, privacy and security expertise was not needed when the Maccabi service was established. The already-existing guidelines for the central electronic medical record (which was transparent to both the medical personnel and the patients) were adapted to fit the new context. Hence, this was not considered as a critical success factor for this service. All the members of personnel in Maccabi are indeed familiar with these various guidelines and know, understand, and have been using them for some years.

4.6 Illustration of this critical success factor from the RxEye case

The Swedish RxEye service represents a new and different teleradiology service. Thus, legal consultancy and/or the presence of a lawyer was necessary. The lawyer ensured that the service complied with the relevant legal framework.

4.7 Illustration of this critical success factor from the Teledialysis case

In the Norwegian Teledialysis case, an information security risk assessment was conducted initially to comply with Norwegian legal requirements. Norwegian legislation requires regular risk assessments to be undertaken. According to the legislation in force, risk assessments shall be repeated when changes have an influence on information security (FOR-2000-12-15-1265). According to the Norwegian Code of conduct (Hdir 2014), risk assessment should be

[13] In particular, deliverable D5.2 covers a number of issues that relate to organisational management and change management.

conducted regularly. The International Organization for Standardisation (ISO) standard for information security risk management (ISO/IEC 27005 2011) states that "information security risk management should be a continual process".

In this case, measures to secure the quality, reliability and security of the service were also discussed and implemented. Local guidelines were worked out in these three fields in close cooperation with the telemedicine doers. Routines for documentation of the service were adapted to the Norwegian legislation in force.

In Norway, the telemedicine users, who are medical staff members, know whom they can ask if problems arise or if they are worried about a particular legal or security issue. The people from whom they can ask advice and guidance are lawyers and security staff at the Norwegian Centre for Integrated Care and Telemedicine (NST) in addition to the data protection supervisor at the relevant hospital.

4.8 Illustration of this critical success factor from the ITHACA case

Legal services were involved in the collaboration agreements (contracts with service level agreements). The project details were scrutinised by the ethical committee on the initiative of its promoters and it was validated. Privacy and security advice was provided by Indra, one of the organisations involved, to guarantee health level compliance with the Spanish Data Protection Act.

4.9 Illustration of this critical success factor from the Patientenhilfe case

No information pertinent to this critical success factor was given.

4.10 Illustration of this critical success factor from the KSYOS case

No information pertinent to this critical success factor was given.

4.11 Illustration of this critical success factor from the Cardio Online Europe case

No information pertinent to this critical success factor was given.

4.12 Lessons learned on involving legal and security experts from the cases

Four of the cases have explicitly reported that legal and security experts were used at some stage during the development and deployment process.

From the four reported services, it appears that:

- Maccabi – did not use legal experts at the time of establishing the service, because they had been used for the development of the underlying services from which this particular Maccabi service emerged.
- RxEye – used legal experts to make sure that this new type of telemedicine service would fit into the relevant legal framework.
- Teledialysis – used legal and security experts to conduct risk assessments, both in the security and legal fields, and for clarifications whenever they were needed.
- ITHACA – used legal experts for the collaboration agreements (contracts and service level agreements). Legal agreement is even more demanding when there are several partners taking part in the development of a new service, as was the case in ITHACA. One of the partners (BSA) had the responsibility to ensure privacy and security in compliance with Spanish law.

The three remaining respondents did not state that legal and security experts were *not* used. They simply did not comment on the matter since other aspects of telemedicine deployment were in focus when the specific services were presented and discussed.

4.13 Overall analysis on involving legal and security experts from the cases

When legal and security experts were used, they were used for different purposes and at different stages of the development and implementation process for the various services. This illustrates that experts should be available during the whole process, for the telemedicine doers to involve them when needed. Besides, the wide range of topics they were asked about, call for experts with broad skills. No matter how support from legal and security experts is organised, it presupposes an appropriate allocation of resources.

4.14 Further relevant discussion

The fact that this critical success factor was not commented on by three of the services, might illustrate that this critical success factor to a certain extent overlaps with and elaborates on the previous critical success factors about whether (or not) the service is legal, and the availability of appropriate guidelines. It seems, however, that these factors might be important at different stages of the development and implementation process.

It could be debated whether the two critical success factors concerning the use of legal and security guidelines and experts should be integrated in or presented as sub-sections of the critical success factor "Assess the conditions under which the service is legal". However, it might be of importance to draw attention to these two subjects in particular, as they might help telemedicine doers to focus on legal and security issues throughout the whole development and implementation process.

5. Ensure that telemedicine doers and users are "privacy aware"

This section of the report describes the issues surrounding ensuring that telemedicine doers and users are "privacy aware".

5.1 What this critical success factor is

Knowledge about appropriate practice when it comes to privacy and security behaviours can be termed "privacy awareness". Such knowledge is based on current ethical and legal principles and applies to developers during system design and implementation, as well as end-users during operational use. It is acquainted with "privacy by design".[14] It is therefore important to make sure that everyone who is involved in the deployment of the telemedicine service or is using it or who is handling health information maintains a high degree of privacy awareness, knows the regulations in the field, and acts in accordance with them.

"Privacy awareness" or "being privacy aware" can be achieved through education, training, strategic attitudes stipulated in the organisation, and the development of a privacy aware company culture or organisational culture. "Culture building" is intended to make telemedicine doers, the relevant stakeholders, and end-users, including patients, aware of good practice. Security measures to ensure privacy must be prioritised even if their inclusion might sometimes be experienced as bothersome and time-consuming.

Privacy awareness and a good security culture can also be achieved and maintained through repeated training measures and steady reminders about these topics.

Training must introduce norms and basic principles for "secure and privacy aware behaviour", illustrated by local guidelines, policies, and examples. Training and education could comprise the following themes:

- What is privacy and Personally Identifiable Information (PII).
- Privacy laws, policies, and principles.
- Roles and responsibilities in protecting privacy.
- Potential threats to privacy.
- Consequences for privacy violations.
- Protection of PII in different contexts and formats.

As an example of what could be included in privacy awareness training, a presentation from the United States Department of Health and Human Services offers some ideas (HHS 2014).

[14] Privacy by design (Cavoukian 2009) requires privacy awareness among developers and can lead to avoidance of many security challenges.

Other books and training programmes are available (Herold 2010), as well as e-learning courses on privacy awareness (NIH 2014) and video courses (STH 2014).

5.2 Objectives

There are three main objectives supporting this critical success factor.

The first objective is based on the presumption that privacy awareness can contribute to strengthen peoples' confidence in and, hence, willingness to use telemedicine, whether they are healthcare professionals or patients. By creating privacy awareness, the telemedicine doer will ensure two achievements. On the one hand, it will contribute to routine use of telemedicine services in accordance with best practice in the field. On the other hand, it will ensure patients' confidence in and willingness to receive healthcare via telemedicine means. The importance of confidence in this connection should not be neglected. For example, in the "Chain of Trust" project it is, among other items, concluded that "mutual confidence between users is considered crucial and should not be underestimated" (eHSG 2014, p.10).

The second objective is to take care of a patient's privacy in general in accordance with the regulations in the field.

Third, privacy awareness must enable organisations to make sure that:

- As an organisation, they are not handling patient data illegally.
- Their employees are acting legally with regard to patient privacy.
- Their patients are handling their data appropriately in terms of privacy legislation.

As background to the objectives of this critical success factor, it is important to understand the contextual setting.

5.3 Context

All over Europe, there is an increasing focus on the privacy of personal data, with the increasing number of reports on occurrence of privacy violations, like identity theft (Eurobarometer 2010).

At the same time, the European Union is strengthening online privacy rights with the adoption of a new General Data Protection Regulation (EurActiv 2013).

Technological progress and globalisation have profoundly changed the way in which data is collected, accessed, and used. Thus, the rules in Directive 95/46/EC (EC 1995) need to be modernised, since they were introduced when the internet was still in its infancy, and they do not consider new technological developments like social networks and cloud computing (EU Justice 2012).

For this critical success factor, it is important to consider that, when telemedicine services involve personnel from various organisations in the same or in more than one country, one has to make sure that the organisations’ policies concerning privacy and information security are the same or are at least compatible.

In addition, for this critical success factor, it is also significant whether or not patients are directly involved in the telemedicine service (i.e., in the case of doctor-to-patient services). In such cases, patients should also be made “privacy aware”.

5.4 First thoughts on pre-requisites

Resources for privacy awareness training must be allocated and routines for such training must be established and systematised, both for the developers of the new service and for the healthcare workers.

In the deployment of a new service, privacy awareness training should be part of the change management plan (see deliverable D5.2 for details on change management), and should thus be part of the job description of the employees in the healthcare institutions involved in the actual telemedicine service. Such training should be considered by the healthcare workers as a benefit. It should be documented and become a part of the career path of each individual, as such training is no doubt relevant for the individual’s professional development.

The management of the institution must also recognise the importance of “privacy awareness” culture building.

5.5 Illustration of this critical success factor from the Maccabi case

Patients’ consent to access to their electronic medical record by the relevant Maccabi personnel involved is a condition for patients’ subscription to the Maccabi service, which in turn is voluntary.

“Privacy awareness” is needed both for doers and for telemedicine users. It is very important, certainly from an ethical point of view.

In Maccabi, privacy awareness was addressed by making sure that everyone directly involved in the scheme (including patients and doctors) knew that access to the electronic medical record was essential for the nurses and multidisciplinary staff at the telemedicine centre.

5.6 Illustration of this critical success factor from the RxEye case

The Swedish RxEye service de-identifies radiology-related referral letters and images.[15]

Privacy awareness is important because patients should know where and by whom their medical data (including radiological images) are viewed.

[15] With de-identification one can identify the person backwards, which is not the case when data are anonymised.

Often the healthcare institution that uses teleradiologists from outside the organisation for reporting, acquires informed consent from the patient before this happens.

5.7 Illustration of this critical success factor from the Teledialysis case

In the Norwegian Teledialysis case, the duty of professional secrecy is important for the healthcare staff. If patient information goes astray due to insufficient technical security measures and/or unsatisfactory routines for the handling of patient information, this, based on a total assessment of the circumstances, might be considered as a breach of duty of professional secrecy on the part of the health professionals.

In this case, brief guidelines for secure conduct were therefore worked out in advance, to be used by both parties who took part in the video conferencing involved. They were established in order to create best practice in this field and, hence, prevent patient information from going astray which would otherwise represent a breach of legal obligations.

5.8 Illustration of this critical success factor from the ITHACA case

Patients signed an informed consent document before being checked in to using the service. Health professionals (doers) are aware of privacy issues as they are accustomed to work on electronic clinical records that have the same level of privacy protection.

5.9 Illustration of this critical success factor from the Patientenhilfe case

No information pertinent to this critical success factor was given.

5.10 Illustration of this critical success factor from the KSYOS case

In the KSYOS case, in connection with the topic of contractual arrangements with health workers and health payers, the founder of the service emphasised that telemedicine doers and users have to have privacy awareness (specifically, i.e., there has to be informed consent).

5.11 Illustration of this critical success factor from the Cardio Online Europe case

No information pertinent to this critical success factor was given.

5.12 Lessons learned on ensuring that telemedicine doers and users are privacy aware from the cases

In the context of the information provided to Momentum in response to its survey undertaken in spring/summer 2012, the respondents offered little information about training in "privacy awareness". However, in several responses, "patient consent" was mentioned as an example of privacy awareness. The same is the case for the four Momentum telemedicine services that have been analysed more thoroughly:

- Maccabi – bases its telemedicine service on the patients' consent to access to their medical records being given to relevant Maccabi personnel.
- RxEye – indicates that institutions that are using teleradiologists from outside the organisation acquire informed consent from the patient.
- ITHACA – reports that patients signed an informed consent document before starting to use the service.
- KSYOS – states that there has to be informed consent on the part of the patient.

In general, privacy awareness is mentioned by the respondents as an important topic. It is essential for the telemedicine doers, who are aware of privacy issues in their daily work (e.g., in ITHACA and Teledialysis), and it is of importance for the patients, who should know who can access their data (e.g., in Maccabi and RxEye). Teledialysis worked out brief guidelines for secure conduct, based on the risk assessment that its staff had undertaken.

5.13 Overall analysis on ensuring that telemedicine doers and users are privacy aware from the cases

Privacy awareness training is an essential part of the development of a privacy aware company culture.

Depending of the type of service, privacy awareness training should be given to a wide range of end-users. Healthcare workers should be expected to have the necessary knowledge in the privacy field. Training in privacy awareness should be offered to new doers and users when new services are adopted. In addition, whenever health information systems are updated or maintained, repeated training should be offered to more veteran or long-term doers and users.

For telemedicine services where patients are directly involved (i.e., in doctor-to-patient services), privacy awareness training, especially accommodated for the patients' needs, should be offered to the patients. Therefore:

- Patients should be made "privacy aware" in any accompanying patient consent information, as a basis for giving informed consent to the processing of their personal health information.
- Privacy awareness training/education to health personnel (i.e. telemedicine doers) should also include the legal requirements surrounding how to obtain patient consent properly.

As has been mentioned earlier, several respondents to the Momentum 2012 survey commented on issues relating to privacy awareness and patient consent. These two matters are not identical but, nevertheless, there is a relation between them.

5.14 Further relevant discussion

When privacy awareness training is planned and held, particular circumstances have to be taken into account. This includes the size of the service, both in terms of number of persons to be made "privacy aware" and geographical dispersion. These attributes, regarding service size and geographic distribution, will influence the volume of resources needed, both in terms of time and financing. Distance learning and e-learning courses are obvious alternatives in terms of the training needed for larger telemedicine services. There might be other aspects of relevance, as well: for example, adaption to various target groups and topics related to the actual service or context in particular.

In several cases, it seems that patient consent is regarded as being identical with privacy awareness (e.g., Maccabi, RxEye and KSYOS). These are not identical issues, but since patient consent is mentioned by several respondents, it should be a topic for further discussion (see also section 6 of this deliverable, specifically item 6.2).

One side of the coin is about "signing away" privacy rights, which is not in accordance with the European Data Protection Directive 95/46/EC (EC 1995).

The other side of the coin is that consent now and then emerges as a topic when it comes to use of telemedicine in general. In some cases, it is stated that use of telemedicine presupposes consent on the part of the patient. When a telemedicine service has become routine in terms of the way in which a healthcare service is delivered, how should this be handled? Should the "old-fashioned way" of doing things be upheld, in parallel, just in case somebody does not give his or her consent to the new telemedicine service being used? For instance, if RxEye presupposes that there is consent on the part of the patient, how should this be handled in the long term?

6. Observations or concerns

Overall, four observations have been raised when discussing the legality of telemedicine services, some of which are additional to matters already discussed earlier in this deliverable, others not: the accreditation of health personnel; informed consent; the size of services i.e., the size of services involving patients as a source of increased risk for legal and security challenges; and the differences between public services and private services.

1. Accreditation of health personnel

Accreditation of health personnel working with telemedicine has been raised as an issue, but is not considered as a critical success factor. Input from the Momentum survey responses gathered in spring/summer 2012 shows that opinions on this matter vary.

2. Informed consent and taking care of patients' rights

These two topics have emerged in connection with the legal and security aspects of telemedicine services, but are not identified as an explicit critical success factor. Some of the responses to the Momentum survey, however, included patient consent as an aspect of "privacy awareness", cf. section 5.13.

As these two topics are about telemedicine based on patients' consent and taking care of patients' rights, they might be considered as being about putting the patient at the centre of the service (see deliverable D5.2 for a further discussion of this issue). Opinions are, however, divided on the need for a specific form of patient consent whenever telemedicine is used as a tool for the delivery of healthcare.

3. Size of services involving few or many patients as a source of increased risk for legal and security challenges

From the data gathered through the Momentum questionnaire, it appears that some of the routine services described involved only a few patients. In a general way, special interest group 3 (SIG 3) members have therefore wondered whether legal impediments appear to be less important in relation to small-scale services than in large-scale services. If so, a possible explanation for this phenomenon could be that smaller projects are often anchored locally and are driven by enthusiasts from the healthcare sector with their sole focus being on the well-being of the patients. They may also have limited resources. Larger telemedicine initiatives have a broader focus and access to more resources.

4. Private initiative and public initiative and handling of legal challenges

Leonard Witkamp, of the KSYOS TeleMedical Centre, commented that legal issues could be handled gradually and do not necessary need to be approached at an initial stage of an initiative: "do not let [them] stop you to be an entrepreneur". This statement could be debated.

Legal challenges were handled by KSYOS by joining an International Organization for Standardization (ISO) working group and collaborating closely with the relevant standards. As Leonard Witkamp said: “Legal also runs behind/after the development.”

The debate therefore arose in this SIG, and among the consortium members, about whether there are differences between public and private initiatives when it comes to the handling and “timing” of considerations in relation to legal challenges.

7. Conclusions

Two main conclusions can be drawn with regard to telemedicine deployment in the legal and security fields:

1. It is important to take care of legal, regulatory and security challenges when the time is right

In the initial MOMENTUM questionnaire respondents were asked whether legal impediments had been decisive. No respondents thought of that as a fact, even though a few persons answered “yes” when they were asked if there were legal hindrances.[16]

Legal hindrances were also not mentioned as constraints in six of the seven in-depth cases referred to in this report (there is currently no pertinent information available related to the Patientenhilfe case). However, it is regarded as really important to pay attention to legal, ethical and regulatory issues during the process when a new telemedicine service is developed, implemented, scaled up and put into operation. In the cases described, these three aspects (of law, ethics and regulation) have been taken care of during the process, but at different stages.

Particularly, in the Maccabi example these considerations were handled beforehand in connection with another, similar service. In relation to the KSYOS case, it has been said on a general basis that the timing of the critical success factors is important, as different critical success factors might be particularly relevant at various phases of the development of a telemedicine service. For example, exploring and dealing with medical liability, privacy and ethical issues were mainly dealt with at a rather late stage in the process; in the scale-up phase following a service development phase, a usability research phase and efficiency research phase. In the other examples, however, it was reported that these issues were important from the outset.

The general conclusion on this matter is that telemedicine doers must keep an eye on legal and security issues throughout the whole telemedicine process. Specifically, the examples from the two Maccabi and KSYOS cases indicate that the right time to set to work on legal/security issues may vary, depending on the circumstances.

2. There are four critical success factors in the legal and security field

The following four critical success factors have been identified in the legal and security field:

- Assess the conditions under which the service is legal.
- Identify and apply relevant legal and security guidelines.
- Involve legal and security experts.

[16] When asked about details relating to this question, respondents referred to a lack of reimbursement schemes (this was not actually what was had in mind when the questionnaire designers posed that specific question).

- Ensure that telemedicine doers and users are "privacy aware".

The first three critical success factors are closely related and might be said to overlap or partly overlap each other. It can be claimed that two critical success factors on identifying and applying relevant legal and security guidelines, and involving legal and security experts are about how to handle and fulfil the first critical success factor outlined in this deliverable which is about assessing that the telemedicine service is legal. Therefore, an alternative way to organise the first three critical success factors could be to regard the critical success factors related to guidelines and experts as sub-elements to the assessment of the conditions under which the service is legal.

The critical success factors do not entirely, however, overlap. In this deliverable, they are therefore kept as independent and separate critical success factors. This choice has been made mainly due to the content of the responses given to the Momentum 2012 questionnaire and the in-depth analysis of the seven services.

The conclusion on this second matter is that, by offering a certain level of detail in relation to these four legal and security critical success factors, telemedicine doers can be helped to take all the relevant legal, regulatory and security aspects into consideration when the time right.

8. Bibliography

ACR (2013): "ACR White Paper on Teleradiology Practice: A Report from the Task Force on Teleradiology Practice". Journal of the American College of Radiology, Volume 10, Issue 8, Pages 575–585, August 2013. http://www.jacr.org/article/S1546-1440%2813%2900185-3/pdf (Accessed 2014-09-05)

Cavoukian A, Hoffman DA., Killen S (2009), "Remote Home Healthcare 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 2014-09-05)

Chalmers John, et al. (1999), "World Health Organization International Society of Hypertension guidelines for the management of hypertension", Journal of hypertension, 1999, vol. 17, no 2, p. 151-183

Chobanian Aram V., et al. (2003), "The seventh report of the joint national committee on prevention, detection, evaluation, and treatment of high blood pressure: the JNC 7 report", Jama, 2003, vol. 289, no 19, p. 2560-2571

CPME (1997), "Ethical guidelines in telemedicine", Standing Committee of European Doctors, CPME, 1997, http://www.unav.es/cdb/cpme97a.html (Accessed 2014-09-05)

EC (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"**,** The European Parliament and the Council of the European Union, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (Accessed 2014-09-05)

EC (2013), "Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange in accordance with the *cross*-border directive 2011/24/EU", release 1, Status: ADOPTED by the eHealth Network, Version: 1.0, 19 November 2013, http://ec.europa.eu/health/ehealth/docs/guidelines_patient_summary_en.pdf (Accessed 2014-09-05)

EC (2014), "Green Paper on mobile health ('mHealth)", Digital Agenda for Europe, http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth (Accessed 2014-09-05)

eHSG (2014), "Widespread Deployment of Telemedicine Services in Europe", Report of the eHealth Stakeholder Group on implementing the Digital Agenda for Europe Key Action 13/2 'Telemedicine', Version 1.0 final (12 March 2014) http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5167 (Accessed 2014-09-05)

ESR (2014), "ESR white paper on teleradiology: an update from the teleradiology subgroup", European Society of Radiology (ESR), 2014. http://link.springer.com/article/10.1007%2Fs13244-013-0307-z (Accessed 2014-09-05)

EU Justice (2012), "Commission proposes a comprehensive reform of the data protection rules", Data Protection Newsroom, date: 25/01/2012 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (Accessed 2014-09-05)

EurActiv (2013), "EU lawmakers vote stricter data privacy rules", published 22/10/2013, http://www.euractiv.com/infosociety/eu-lawmakers-vote-stricter-data-news-531217 (Accessed 2014-09-05)

Eurobarometer (2010), "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359. Report. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (Accessed 2014-09-05)

Finlands Läkarförbund (2004), "Medicinsk etik" *(English: "Ethics in Medicine")*, Suomen Lääkäriliiyyo/Finlands Läkarförbund, 2004, http://www.laakariliitto.fi/site/assets/files/1273/med_etik06.pdf page 187 (Accessed 2014-09-05, available in Swedish)

FOR-2000-12-15-1265, "Forskrift om behandling av personopplysninger (Personopplysningsforskriften)" http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html (In Norwegian. Accessed 2014-09-05)

English version: "The Norwegian regulations on the processing of personal data (Personal data regulations)", http://www.ub.uio.no/ujur/ulovdata/for-20001215-1265-eng.pdf (Accessed 2014-09-05)

Guirado E A, et al. (2003), "Hipertensió Arterial. Guies de pràctica clinica i material docent", Institut Català de la Salut http://www.gencat.cat/ics/professionals/guies/docs/guia_hipertensio_completa.pdf (Accessed 2014-09-05, available in Spanish)

Hdir (2014): "Norm for informasjonssikkerhet helse- og omsorgstjenesten (Normen)", http://normen.no (In Norwegian. Accessed 2014-09-05)
English version: "Code of Conduct for information security in the healthcare, care, and social services sector" http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/english/Sider/default.aspx (Accessed 2014-09-05)

Herold R (2010), "Managing an Information Security and Privacy Awareness and Training Program", CRC Press 2010 http://www.amazon.com/Managing-Information-Security-Awareness-Training/dp/1439815453 (Accessed 2014-09-05)

HHS (2014), "Privacy Awareness Training", US Department of Health and Human Services http://www.hhs.gov/ocio/securityprivacy/awarenesstraining/privacyawarenesstraining.pdf (Accessed 2014-09-05)

HOD (2001), "Telemedisin og ansvarsforhold" *(English: "Telemedicine and Responsibility")* http://www.regjeringen.no/nb/dep/hod/dok/rundskriv/2001/i-122001.html?id=108946 (Accessed 2014-09-05, available only in Norwegian)

ISO 9001:2008, "Quality management systems – Requirements", International Organization for Standardization (ISO), http://www.iso.org/iso/catalogue_detail?csnumber=46486 (Accessed 2014-09-05)

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 2014-09-05)

ISO/IEC 27001:2013, “Information technology — Security techniques — Information security management systems – Requirements”, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (Accessed 2014-09-05)

Jack C, Mars M (2008): “Telemedicine: a need for ethical and legal guidelines in South Africa”, SA Fam Pract 2008, Vol 50 No 2. http://www.ajol.info/index.php/safp/article/viewFile/13441/64239 (Accessed 2014-09-05)

Legido-Quigley H, Doering N, McKee M (2014): “Challenges facing teleradiology services across borders in the European union: A qualitative study”*,* Health Policy and Technology, Vol 3 No 3, pp160-166, September 2014 http://www.healthpolicyandtechnology.org/article/S2211-8837(14)00029-X/abstract (Accessed 2014-09-05)

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (The Spanish Personal Data Protection Act)

Loane M, Wootton R (2002): “A review of guidelines and standards for telemedicine”, Journal of Telemedicine and Telecare 2002; 8: 63.71, http://jtt.sagepub.com/content/8/2/63.full.pdf+html (Accessed 2014-09-05)

NIH (2014), “NIH Information Security and Privacy Awareness Training”, National Institutes of Health: http://irtsectraining.nih.gov/ (Accessed 2014-09-05)

Norsk Psykologforening (2002), “Veileder for psykologers faglige virksomhet på Internett» *(English: “Guidance on psychologists' professional activities on the Internet”)*, Tidsskrift for Norsk Psykologforening, 2002, http://www.psykol.no/content/download/34530/345933/version/1/file/veilederTNPF2002.pdf (Accessed 2014-09-05, available only in Norwegian)

STH (2014), “STH.Healthcare Training”, http://www.securingthehuman.org/healthcare/demo-training-lab (Accessed 2014-09-05)

Sundhedsstyrelsen (2005), “Vejledning om ansvarsforholdene mv. ved lægers brug af telemedicine” *(English: “Guidance on Responsibilities etc. by Doctors’ use of Telemedicine”)* http://sundhedsstyrelsen.dk/da/udgivelser/2005/vejledning-om-ansvarsforholdene-mv-ved-laegers-brug-af-telemedicin.aspx (Accessed 2014-09-05, available only in Danish)

UEMS (2009), “European definition of the Medical Act”, UEMS 2009/14, 25 April 2009, http://www.uems-ophtalmologie.org/uems_documentation_doc_9i_definition_medical_act.php (Accessed 2014-09-05)

WHO (2012), “Legal frameworks for eHealth”, Global Observatory for eHealth series, Volume 5, World Health Organization. http://www.who.int/goe/publications/ehealth_series_vol5/en/ (Accessed 2014-09-05, available in English, French and Spanish)