Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of

patient summary and electronic prescription

Key Task 2.1.1

Legal and Regulatory Requirements at EU level

February 24th, 2012

Document Version: final

Document Information

Project name	KT2.1.1 Legal and Regulatory Requirements at EU level
Author/ person responsible	Zoi Kolitsi , Sebastian Reimer
Document owner	Sebastian Reimer, Zoi Kolitsi
Document name	D2_1_1_legal_requirements_final
Status	Final submitted

History of Alteration

Version	Date	Editing description	Editor
0.1	21-03-2011	First draft	Sebastian Reimer
0.2	11-04-2011	Chapter on third country data transfer added	Sebastian Reimer
0.3		Further information, esp. on liability added; revision	Sebastian Reimer
0.4	19-09-2011	Fundamental revision based upon D1.4.1	Sebastian Reimer
0.5	26-09-2011	Revision based upon WP2.1-TCon	Sebastian Reimer
0.6	11-10-2011	1st draft for WP21	Sebastian Reimer
0.7	20-10-2011	Revision based upon written comments from Zoi Kolitsi, Lucyna Luczak and Karel Neuwirt as well as the second WP2.1-TCon	Sebastian Reimer
0.8	02-11-2011	Revision based upon written comments from Zoi Kolitsi, Lucyna Luczak and Petra Wilson	Zoi Kolitsi, Sebastian Reimer
0.81	06-11-2011	Revision against the backdrop of WP21 f2f meeting in Athens with particular input from Zoi Kolitsi, Lucyna Luczak, Caroline Ringstad-Schultz and Petra Wilson	Sebastian Reimer
0.82	18-11-2011	Incorporation of final comments from Zoi Kolitsi and Petra Wilson	Sebastian Reimer
0.9	25-01-2012	Changes after Brussels use case workshop and Vienna TPM meeting; includes treatment of comments by NEPCs	Zoi Kolitsi
Final draft	07-02-2012	Revision based upon written comments TPM, NEPCs and WP2.1. core group	Zoi Kolitsi, Sebastian Reimer
Final	24-02-2012	Revision after QA	Zoi Kolitsi

Reference Documents

Date	Type	Description	Version	Origin	Document
21/10/2011	deliverable	epSOS_use case description	Approved by PSB	WP1.4.	D1.4.1

Disclaimer

The views expressed in this document may not, in any circumstances, be interpreted as stating an official position of the European Commission. The European Commission does not guarantee the accuracy of the information included in this document, nor does it accept any responsibility for any use thereof. Reference herein to any specific products, specifications, processes, or services by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute nor imply its endorsement, recommendation, or favouring by the European Commission. All care has been taken by the authors to ensure that they have obtained, where necessary, permission to use any parts of manuscripts including illustrations.

Table of contents

Abbreviations and acronyms

acc.	according
ann.	annotation
Art.	Article
cf.	confer
CONTsys	System of concepts to support continuity of care
D*x…*	(epSOS) Deliverable *x…*
DG	Directorate General
DP	Data Protection
DPA	Data Protection Authority
DPD	Data Protection Directive (D 95/46/EC)
DPR	Data Protection Regulation (proposal state at the moment)
EC	European Commission
EC	European Community
EU	European Union
EEA	European Economic Area
EESSI	Electronic Exchange for Social Security Information
EED	epSOS Evolving Document
EHR	Electronic Health Record
EFTA	European Free Trade Association
e.g.	example given
eID	electronic Identification
eP	ePrescription
et sqq	et sequentes (“and the following”)
FWA	(epSOS) Framework Agreement
HC	healthcare
HCP	healthcare provider
HS	Health System(s)
ICT	Information and Communication Technology
i.e.	id est (“that is”)
IMI	Internal Market Information System
incl.	including
ISMS	Information Security Management System
L	Leges/Lois (“laws”)
LI	Liability

lit.	litera
MDD	Medical Device Directive (D 93/42/EEC)
MED	medication
MRO	Medication Related Overview
MS	Member State
MTC	Master Translation Catalogue
NCP	National Contact Point
NEPC	National EpSOS Pilot Coordinator
no.	number
OJ	Official Journal (of the European Union)
p.	page
PAC	Patient Access
para.	paragraph
PIN	Patient Information Notice
PN	(epSOS) Participating Nation
PNR	Passenger Name Records
PQD	Professional Qualifications Directive (D 2005/36/EC)
PR	Professional & Regulatory
PRD	Patients' Rights Directive (D 2011/24/EU)
PS	Patient Summary
Reg	Regulation
resp.	respective(ly)
SCC	Standard Contractual Clauses
TFEU	Treaty on the Functioning of the European Union (= former Treaty establishing the European Community)
UC	Use Case
WP	(epSOS) Work Package

Executive Summary

The objective of this document is twofold: on one hand it answers to the most relevant epSOS related legal questions that relate to the epSOS extension; on the other hand a fundamental understanding of epSOS' legal foundation is provided.

The document builds on D2.1 Legal and Regulatory constraints on epSOS which has examined the legal basis for cross border health data exchange and intends to elaborate requirements emerging from the extension of epSOS as well as the evolving EU regulatory environment. The process involved a review of legal developments since the delivery of that document as well as new knowledge that emerged as a result of discussions and decisions in the process of implementation of the epSOS Framework Agreement (FWA).

The first two chapters (Introduction and Background) provide the general framework for the development of this document and links to work in epSOS with respect to completed or ongoing tasks.

The extension of epSOS is two-dimensional: on the one hand the number of Participating Nations is increased (chapter 3.1) raising especially the issue of transmission of data to third countries (chapter 3.1.1). On the other hand the epSOS is extended to additional use cases, which focus on communication of treatment information back from country B to country A; extended access and update of medication information abroad; emergency call systems and patient's increased autonomy due to the new Patient Access use case. Chapter 3 gives the context of use of epSOS services and describes the requirements derived from the two dimensions of extension. These are summarised in chapter 3.3 in tabular form, giving title, unique ID and short description.

The legal foundations that have become relevant in addition to epSOS I are described in chapter 4. The "new" relevance of them can either be due to the extension of epSOS, which is for example the case with regard to the transmission of health data to third countries (chapter 4.1) or to new legislation that has been enacted since the last legal analysis in the course of epSOS I, which is for example the case for chapter 4.3, dealing with the Patients' Rights Directive, adopted in 2011. Although epSOS will not deal with issues of the Social Security Systems Regulation (EC) 883/2004, a view to co-ordinating any overlaps of epSOS with other projects like EESSI (Electronic Exchange for Social Security Information) and epos NCPs with organizations like the NCPs according to Art. 6 PRD (chapter 4.3.5) must be always maintained. Section 4.4. on conflict of laws is also inspired by the extension of epSOS, as third countries are not (directly) subject to the Rome Regulations and might be not included into the Brussels Regime – an issue that can possibly lead to further legal questions.

The use of terms and definitions are provided in the appendix.

1 Introduction

The objective of this document is twofold: on one hand it answers to the most relevant epSOS related legal questions that relate to the epSOS extension; on the other hand a fundamental understanding of epSOS' legal foundation is provided.

The document builds on D2.1 Legal and Regulatory constraints on epSOS which has examined the legal basis for cross border health data exchange and intents to provide a review of legal developments since the delivery of that document as well as new knowledge that emerged as a result of discussions and decisions in the process of implementation of the epSOS Framework Agreement (FWA).

In addition a Liability Analysis has been performed in order to facilitate the localization of the FWA. The **epSOS Liability Analysis** is an ongoing process which follows the developments in the definitions of the epSOS services, their delivery and the "production" processes in epSOS. It focuses on the pilot nature of the project, but it is meant as an evolving document itself by exploring aspects and lessons learned that would apply to the full deployment of epSOS services. It addresses general concepts in liability flow, rather than setting out specific legal rules. As such it does not enter into the detail of national variations on general European concepts of liability for goods, services or data, leaving it to participating nations to ensure that local legal experts have agreed that compliance with local legislation is achieved.

The document was developed in parallel with the discussion on the extension of use cases and has undergone several revisions following the central discussion in the project. A first round of discussion with the NEPCs yielded few but very useful inputs.

In the meantime the draft Regulation replacing the Data Protection Directive became available still in the form of a discussion document. Although not in vote and adopted at this point, it was felt important to also consider the thrust and directions that it shall provide in the future. At this stage D2.1.1. does not include a section with a full legal analysis of this Regulation; however some initial observations are outlined as part of the background discussion.

The final edited version incorporates a concept based description of how present and future use cases are integrated into the national workflows. This description has been drafted on the basis of the following inputs:

- a working session on the CONTsys concept model and candidate standard in Brussels organized on December 13th by epSOS WP2.2. (KT 2.2.1.);
- the use case consolidation workshop on December 14th facilitated by WP1.4;
- the epSOS video which became available on www.epSOS.eu end of 2011, demonstrating full integration of epSOS services into the clinical practice and ICT tools at national level and the capacity to update the prescription registry in the country of affiliation by information returned by the country of treatment; and
- the comments returned as a result of the validation with the NEPCs.

The epSOS consultation and consolidation activities has been instrumental in shaping the high level concepts around the context of use of the epSOS use cases which is the cornerstone and the needed foundation to address data protection and liability issues effectively.

Therefore this document incorporates a description of the epSOS services and their context of use as part of the national health care processes. It should be noted that it is not the task of WP2.1. to define such processes but rather to interpret information in the different parts of the project in order to create clarity for the legal experts in PNs. Therefore, the description in chapter 3.1. should be read as an interpretation rather than a definition of such processes which are expected to be delivered elsewhere in the project.

2 Background

Cross-border care in epSOS so far has been conceived around two use cases (UC) and foresees both scheduled and unscheduled encounters. UC 1 refers to an occasional visitor in country B and UC 2 to a regular visitor or long term visitor to country B.

The purpose of access to information contained in a Patient Summary or an e-prescription is to improve continuity of care by supporting health professionals to improve patient care in cross border encounters. The epSOS Patient Summary (PS) does not hold detailed medical history or details of clinical conditions or the full set of the prescriptions and dispensations. It is based on a commonly agreed set of basic information about the patient including current medications and known allergies. The project will also enable patients to have e-Prescriptions from their country of residence dispensed at designated epSOS pharmacies in other participating countries.

Each country is responsible for the content of the Patient Summary and the e-Prescription and its creation. The use of the epSOS services is voluntary on the part of the patient. Use of the epSOS services does not alter obligations to fulfil legal requirements existing in the country where medical care is provided to the patients participating in the epSOS pilot.

The present situation with e-prescription is that an e-dispensation notification will be returned to the country where the e-prescription was created. It is then possible that this information is used to update the list of active prescriptions in country A. With respect to the epSOS Patient Summary, the situation is that when a medical intervention occurs in a country B it will be duly recorded there within the local record keeping rules. However the Patient Summary is not updated in country B to reflect the encounter. Therefore, such correspondence is not part of epSOS and happens only in accordance with usual practice at the foreign healthcare provider.

epSOS is now expanding to more nations and extended as well to new use cases; an overview of this extension maybe found in chapter 3.1.

2.1 Background on the Data Protection Regulation

At the end of 2011 the proposal of the Commission for a *Regulation 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*)[1] was in broader discussion within the EU Commission and competent national organizations.

This – being still a draft – has not been considered for in depth analysis by the epSOS legal experts' team. It is however interesting to note some additional new elements, in particular the transparency principle, the clarification of the data minimization principle and the establishment of a comprehensive responsibility and liability of the controller.

The Regulation considers (recital 104) the processing of data concerning health, including health data as a special category of data which deserves higher protection, which may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore the Regulation provides for harmonized conditions for the processing of personal data for health purposes, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health,

[1] Proposal for a Regulation 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), COM(2012) 11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited: Feb. 7th, 2012). Citations of the DPR within this document refer to this version.

for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided.

With respect to challenges that epSOS faced in the past and in the extension, the Regulation provides vital clarity building on the current Data Protection Directive 95/46/EC. Due to the fact of being an EU Regulation the Data Protection Regulation will come directly into effect within all EU Member States. National law in the scope of the Regulation – as for example the national data protection laws – will have to be repealed, unless specified otherwise in the Regulation as for example in Art. 81 para. 1 DPR concerning national law that provides safeguards to the processing of health related personal data.

2.1.1 Data Security and Patient Consent

(i) **Security and Patient Consent**

- The Regulation clarifies the conditions for Consent to be valid as a legal ground for lawful processing as well as Data Security high level requirements.
- The Regulation obliges the controller and the processor to implement appropriate measures for the security of processing, based on Article 17(1) of Directive 95/46/EC and extending that obligation to processors, irrespective of the contract with the controller. This is particularly relevant to epSOS which will now need to proceed to define such "appropriate" measures.
- The Regulation also introduces a mandatory data protection officer (currently Article 32) and the drawing up of sector specific codes of conduct
- Member States are obliged to further to the conditions for special categories of data, to ensure specific safeguards for processing for health purposes (currently Article 81).

2.1.2 Transfer to third countries

The Regulation will also clarify transfers to third countries, where no adequacy decision has been adopted by the EU Commission, to adduce appropriate safeguards, in particular standard data protection clauses, binding corporate rules and contractual clauses. As a new component, such standard data protection clauses may now also be adopted by a supervisory authority and be declared generally valid by the Commission. Binding corporate rules are now specifically introduced in the legal text. The option of contractual clauses gives certain flexibility to the controller or processor, but is subject to prior authorization by supervisory authorities.

Other areas of the Regulation that bear immediate relevance to epSOS and the specification of epSOS services include:

- the obligation of the controller to provide procedures and mechanism for exercising the data subject's rights, including means for electronic requests, requiring response to the data subject's request within a defined a deadline, and the motivation of refusals (Art. 10 DPR);
- the obligation to notify personal data breaches, building on the **personal data breach notification** in Art. 4 para. 3 of the E-Privacy Directive 2002/58/EC (Art. 31 and 32 DPR);
- the obligation of controllers and processors to carry out a **data protection impact assessment** prior to risky processing operations (Art. 33 DPR); or
- in some specific situations, e.g. third country data transfers, the obligation of the controller to obtain an authorization from the supervisory authority (Art. 34 DPR).
- an obligation for documentation (currently article 28) foreseen as part of the tasks of KT2.1.3.

The above list of relevant areas of the DPR is by no means complete and additional new principles and requirements of the DPR proposal can substantially affect decisions in epSOS and shall therefore be subject of further work in epSOS as for example questions in the context of:

How will epSOS fulfil this requirement and what are the implications for the pilots of the following requirement?

- Article 33 on Data Protection Impact Assessment stipulates that if the processing of health data is a specific risk to the rights and freedoms of individuals then the controller shall carry out an assessment.
- Article 34 on Prior Authorisation and prior consultation i.e., in some specific situations which also related to data transfer, the data controller should obtain an authorisation from supervisory authority or is obliged to consult them.
- Article 35 on Data protection officer i.e., if the healthcare provider is the public body then it must appoint a DP officer.

Are the following requirements applicable to epSOS ? How ? When?

- the right to data portability (Art. 18 DPR);
- joint controllers (Art. 24 DPR); or
- the communication of personal data breaches to the data subject (Art. 32 DPR).

3 epSOS Extension

epSOS has at this stage established foundations of organizational, legal, semantic and technical interoperability. The extension shall demonstrate that these infrastructures can accommodate all Participating Nations (PNs) and can support further development of use cases, eventually leading to a sustainable mechanism.

3.1 Extension to additional Participating Nations

epSOS initially foresaw piloting between 10 European Member States. The extension of epSOS includes Norway (EFTA[2]), Switzerland and Turkey (third countries). Third countries are all non-EEA[3] states, as for example Albania, Croatia, Macedonia, Serbia, Switzerland or Turkey.

Norway, Iceland and Liechtenstein – being EFTA and thus EEA member states – adopted the Data Protection Directive (DPD) by Decision of the EEA Joint Committee (see below footnote 12, p. 28).

Switzerland, is accepted by the European Commission (EC) as having a sufficient level of data protection through Decision 2000/518/EC of July 26, 2000. This is currently not the case for Turkey.

3.1.1 Transmission of data to third countries

Issue:	**Issue code:**	**Primary legal reference:**
Transmission of data to third countries	L-DP-01	Articles 25 et sqq DPD
Process	**Process step**	
This is a horizontal issue that cuts across all use cases	access of health professionals to health data from abroad	
Description:		
With regard to those countries that have been certified as having an adequate level of data protection, the legal approach – from the data protection point of view – may be the same as for EU Member States. Switzerland for example could implement the Framework Agreement the same way as EU Member States. When a EU MS wishes to export data to a third country, that has not been accredited as having an adequate level of data protection by the European Commission, additional legal safeguards are required. According to the Data Protection Directive (DPD) one solution is to conclude contracts, based on model contracts, which are published by EC Decisions and are also called Standard Contractual Clauses (SCC). Such contracts are to be concluded between the data exporter and the data importer and may "*include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses*"[4]. WP2.1 has considered the alternatives and proposes that epSOS will offer a standard form contract which incorporates the required SCC as well as the necessary elements of the FWA so		

[2] European Free Trade Association, http://www.efta.int (last visited: Nov. 6th, 2011).

[3] European Economic Area.

[4] Cf. for example Clause 10 of the Standard Contractual Clauses as provided for in the Annex of EC Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, OJ L 39, 12.2.2010, p. 5 et sqq.

that Turkey or another third country can draft a contract to allow exchange of data within the terms of the Data Protection Directive (DPD).

This discussion needs to be concluded with Turkey before any proposals are brought forward to the PSB.

3.1.2 Extension of existing uses cases

epSOS is also expanding in a number of new areas in the Patient Summary and the e-prescription use cases and also engaging in two new areas, namely patient accessing own data and emergency 112 services accessing patient. These use cases are described in deliverable D1.4.3. and the reader is referred to that deliverable for the details of the use case description. What is more relevant for the legal analysis is undemanding the context of use of epSOS services as part of the day to day care processes. This concept is briefly described below:

All the epSOS services, including the ones developed under D1.4.3. are intended to improve the care provided to a patient in a cross-border health care situation. Therefore, the utility of the epSOS services ultimately depends on the way the services perform in actual clinical processes. The clinical process and its central concepts can be visualized in the following diagram, which is representative of a general process, which is conceptualized at a generic level, non specific to the national environment.

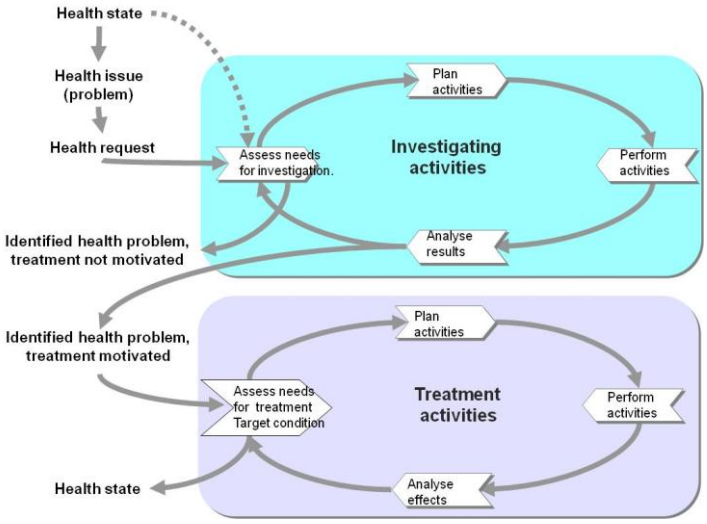

Figure 1: The general clinical process and associated concepts as used in the analysis for national electronic health records development in Sweden.

The epSOS services facilitate the *clinical process* by supporting one specific relation in the CONTsys concept model – that of accessing a part (extract) of a health record (read or write, with translation), within a *health care activity period*. Since this access is part of a clinical process, it also is described by the concepts of *health care mandate* (authorization), which is based on either law or (usually) consent. Even the patient access is, conceptually, a situation where the patient is a health care actor providing the mandate to retrieve and process his or her own data.

Thus, the added value the epSOS services provide for the patient and the health professional can be located to the clinical process, which facilitates identifying specific needs for these services, e.g. the semantic content needed for developing the services for specific health issues.

The epSOS video at http://www.epsos.eu demonstrates how this has been made possible in practice in epSOS so far: the epSOS functionality is included in the natural process flow at the community pharmacy; some additional safeguard such as the collection of the written informed consent

required by national legislation are implemented; the delivery of the medication in the country of treatment (Greece) results in an update of the dispensation status in the country of affiliation (Italy).

3.1.3 Context of Use of epSOS services within the national care process

The epSOS use cases in their extended form involve a number of generic processes and process steps. For the purposes of the legal and regulatory analysis the following model has been developed, based on CONTsys concepts[5]. Figure 2 illustrates how the clinical process in as much as it is relevant to the epSOS scope can be portrayed in the form of a block diagram. This format allowed a better understanding of involved parties, their main roles in the process and their mandates and responsibilities. It is not the intention here to enter into details of the clinical process beyond what is necessary for the legal analysis i.e., who performs what type of data processing on what data for what purpose.

It is also noted that the terms and concepts used are defined under Concepts and Terms and they are derived from the CONTsys data dictionary.

On the background of the global high level clinical process of figure 2, represents an aggregation of displays specific to each use case provided in Annex II as part establishing clear links to D1.4.3.

- These elements of the epSOS extensions of use cases are portrayed using the following conventions: solid green lines indicate national data flows regulated by national regulations and/or law;
- Red solid lines indicate international access made possible through incorporating the epSOS specification in national implementations and applying the epSOS legal and security safeguards;
- Red dotted lines represent return of information from the country of treatment to the country of affiliation for incorporation into national repositories according to national procedures and responsibility;

A subject of care may access own data in the country of affiliation if national legislation and implementation permits; this data is normally found in sharable national repositories. These repositories may also include data on access logs making it possible for person to know who has accessed his/her health data. epSOS extension foresees that patient access to the epSOS Patient Summary will be made possible. WP 2.1. has recommended,- and lately WP29 in their epSOS working document has also issued a recommendation to the project – to consider also patient access to the epSOS access logs, an issue which is however still in discussion. Last but not least a data subject may access his/her epSOS patient summary with the intention to provide this information to a health professional in the context of an established care relationship (consent/commitment) thus replacing the need for providing specific consent to access to data by a health professional in non emergency cases.

A health professional will normally access health information of subjects of care he/she has made a healthcare commitment to, in order to plan or perform clinical activities or evaluate clinical results and make clinical decisions. Such data is also sharable data e.g. in national repositories, the Medication Related Overview (MRO) or an ePrescriptions repository. He/she also contributes new data resulting from these clinical activities. epSOS use cases and their extensions make it possible to access such sharable data by a health professional in a country of treatment abroad and to return

[5] To maintain a consistent perspective into this process, the epSOS services were mapped onto the ContSYS – based NHS continuity of care concept model, http://www.datadictionary.nhs.uk/contsys/ (last visited: Feb. 7th, 2012).

new health information created abroad for incorporation into the national repositories of sharable data including through depositing such data into an epSOS e-Safe[6].

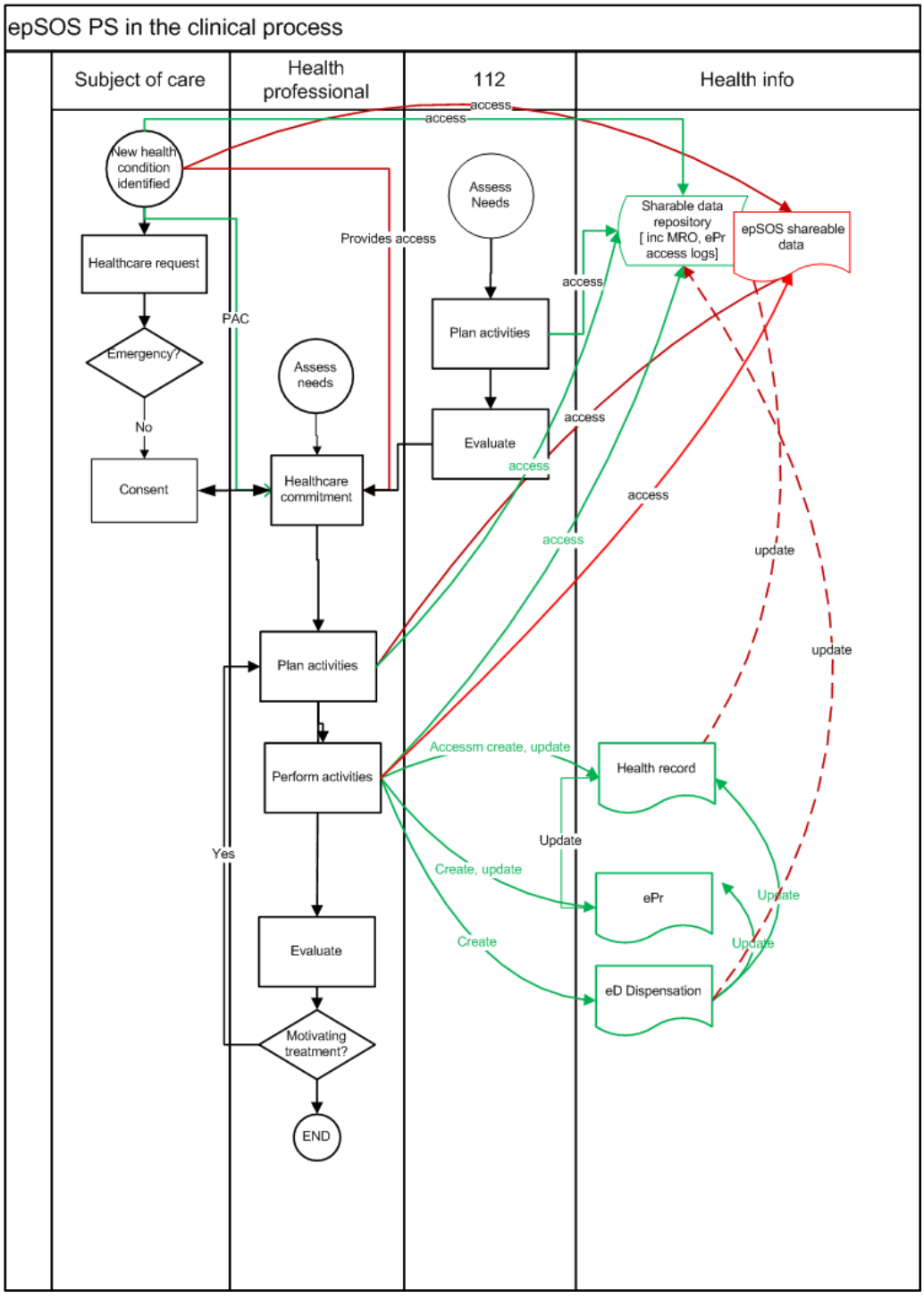

Figure 2: A block diagram conveying the clinical process of figure 1 in the context of clinical epSOS

An Emergency 112 service in a country other than the country of affiliation may be provided access to a subset of patient summaries suitably selected to support decision making, appraisal of the

[6] The inclusion of an epSOS data sink under the full control of the patient is not definitive at present.

clinical situation and planning of activities. epSOS use cases make it possible that such access to information is also provided in the epSOS format to an 112 service abroad.

The **epSOS shareable data is**

the epSOS Patient Summary;

[potentially] the Medication Related Overview;

the list of active e-Prescriptions; and

[potentially] the cross border access logs.

Access to these documents is provided to health professionals and patients according to national legislation at the country of treatment.

The **means of access to these documents is** through the epSOS National Contact Points that make available this information in the form of standard epSOS displays in the local language or through access to an data sink under the full control of the patient where new information originating in the country of treatment may be deposited..

The **update of the shareable epSOS data from abroad** is through return of information in the epSOS format from the country of treatment to the NCP of the country of affiliation. A "push" approach has been adopted where the treating health professional submits the created record through his/her NCP to the country of affiliation; further action for incorporating into the national repositories is normally taken at the home country unless directly actualized as in the case of e-Dispensation in the country of treatment, triggering an automatic update of the active ePrescription list (already shown to be possible in epSOS).

No personal health data from country B can be stored at NCP-A (see L-DP-07). An alternative route for returning updates of sharable data could be through an epSOS data sink under the full control of the patient which would be managed by the patient; update information in this case would be forwarded to the appropriate function in the country of treatment by action of the patient.

In all cases, triggering an update of the list of active e-prescriptions r is just an option and in principle, country A decides how to handle dispensation reported from country B.

3.2 Legal Requirements

The requirements that are documented in this section are legal requirements; as such they are non functional requirements and are intended to provide the legal and normative framework towards better defining the use cases, increasing their value as facilitators for cross border eHealth and also to provide certainty around major decisions in the project implementation approach.

The intention is that they are regularly reviewed especially in the light of new knowledge in the EU data protection policy domain.

The requirements are classified under the categories defined in "D2.1. Legal and Regulatory Constraints for epSOS Design - Participating Member States" which are:

- Data Protection and Confidentiality (DP),
- Health Systems (HS),
- Professional & Regulatory (PR) and
- Liability (LI).

3.2.1 The epSOS NCP within the Patients' Rights Directive

Issue:	Issue code:	Primary legal reference:
The epSOS NCP within the Patients' Rights Directive	L-HS-01	Art 6 PRD National Contact Points for cross-border healthcare
Process	**Process step**	
Preparation	establishment and commissioning of the epSOS NCP conclude legal agreements	

Description:

PNs shall establish National Contact Points for cross border care and communicate them to the European Commission. Those NCPs shall co-operate to create transparency to patients on their rights to cross border care and information on the HC system.

Besides the obvious conflict of the term "NCP" used in different ways in epSOS and in the Patients' Rights Directive (PRD) a further analysis of the relationship between the two in the context of the PRD must further explored, including opportunities to co-locate the PRD and epSOS functions.

3.2.2 International epSOS agreements

Issue:	Issue code:	Primary Legal Reference:
International epSOS agreements	L-HS-02	Art. 10 para. 2 and 3 as well as Art. 14 PRD
Process	**Process step**	
Preparation	conclude legal agreements	

Description:

The legal framework of the PRD creates conditions for sustainable international (interoperability) legal agreements for sustainability of epSOS services.

Acc. to Art. 14 PRD Member States shall facilitate cooperation in cross-border healthcare provision at regional and local level as well as through ICT and other forms of cross-border cooperation. The European Commission shall encourage Member States, particularly neighbouring countries, to conclude agreements among themselves. The Commission shall also encourage the Member States to cooperate in cross-border healthcare provision in border regions.

epSOS must address this challenge, see also L-DP-03. For further harmonization on data protection, data controller roles should be pursued.

3.2.3 Electronic cross border access to medical information

Issue:	Issue code:	Primary legal reference:
Remote access to medical	L-HS-03	Art. 5 lit. d and Art. 14 PRD

information		responsibility of MS of affiliation
Process	**Process step**	
Preparation	PS and prescription are made available in epSOS standards	
Description:		
Patients who seek to receive or do receive cross-border healthcare must have remote access to or have at least a copy of their medical records, in conformity with, and subject to, national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC (Art. 5 lit. d PRD). The voluntary network of Art. 14 PRD shall draw up guidelines on a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders. The epSOS Patient Summary must be aligned /influence the development of these guidelines.		

3.2.4 Patient Information Notice (PIN)

Issue:	**Issue code:**	**Primary legal reference:**
Patient Information Notice	L-DP-02	Art. 8 para. 2 lit. a and Art. 10 para. 3 DPD
Process	**Process step**	
Preparation	obtaining patient's prior agreement to epSOS pilots	
Description:		
The extension of epSOS to third countries and new use cases, as well as the possibility for patient to get access to own data and provide it to health professionals (in analogy to the way patients provide paper records to health professionals today), introduces new challenges on information to be provided to patients and will require a considerable update of the Patient Information Notice (PIN). Such information must be sufficient – i.e. the right level and content – to enable the patient to give explicit consent to the processing of data in accordance with the requirements of the DPD and the anticipated Data Protection Regulation.		

3.2.5 Security

Issue:	**Issue code:**	**Primary legal reference:**
Security	L-DP-03	Art. 1 para. 2 and Art. 17 DPD Art. 14 PRD
Process	**Process step**	
Preparation	Establish an ISMS, including regular audits; Communicate results and obtain permission to enter the epSOS pilot	
Description:		

The Member States – through the voluntary Network acc. to Art. 14 PRD – shall work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare.

From a European perspective, security requirements vary considerably in Member States. The new Data Protection Regulation provides clarity. What should be pursued is the specification of a realistic appropriate security level and a description of a code of conduct which can be gradually enhanced, that will allow PNs to implement basic cross-border services and continue to optimize, align and gradually improve them.

epSOS addresses this challenge by pursuing agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations and elaborate such codes of conduct as part of the epSOS Information Governance.

The Patient Access Use Case (PAC) can also play an important role as an alternative method of providing consent.

A possible long-term solution could arise from the Data Protection Regulation, esp. Art. 30 para. 3 that empowers the EU Commission to "*to adopt delegated acts [for] further specifying the criteria and conditions for the technical and organisational measures […], including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology*".

3.2.6 Informed Choice

Issue:	**Issue code:**	**Primary legal reference:**
Informed Choice	L-HS-04	Art. 4 para. 2 lit. a and b PRD
Process	**Process step**	
Access to cross border care	patient accesses cross border care	

Description:

The member state of treatment shall create conditions of transparency on standards applied and inform about "*… availability, quality and safety of the healthcare provided*" (Art. 4 para. 2 lit. b PRD).

epSOS healthcare providers shall report on availability of epSOS services and performance data and shall provide clear information sheets for patients on use of epSOS sites.

3.2.7 Common identification and authentication measures

Issue:	**Issue code:**	**Primary legal reference:**
Common identification and authentication measures	L-DP-04	Art. 14 PRD
Process	**Process step**	
Healthcare encounter	Identification of patient (including authentication and authorization)	

Description:
The Art. 14 PRD voluntary network shall support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare. epSOS shall consider the opportunity to migrate to such a common eID EU approach.

3.2.8 Authorization

Issue:	**Issue code:**	**Primary legal reference:**
Authorization	L-DP-05	Art. 1 Directive 2005/36/EC on recognition of professional qualifications (PQD) Art. 10 para. 4 PRD
Process	**Process step**	
Healthcare encounter	Identification of health professional (including authentication and authorization)	

Description:
Member States of treatment shall ensure that information on the right to practise of health professionals listed in national or local registers established on their territory is, upon request, made available to the authorities of other Member States, for the purpose of cross-border healthcare. The Directive on Professional Qualifications requires that all MS recognize the qualifications regulated professions which include doctors, nurses, midwives, and pharmacists. Accordingly, given that epSOS will not provide means for NCP-A to verify status of right to practice e.g. through IMI, epSOS shall include organisational safeguards for verifying professional qualification and the right to practice in country B. epSOS shall consider the opportunity to incorporate provisions for authorization of health professionals, in compliance to the PRD.

3.2.9 Patient Consent

Issue:	**Issue code:**	**Primary legal reference:**
Patient Consent	L-DP-06	Art. 8 para. 2 lit. a and c DPD
Process	**Process step**	
Healthcare encounter	Patient consent Patient shares health data with health professional	

Description:
Explicit consent for returning data back from country of treatment to country of affiliation will be required to be provided to the health professional in country B. The possibility of indirect access of the health professional to health data through patient access creates new opportunities and risks to patient consent and must be thoroughly investigated. Purpose and manner of the data processing need to be covered by the patient's consent. The two step approach of epSOS – i.e. full, general information at the time of participation (epSOS Privacy

Information Notice & Terms and Conditions) plus individual information at the time of access (either by the epSOS healthcare provider or for example a message box with regard to each use case) – can also be used.

For the 112 Emergency use case in addition access to data for emergency purposes will be on the additional legal ground of vital interests (Art. 8 para. 2 lit. c DPD) that is very likely to be applied in those cases, as patients will rarely be able to consent in the situation of emergency.

3.2.10 Right to access to health information

Issue:	**Issue code:**	**Primary legal reference:**
Right to access to health information	L-HS-05	Art. 4 para. 1 lit. a PRD
Process	**Process step**	
Health care encounter	Health professional requests access and receives Patient Summary/e-prescription/medication record from abroad according to professional role	

Description:

Cross-border healthcare shall be provided in accordance with:

- the legislation of the Member State of treatment,
- standards and guidelines on quality and safety laid down by the Member State of treatment and
- Union legislation on safety standards.

Whilst patient access to records is required by the PRD and must be made possible in all MS, such access is not necessarily to the electronic record and could entail a patient being given a print out of parts of the record.

3.2.11 Traceability

Issue:	**Issue code:**	**Primary legal reference:**
Traceability	L-LI-01	FWA
Process	**Process step**	
Health care encounter	Health professional requests access and receives Patient Summary/e-prescription/ medication record from abroad according to professional role	

Description:

All transactions shall be logged and an audit trail created and stored for audit and litigation purposes. A patient should also have the right to see the log and know who used or saw his medical data. Traceability of orally transmitted information e.g. in the case of 112 use case will be also a challenge to be explored.

3.2.12 Updating of patient records

Issue:	**Issue code:**	**Primary legal reference:**
Updating of patient records	L-HS-06	Art. 4 para. 2 lit. f PRD
Process	**Process step**	
Health care encounter and information returned to NCP A	Health professional requests access and receives Patient Summary/e-prescription/medication record from abroad according to professional role. New data created in country B is transmitted to country A for updating purposes.	

Description:
In order to ensure continuity of care, patients who have received treatment (in country B) are entitled to a (written or) electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC. The operational framework necessary for MS of affiliation (country A) to receive electronic data sent by MS of treatment (country B) for the purposes of updating information available to health professionals in country A does not exist. The existence of an operational process in country A is a prerequisite. The relevant service specification must take into account national operational approaches for updating of patient summaries.

3.2.13 Patient safety

Issue:	**Issue code:**	**Primary legal reference:**
Patient safety	L-LI-02, L-LI-03	Medical Device Directive[7]
Process	**Process step**	
Healthcare encounter	Health professional receives semantically mapped epSOS	

[7] For more detailed information cf. chapter 4.5 Medical Device Directive (MDD), p. 43.

and Patient Summary is updated in country A	document. Patient accesses own health data and requests semantically mapped presentation.	

Description:

This issue is about the liability for patient safety against the backdrop of the Medical Device Directive (MDD). However it must be further elaborated whether software in epSOS is a medical device in the terms of the Medical Device Directive or not. However the issue is considered relevant in relation to subsequent running beyond the pilot phase.

This process of semantic mapping is cross cutting of the processes of both nations involved in the data exchange. Liability is therefore shared for the central services and the risk can be only managed if MTC (Master Translation Catalogue) related processes are standardized according to epSOS standards and implementation is audited.

Liability is also related to clinical decisions support by information in medical records. When data is returned to country A, basing clinical decisions on such data also becomes a (shared) liability issue. When country A incorporates newly, in country B created information into the records, it assumes liability for quality of data.

epSOS shall elaborate commonly accepted and auditable processes for production of the MTCs.

Quality of data in medical records is a major issue and almost too large of a challenge for epSOS.

L-LI-03: epSOS shall deal with clinical governance issues to the appropriate depth as far as issues of quality of data (data coding) is concerned.

3.2.14 Interoperability of ePrescriptions

Issue:	**Issue code:**	**Primary legal reference:**
Interoperability of ePrescriptions	L-HS-07	Art. 11 PRD
Process	**Process step**	
Healthcare encounter and Patient Summary is updated in country A	health professional creates new/updates clinical or e-prescription or dispensation record stored in the country of treatment	

Description:

If a medicinal product is authorized to be marketed on their territory, Member States shall ensure that prescriptions issued for such a product in another Member State for a named patient can be dispensed on their territory in compliance with their national legislation in force.

In addition, a Member State of affiliation shall take all necessary measures in order to ensure continuity of treatment in cases where a prescription is issued in the Member State of treatment for medicinal products or medical devices available in the Member State of affiliation and where dispensing is sought in the Member State of affiliation.

The recognition of such prescriptions shall not affect national rules governing prescribing and

dispensing. The EC shall adopt guidelines on the interoperability of prescriptions. MTC

3.2.15 Proportionality and purpose limitation

Issue:	**Issue code:**	**Primary legal reference:**
Proportionality and purpose limitation	L-DP-07	Art. 6 para. 1 lit. e DPD
Process	**Process step**	
New health record/order created and stored and Patient summary is updated in country A	Health professional creates new/updates clinical or dispensation record in country of treatment Patient summary is updated	
Description:		
The processing of personal data must be strictly limited to the minimum which is necessary for the fulfilment of the epSOS purposes. Each query about the personal data available through epSOS should be based on a real need of access to the specific information and no personal data returned by country B shall be stored at the NCP.		

3.3 Summary of legal requirements

The table below summarizes the list of legal requirements:

TABLE 2: Summary of requirements emerging from the legal analysis of the epSOS extension			
Chapter	**Issue**	**Identifier**	**Requirement**
3.1.1	Transmission of data to third countries	L-DP-01	A standard form contract which incorporates the necessary elements of the FWA, the required SCC as well as the specific clauses pertinent to the bilateral relationship, to be signed bilaterally by each PN piloting with Turkey, shall be drafted.
3.2.1	The epSOS NCP within the Patients' Rights Directive	L-HS-01	Against the backdrop of the efficiency requirement (Art. 12/2/d PRD) an analysis of the duties of the epSOS NCP in the framework of the PRD including opportunities to co-locate the PRD and epSOS functions must be performed.
3.2.2	International epSOS agreements	L-HS-02	Member States shall facilitate cooperation in cross-border healthcare provision at regional and local level as well as through ICT and other forms of cross-border cooperation. The Commission shall encourage Member States, particularly

			neighbouring countries, to conclude agreements among themselves.
3.2.3.	Electronic cross border access to medical information	L-HS-03	The epSOS PS shall be aligned/influence the development of guidelines on a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders.
3.2.4.	Patient Information Notice	L-DP-02	The Patient Information Notice must be sufficient to enable the patient to give explicit consent to the processing of data in accordance with the requirements of DPD and PRD.
3.2.5.	Security	L-DP-03	epSOS agreements on appropriate security measures (such as for protection of personal data, integrity and authorship of documents, access control and role mandate management) mutually accepted by all involved Participating Nations must be secured and codes of conduct as part of the epSOS Information Governance must be elaborated .
3.2.6.	Informed Choice	L-HS-04	epSOS healthcare providers shall notify on availability of epSOS services and report on performance data and shall provide clear information on use of epSOS for patients.
3.2.7.	Common identification and authentication measures	L-DP-04	epSOS shall consider the opportunity to migrate to the common eID EU approach foreseen in Article 14 of the PRD.
3.2.8.	Authorization	L-DP-05	epSOS shall consider the opportunity to incorporate provisions for authorization of health professionals in compliance to the PRD.
3.2.9.	Patient Consent	L-DP-06	Purpose and manner of the data processing need to be covered by the patient's consent in PAC and 112.
3.2.10.	Right to acess to health information	L-HS-05	Whilst patient access to records is required by the PRD and must be made possible in all PNs, such access is not necessarily to the electronic record and could entail a patient being given a print out of parts of the record.
3.2.11.	Traceability	L-LI-01	All transactions shall be logged and an audit trail created and stored. A patient should also have the right to see the log and know who used or saw his medical data.
3.2.12.	Updating of patient records	L-HS-06	The relevant service specification must take into account national operational approaches for updating of patient summaries.
3.2.13	Patient Safety	L-LI-02	epSOS shall elaborate commonly accepted and auditable processes for production of the MTCs.
		L-LI-03	epSOS shall deal with clinical governance issues to the appropriate depth as far as issues of

			quality of data (data coding) is concerned.
3.2.14	Interoperability of ePrescriptions	L-HS-07	epSOS shall adhere to/influence the development of guidelines foreseen under Art. 14 PRD supporting the Member States.
3.2.15	Proportionality and purpose limitation	L-DP-07	Each query about the personal data available through epSOS should be based on a real need of access to the specific information and no personal data returned by country B shall be stored at the NCP.

4 epSOS II legal foundations

4.1 Transmission of health data to third countries

4.1.1 Applicable law (Art. 4 DPD)

In the area of data protection Art. 4 is deemed a lex specialis with regard to the "general" conflict of laws rules. According to Art. 4 DPD a Member State's national law is to be applied, if:

1. the processing is carried out by a national establishment[8] of the (foreign) data controller (Art. 4 para. 1 lit. a DPD) or
2. the data controller is established outside the Member State's territory, but in a place where its national law applies by virtue of international public law (Art. 4 para. 1 lit. b DPD) or
3. the data controller is situated outside the EU and makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community (Art. 4 para. 1 lit. c DPD).

Art. 4 DPD can for example be relevant in cases of foreign hospital owners, which is for example a familiar situation to Czech Republic. From the Patients' Rights Directive (PRD) point of view the legal person operating concrete establishments in Czech Republic would have to apply Czech Data Protection law regardless of the operators legal residence or establishment

By the second case of Art. 4 (Art. 4 para. 1 lit. b) exterritorial areas, as for example embassies, consulates, ships or airplanes shall be included within the scope of national law. Missions and international organizations are subject to Art. 4 para. 1 lit. a[9].

Art. 4 para. 1 lit. c is relevant for non-EEA countries, as for example Turkey. This provision is only to be applied if the controller does not have any establishment within EEA[10]. Crucial for interpretation is the term "equipment" that should be read in the sense of "mean" [11]. In the scope of Art. 4 para. 1 lit. c DPD data controllers have to designate representatives in the territory of the EEA country, where the equipment is used (Art. 4 para. 2 DPD).

4.1.2 General issues on the transmission of data to third countries

Third countries are all non-EEA states, as for example Albania, Croatia, Macedonia, Serbia, Switzerland or Turkey. Norway, Iceland and Liechtenstein – being EFTA and thus EEA member states – adopted the DPD by Decision of the EEA Joint Committee[12].

The general rule for EU-internal exchange of data is laid down in Art. 1 DPD, stipulating that "*Member States shall neither restrict nor prohibit the free flow of personal data between Member*

---

[8] *Art-29 Group*, WP 179, p. 11 defines establishment as follows:
"*It is furthermore important to emphasise that an establishment need not have a legal personality, and also that the notion of establishment has flexible connections with the notion of control. A controller can have several establishments, joint controllers can concentrate activities within one establishment or different establishments. The decisive element to qualify an establishment under the Directive is the effective and real exercise of activities in the context of which personal data are processed*".

[9] *Art-29 Group*, WP 179, p. 18.

[10] *Art-29 Group*, WP 179, p. 19.

[11] *Art-29 Group*, WP 179, p. 20.

[12] Decision of the EEA Joint Committee, No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:296:0041:0043:EN:PDF (last visisted: Nov. 16, 2011).

States for reasons connected with the protection" of data. As a consequence transmission of data cannot be interdicted with reference to national data protection legislation!

The general rule for transmission of data to third countries – that transmission is not allowed – is not explicitly laid down in the European data protection legal framework, but may be derived from the structure of Chapter IV DPD, dealing with "Transfer of personal data to third countries" (Art. 25 et sq). Under the terms of Chapter IV DPD the following legal foundations are exceptions from this general rule and can be used to legitimate transmission of data to third countries:

- adequate protection of data acknowledged by EU Decision (Art. 25 DPD) or
- consent of data subject (Art. 26 para. 1 lit. a DPD) or
- necessity for performance of contract (Art. 26 para. 1 lit. b & c DPD) or
- important public interest grounds (Art. 26 para. 1 lit. d DPD) or
- defence of claims (Art. 26 para. 1 lit. d DPD) or
- vital interests of the data subject (Art. 26 para. 1 lit. e DPD) or
- necessity for public registers (Art. 26 para. 1 lit. f DPD) or
- use of standard contractual clauses (Art. 26 para. 2 DPD).

The acknowledged adequate level of data protection (Art. 25 DPD) and the use of standard contractual clauses (SCC – Art. 26 para. 2 DPD) appear the most relevant approaches in practice, as they are easy to use, do not require complex legal argumentation and provide a good amount of legal certainty.

Third countries have to be aware that according to Art. 4 para. 1 lit. c DPD the data protection law to be applied to epSOS operations is the law of the Member State, exporting or importing data. The data transfer among third countries, without any EU Member State participating, is not governed by Union law, but subject to the respective international law provisions of the involved third countries. The transfer of personal data from Switzerland to Turkey for example would not be subject to the DPD, as – according to the current understanding of epSOS use cases – "equipment is used only for purposes of transit through the territory of the Community" (Art. 4 para. 1 lit. c DPD). Therefore such a transfer of personal data follows the bi- or multilateral rules among the concerned Participating Nations.

In case of misuse of personal data by a third country healthcare provider it is a matter of fact, that – especially in cases of an absent enforcement agreement – legal protection may easily be levered out, simply by ignoring contractual provisions and judgements. This risk could be minimized by the third country healthcare provider's duty to immediately delete the data after treatment. On the other hand such an obligation would – in case of medical maltreatment due to wrong data for example – perhaps hamper the epSOS patient in demonstrating the maltreatment.

4.1.3 Adequate level of data protection as legal ground for third country data transfers

The European Commission issued several Decisions about countries, projects and situations, deemed to satisfy the European data protection requirements as laid down in both data protection directives. An updated list of those decisions may be found online at the EC DG Justice, Department Data Protection[13]. As of April 2011 the following countries, projects and situations are regarded to provide an adequate level of data protection:

- Israel: Decision 2011/61/EU of January 31, 2011,
- Andorra: Decision 2010/625/EU of October 19, 2010,
- Faroe Islands: Decision 2010/146/EU of March 5, 2010,

[13] *EC DG Justice*, Commission decisions on the adequacy of the protection of personal data in third countries, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (last visited Nov. 16th, 2011).

- Jersey: Decision 2008/393/EC of May 8, 2008,
- Isle of Man: Decision 2004/411/EC of April 28, 2004,
- Guernsey: Decision 2003/821/EC of November 21, 2003,
- Argentina: Decision 2003/490/EC of June 30, 2003,
- Canada: EC Decision 2002/2/EC of December 20, 2001,
- USA (Safe Harbour[14]): EC Decision 2000/520/EC of July 26, 2000 as well as
- Switzerland: EC Decision 2000/518/EC of July 26, 2000.

Not relevant for epSOS, because only referring to Passenger Name Records (PNR) are for example the following decisions:

- Canada Border Services Agency (PNR): EC Decision 2006/253/EC of September 6, 2005 and
- US Bureau of Customs and Border Protection (PNR): EC Decision 2004/535/EC of May 14, 2004.

Those decisions do not completely equate the cited countries, projects or situations, meaning that the European data protection framework – as for example Art. 1 para. 2 DPD – is to be unrestrictedly applied, but attest them to comply with Art. 25 DPD. Usually those EC Decisions include provisions allowing the competent authorities in Member States to suspend data flows to recipients resided in the country or being part of the projects or situations subject of the respective EC Decision, in case a national authority – of the country, not the Member State, concerned – has determined a breach of the data protection standards or an infringement of those standards is very likely to occur.

4.1.4 Standard contractual clauses (SCC) as legal ground for third country data transfers

In order to facilitate data flows from the Community, it is desirable for data controllers to be able to perform data transfers globally under a single set of data protection rules. In the absence of global data protection standards, standard contractual clauses provide an important tool allowing the transfer of personal data from all Member States under a common set of rules.[15] According to Art. 26 DPD another way to legally transfer personal data to third countries is the usage of such Standard Contractual Clauses (SCC), also called model contracts, as published by decisions of the European Commission. Decisions based upon Art. 26 para. 2 DPD allow Member States to recognize data importers in third countries using such Standard Contractual Clauses as data importers who offer an "adequate level of data protection". Those model contracts are as well online, ready for download at the DG Justice, Department Data Protection website[16]. Basically there are two approaches:

1. Two sets of clauses are designed for personal data transfer between data controllers “controller-to-controller transfer”[17].

[14] Safe Harbor refers to a framework of national and international contracts, providing for a distinct level of data protection (cf. http://export.gov/safeharbor/eu/eg_main_018365.asp, last visited: Nov. 11th 2011, for more detailed information). An updated list of the currrent Safe Harober companies can be retrieved at http://safeharbor.export.gov/list.aspx (last visited: Nov. 11th, 2011).

[15] Recital 1 EC Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004, p. 74.

[16] EC DG Justice, Model Contracts for the transfer of personal data to third countries, http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm (last visited: Oct. 20th, 2011).

[17] EC Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4.7.2001, p. 19, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:EN:PDF (last visited: Nov. 7th, 2011) and Commission Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385,

2. One set of clauses set up for personal data transfer between data controllers and data processors[18]. These clauses are to be used only for transfer of personal data to "data processors" (but not between "data controllers"). One of the main innovations is that this set of clauses contains also legal regime for data transfer from "processor" to "sub-processor" (clause 11).

Both EC Decisions defining the model contracts share more or less the same structure:

1. Recitals,
2. General Provisions on
    a. aim,
    b. scope,
    c. defined terms and
    d. the Member States' authorities' power to restrict or totally prohibit data flows if necessary for data protection reasons and
3. Annex, holding
    a. the general provisions of the model contract and
    b. appendixes to the model contract, describing the data transfer and the applied data security measures in more detail.

The data controller approach is based upon EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC. Actually there are two model contracts on the transfer of personal data to data controllers in third countries described. The second set of model contracts, inserted by EC Decision 2004/915/EC, provides more "*flexible auditing requirements and more detailed rules on the right of access*" as well as a "*liability regime based on due diligence obligations*" of both the data exporter and the data importer.[19]

The competent national authorities may unilaterally prohibit or suspend ongoing data transfers, in case

- the data importer refuses to cooperate in good faith with the data protection authorities, or to comply with his clear obligations under the contract (Art. 4 para. 2 lit. a EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC) or
- the data exporter refuses to take appropriate steps to enforce the contract against the data importer within one month (Art. 4 para. 2 lit. b EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC).

The data processor approach is based upon EC Decision 2010/87/EU, repealing EC Decision 2002/16/EC. The new Decision applies "*to the transfer of personal data by controllers established in the European Union to recipients established outside the territory of the European Union who act only as processors*" (Art. 2 D 2010/87/EU)[20]. It does not apply to subcontracting by a processor established in the EU to a sub processor established outside the EU[21], but allows for data transfers from an EU data controller to third country processors and their resp. sub-processors.

29.12.2004, p. 74, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF (last visited: Nov. 7th 2011).

[18] EC Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, OJ L 39, 12.2.2010, p. 5, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF (last visited: Nov. 6th 2011).

[19] Recitals 4 and 5 EC Decision 2004/915/EC.

[20] The underlying idea was to provide an updated legal basis for out-sourcing data processing outside the EU.

[21] Recital 23 EC Decision 2010/87/EU, OJ L 39, 12.2.2010, p. 7.

As there is no doubt that the healthcare providers are regarded data controllers, only the data controller approach can be applied for the purposes of epSOS.

4.1.5 Consent as legal ground for third country data transfers

According to Art. 26 para. 1 lit. a DPD also the data subject's consent can be used as legal foundation to transfer personal data between EU/EEA Member States and third countries.

The advantage of such an approach is the comparably easy implementation within epSOS, that could be accomplished by amending the consent declarations of the epSOS patients. A major drawback would be the lack of contractual control as provided for example by Art. 5 of the above cited model contract ("obligations of data importer").

4.1.6 Considerations on the implementation of third country data transfer in epSOS

With regard to those countries that have been attested an adequate level of data protection, the legal approach – from the data protection point of view – may be the same as for EU Member States. Switzerland for example could implement the Framework Agreement the same way as the others EU Member States do respectively did.

With regard to countries that do not provide for an adequate level of data protection, additional legal safeguards are required. The EC model contracts – also known as standard contractual clauses (SCC) – are to be concluded between the data exporter and the data importer. Both "*are free to include any other clauses on business related issues which they consider as being pertinent for the contract as long as they do not contradict the standard contractual clauses*"[22].

The practical considerations on how to implement the model contracts between which parties, bring us back to the original epSOS I discussion, whether epSOS National Contact Points are data controllers or data processors[23]. Even though this question now – in epSOS II – needs to be answered consistently among the epSOS Participating Nations[24], there are two ways to tackle this model contract implementation issue:

- the epSOS National Contact Points located in the third countries are regarded data controllers[25] (i.e. data importers for the purpose of EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC), meaning that all epSOS National Contact Points have to enter into model contracts according to cited EC Decision or
- each healthcare provider (HCP) of the third country is regarded a data controller (i.e. data importer for the purpose of EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC). This approach would require contractual relations at least between each epSOS National Contact Point located within EU/EEA and each third country healthcare provider and is for practical reasons obviously not the right choice.

Problems because of the unmanageable number of contracts to conclude, could be evaded by splitting the model contracts into two separate, but correlating unilateral declarations, which could be signed independently. The execution of those declarations would be a conditio sine qua non for the active participation of third countries in epSOS.

---

[22] Recital 4 EC Decision 2010/87/EU, OJ L 39, 12.2.2010, p. 5.

[23] *WP21*, Liability in epSOS, p. 9.

[24] The necessity of a coordinated/uniform approach results from the practical need, not to mingle both model contracts.

[25] This means they have to be designated as such, e.g. in the FWA.

It is important to note that these standard contractual clauses do not allow for transfers of personal data on a "processor-to-processor" basis. The EU/EEA participant of the data transfer needs to be a "controller". That implies such clauses can only be signed by epSOS National Contact Points that are considered to be "data controllers", as this is the case for example in Norway and Greece. In other countries, as for example Austria, Czech Republic, Italy and Spain this clauses could only be signed by the healthcare providers, which must been seen as serious practical obstacle to this solution.

4.1.7 Addressing different security levels in epSOS

Different levels of data security measures – as being national legislation – must not impose an obstacle to EU-intern exchange of data (Art. 1 para. 2 DPD). International projects, as for example epSOS, may resolve such problems by agreeing on mutual data security standards. In case such if a mutual consent is not achievable, legal action may be taken, as for example infringement proceedings (Art. 258 TFEU[26]) or proceedings for a preliminary ruling (Art. 267 TFEU), as national provisions obviously violate EU legislation.

With regard to the question which Member States data security measures shall be applied the relevant Opinion of the Art 29 Working Party may be cited:

"*Article 17(3) establishes that the contract or the legal act binding the processor to the controller should also ensure compliance with the security measures 'defined by the law of the Member State in which the processor is established'.*

The reason behind this principle is to ensure uniform requirements within one Member State with regard to security measures, and facilitate enforcement. It should be noted however that in a European perspective, security requirements diverge considerably depending on Member States: some provide for very detailed rules while others have just copied the general wording of the Directive. Where national laws are general and their wording is taken from the Directive, this will not have any practical consequences. It would not be a problem for a processor to comply with more detailed obligations imposed on him by the controller according to its national law, or alternatively for a controller to accept more detailed requirements according to the law of the processor.

Only in cases where detailed rules are different or even in conflict, Article 17(3) decides in favour of the law of the processor[33]. However, it seems advisable that further harmonization of security obligations should be included in the scope of discussion on the revision of the data protection framework."[27]

4.1.8 Conclusion

According to the Data Protection Directive there are a number of possible legal foundations for transferring personal data between EU/EEA Member States and third countries. Three of them appear to be appropriate for epSOS, having different advantages and disadvantages. They are:

	pros	**cons**
Adequate level of data protection (Art. 25 DPD)	– easy to implement in epSOS – "like a Member State" – good level of data protection for epSOS	– not universally applicable to all third countries

[26] Treaty on the functioning of the European Union.

[27] *Art-29 Group*, WP 179, p. 25.

	patients	
Consent of data subject (Art. 26/1/a DPD)	– robust approach, as already experienced in epSOS	– epSOS patient is left alone responsible – not the optimum level of data protection – it could be difficult to retrieve the information needed for informed consent
Standard Contractual Clauses (Art. 26/2 DPD)	– good level of data protection for epSOS patients	– probably complex implementation – epSOS NCPs should be data controllers – the extent to which the SCC may be adapted can be very narrow

It is important to note, that the Standard Contractual Clauses acc. to Art. 26 para. 2 DPD are international private law contracts, not to be confused with International Treaties or Executive Agreements, that both aim to legally bind subjects of international law, as for example states, but not private law subjects, as for example patients, healthcare providers or companies.

4.2 Liability

Liability in epSOS has been thoroughly examined within the WP2.1 document "Liability in epSOS"[28]. The fundamental principles of tort law are to be found at national level. Therefore a comprehensive analysis would require careful consideration of national provisions. As far as possible emerging case studies will be included within the cited document.

The epSOS consortium cannot be regarded a legal entity and therefore cannot play an active role in liability issues. The conflict of laws rules, as briefly described below in chapter 4.4, Conflict of laws, p. 39 apply and determine the conditions for potential law suits.

4.3 Directive on the application of patients' rights in cross-border healthcare (PRD)

In March 2011 the Directive 2011/24/EU[29] on the application of patients' rights in cross-border healthcare (Patients' Rights Directive – PRD) was adopted, with the main goals to foster:

- patients' mobility (rec. 5) – although "its application should not result in patients being encouraged to receive treatment outside their Member State of affiliation" (rec. 4),
- legal certainty (rec. 9) and
- cooperation on healthcare between Member States (rec. 10)

to facilitate the access to safe and high-quality cross-border healthcare (Art. 1 para. 1 PRD).

[28] https://service.projectplace.com/pp/pp.cgi/d666303870/Liability in epSOS_final.pdf;version=0.1?save_as=1 (last visited: Nov. 16th, 2011).

[29] Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF (last visited: Oct. 20th, 2011).

As per today the Patients' Rights Directive is not part of the EEA law, but shall be incorporated[30]. Norway intends to implement the Patients' Rights Directive together with the other EU Member States by Oct 2013.

The legal base for implementing the directive is the EEA-Agreement[31] Art. 36.

4.3.1 Scope of the PRD

The directive is characterized by strong references to national legislation, in particular the transposition of the EU data protection law and applies also to EEA countries. The PRD shall apply to the provision of healthcare to patients, regardless of how it is organized, delivered and financed. That means that the responsibilities for the management of health services and medical care as well as allocation of resources assigned to them shall remain with the Member States (Art. 168 para. 7 TFEU).

The PRD applies to individual patients who decide to seek healthcare in a Member State other than the Member State of affiliation (Art. 1 para. 2 PRD). It does not apply to:

- services in the field of long-term care (Art. 1 para. 3 lit. a PRD),
- allocation of and access to organs for the purpose of organ transplants (Art. 1 para. 3 lit. b PRD) and
- public vaccination programmes against infectious diseases (Art. 1 para. 3 lit. c PRD).

4.3.2 Responsibilities of the Member State of treatment/country B (Art. 4 PRD)

The rules to be applied on treatment are the law of country where treatment is delivered (country B in epSOS terms) and the Union legislation on safety standards (Art. 4 para. 1 PRD). The National Contact Point for the PRD – not to be confused with the epSOS National Contact Points – shall according to Art. 6 PRD inform patients on the national standards and guidelines to be applied regarding quality and safety (Art. 4 para. 2 lit. a and b PRD). Furthermore the Member State of treatment shall be responsible for:

- access of patients, that received healthcare treatment within their territory, to at least a copy of the medical record (Art. 4 para. 2 lit. f PRD),
- clear information on prices (Art. 4 para. 2 lit. b PRD),
- transparent complaints procedures (Art. 4 para. 2 lit. c PRD),
- a system of professional liability insurance (Art. 4 para. 2 lit. d PRD),
- adherence to data protection rules and non-discrimination (Art. 4 para. 2 lit. e and Art. 4 para. 3 PRD) as well as
- non-discrimination with regard to financial aspects, as for example same fees for domestic and foreign patients (Art. 4 para. 4 PRD).

4.3.3 Responsibilities of the Member State of affiliation/country A (Art. 5 PRD)

The responsibilities of country of affiliation (country A in epSOS terms) include:

- reimbursement of costs (Art. 5 lit. a and Chapter III [Art. 7 – 9] PRD)

---

[30] Cf. Liechtenstein Chair Work Programme EFTA Standing Committee – Second Half of 2011, http://www.efta.int/~/media/Documents/eea/eea-institutions/2011-06-30-liechteinstein-chair-work-programme-2nd-half-2011.pdf (last visited: Nov. 16th, 2011).

[31] Agreement on the European Economic Area, OJ L 1, 3.1.1994, p. 3, http://www.efta.int/~/media/Documents/legal-texts/eea/the-eea-agreement/Main Text of the Agreement/EEAagreement.pdf (last visited: Nov. 6th, 2011).

- information of patients on cross-border health care, in which clear distinction shall be made between information about this directive and Regulation (EC) 883/2004 (Art. 5 lit. b PRD)
- grant same medical follow-up as in country B (Art. 5 lit. c PRD)
- remote access to or at least a copy of their medical records (Art. 5 lit. d PRD)

4.3.4 Right of the patients to access their medical information

The highly relevant and important provisions of the PRD regarding the patients' right to access their medical information are Art. 4 para. 2 lit. f and Art. 5 lit. d PRD, which read as follows:

"*(f) in order to ensure continuity of care, patients who have received treatment [ann.: in country B] are entitled to a written or electronic medical record of such treatment, and access to at least a copy of this record in conformity with and subject to national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.*"

"*(d) patients who seek to receive or do receive cross-border healthcare have remote access to or have at least a copy of their medical records, in conformity with, and subject to, national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.*"

According to those provisions the following must be guaranteed by the EU/EEA Member States

Access rights according to PRD	Medical records in country A	Medical records in country B
Patient is in country A	(required according to DPD)	Art. 4 para. 2 lit. f PRD
Patient is in country B	Art. 5 lit. d PRD	Art. 4 para. 2 lit. f PRD

It is unclear whether "medical record" refers only to the Patient Summary, or also to medication related data. For the purposes of epSOS the term "medical record" shall be read as referring to both.

4.3.5 National Contact Points (Art. 6 PRD)

The PRD National Contact Points are not to be confused with the epSOS National Contact Points, as they are points responsible primarily for providing information to patients on availability, content and costs of health services. Nonetheless their relevance to epSOS should however be considered by WP1.3. Dissemination and with regard to national, organizational aspects, i.e. the question, whether both functions can be operated by them same institution. From the European law point of view there cannot drawn any legal restriction, that would interdict such an organizational combination.

The general information they shall facilitate to exchange (Art. 6 para. 3 PRD) shall inter alia refer to:

- healthcare providers and their right to provide services,
- patients' rights,
- complaint procedures & mechanisms for seeking remedies as well as
- cross-border healthcare in general.

4.3.6 Mutual recognition of prescriptions (Art. 11 PRD)

An important provision for epSOS is Art. 11 PRD on the recognition of prescriptions issued in another Member State, as medicinal products (Art. 1 no. 2 Medicinal Products Directive [MPD][32]) authorized

[32] Directive 2001/83/EC on the Community code relating to medicinal products for human use, OJ L 311, 28.11.2001, p. 67, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2001L0083:20070126:en:PDF (last visited: Nov. 17th, 2011).

to be marketed within the EU shall in general be dispensed without restrictions within the EU. There are only a few valid reasons allowing to refrain from dispensation.

Special prescriptions (Art. 71 para. 2 MPD), which are prescriptions concerning substances

- classified as narcotics or psychotropic substances or
- bearing the risk of (medicinal) abuse or
- that – due to their novelty – can be considered harmful

are not covered by Art. 11 PRD.

According to Art. 11 para. 2 PRD the Commission shall promote EU prescriptions, by:

- supporting verification of prescriptions' authenticity (Art. 11 para. 2 lit. a PRD),
- guidelines on interoperability (Art. 11 para. 2 lit. b PRD),
- facilitating correct, international non-proprietary identification of medicinal products (Art. 11 para. 2 lit. c PRD) as well as
- facilitating comprehensibility of patients' information (Art. 11 para. 2 lit. d PRD).

4.3.7 Enhanced cooperation across Europe (Art. 10 et sqq. PRD)

The provisions on enhanced cooperation within the EU includes cooperation regarding actively provided cross-border healthcare (Art. 10) as well as policy making (Art. 12 et sqq.).

4.3.7.1 Cooperation regarding actively provided cross-border healthcare (Art. 10 PRD)

According to Art. 10 PRD the Member States shall guarantee:

- the cooperation on standards and guidelines on quality and safety and the exchange of information (Art. 10 para. 1 PRD),
- the cooperation at local & regional level (Art. 10 para. 2 PRD),
- the conclusion of agreements between neighbouring countries (Art. 10 para. 3 PRD) as well as
- the exchange of information about healthcare providers among Member States via the Internal Market Information System (IMI)[33] (Art. 10 para. 4 PRD).

4.3.7.2 Cooperation regarding actively provided cross-border healthcare (Art. 12 – 14 PRD)

According to Art. 12 para. 1 PRD the Commission shall support Member States in the development of European reference networks between healthcare providers and centres of expertise in the Member States, in particular in the area of rare diseases. These voluntary **networks acc. to Art. 12 PRD** shall inter alia:

- support an innovation driven European cooperation regarding highly specialized healthcare,
- maximize the cost-effective use of resources by concentrating them where appropriate or
- facilitate mobility of expertise, virtually or physically, and to develop, share and spread information, knowledge and best practice.

Furthermore the Commission shall subject to Art. 13 PRD support the Member States in the field of rare diseases, by raising awareness

[33] IMI is an online tool, established and maintained by the European Commission to support the crossborder cooperation among national authorities. IMI helps to find the right contact persons and eases communication via online based translation. Currently IMI is used for the purposes of the Professional Qualifications Directive (D 2005/36/EC), the Services Directive (D 2006/123/EC) and the PRD.

- among health professionals of rare diseases' tools, as for example Orphanet (Art. 13 lit. a PRD) and
- among patients, health professionals and insurers of the possibilities offered by Social Security Systems Regulation (SSS Reg)[34] for referral of patients with rare diseases to other Member States even for diagnosis and treatments.

The voluntary eHealth network among the responsible national authorities (Art. 14 PRD) shall take over the trend-setting tasks of

- working towards delivering sustainable economic and social benefits of European eHealth systems (Art. 14 para. 2 lit. a PRD),
- drawing up guidelines on
  - a non-exhaustive list of data for a patient summary and
  - the use of medical information for public health and research (Art. 14 para. 2 lit. b PRD) and
- supporting Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare (Art. 14 para. 2 lit. c PRD).

4.3.8 Reimbursement of cross-border healthcare and EESSI (Art. 7 – 9 PRD)

Chapter III (Art. 7 – 9) of the PRD refers to the reimbursement of cross-border healthcare, that is on European level primarily governed by the Social Security Systems Regulation (SSS Reg), as amended by Regulation (EC) 988/2009[35] and implemented by Regulation (EC) 987/2009[36]. These legal documents encompass the key provisions on the co-ordination of social security systems at European level and are relevant for EEA as well as Switzerland.

The Regulation (EC) 987/2009 breathes life into the highly abstract provisions of the Social Security Systems Regulation, mainly by regulating the concrete ways of cooperation, i.e. exchange of data, liability, etc. The exchange between the Member States' authorities and institutions "*shall be based on the principles of public service, efficiency, active assistance, rapid delivery and accessibility, including e-accessibility*" (Art. 2 para. 1 Reg (EC) 987/2009). The institutions shall without delay provide or exchange all data necessary for establishing and determining the rights and obligations of persons to whom Reg (EC) 883/2004 applies. Such data shall be transferred between Member States directly by the institutions themselves or indirectly via the liaison bodies (Art. 2 para. 2 Reg (EC) 987/2009). As such data ("*necessary for establishing and determining the rights and obligations*") comprises health data and Art. 2 para. 1 leg. cit. Reg (EC) 987/2009 demands efficiency of the exchange, a liaison with epSOS has at least to be considered. A combination of both approaches could also reduce complexity for healthcare providers, by removing redundancies.

Contrary to the PRD, Reg (EC) 987/2009 does not refer to the "*national measures implementing Union provisions on the protection of personal data*" but directly to the "*Community provisions on the*

[34] Regulation (EC) No. 883/2004 on the coordination of social security systems, OJ L 166, 30.4.2004, p. 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:166:0001:0123:EN:PDF (last visited: Nov. 18th, 2011).

[35] Regulation (EC) No. 988/2009 amending Regulation (EC) No. 883/2004 on the coordination of social security systems, and determining the content of its Annexes, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0988:EN:NOT (last visited: Nov. 16th, 2011).

[36] Regulation (EC) No. 987/2009 laying down the procedure for implementing Regulation (EC) No. 883/2004 on the coordination of social security systems, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009R0987:EN:NOT (last visited Nov. 12th, 2011).

protection of individuals with regard to the processing of personal data and the free movement of such data" (Art. 3 para. 3 Reg (EC) 987/2009).

4.3.9 Conclusion

First steps towards a European framework for interoperable eHealth services are taken primarily under Art. 14 PRD on eHealth and the establishment of the voluntary network including action for common eID and authentification measures as well as the elaboration of guidelines on

- a non-exhaustive list of data for a patient summary and
- the use of medical information for public health and research.

Liaisons between epSOS NCPs and NCPs according to Art. 6 PRD as well as EESSI and epSOS in general, with regard to shared infrastructure and common standards may for the sake of harmonization and efficiency be examined and to the fullest extent possible realized (Art. 12 para. 2 lit. d PRD).

4.4 Conflict of laws

International legal disputes primarily raise the following three questions:

1. Where is the place of jurisdiction? (jurisdiction)
2. Which law is to be applied? (choice of law)
3. How and where can judgements be enforced? (foreign judgements)

The law dealing with those questions is referred to as conflict of laws, international private law or private international law. Its regulations can either be national (laws, ordinances, decisions, …) or international (treaties, EU regulations, decisions, …). Depending on how the decision in a legal dispute is made and by whom, one may distinguish **litigation**, as the default (state) dispute resolution, and **arbitration**, as an alternative (private) dispute resolution.

4.4.1 Jurisdiction

Among the EU and EFTA[37] member states the so-called "**Brussels Regime**" applies. It consists of three international legal acts:

- Brussels Convention[38],
- Lugano Convention[39] and
- Brussels I regulation[40].

The differences between these three documents are marginal – the Brussels Convention was the first to be agreed in 1968, the Lugano Convention twenty years later to allow for the integration of the

[37] The European Free Trade Association (EFTA) is currently made up of Iceland, Liechtenstein, Norway and Switzerland.

[38] Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, http://curia.europa.eu/common/recdoc/convention/en/c-textes/brux-idx.htm (last visited: Nov. 16th, 2011).

[39] Convention of 16 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters, http://curia.europa.eu/common/recdoc/convention/en/c-textes/lug-idx.htm (last visisted: Nov. 16th, 2011).

[40] Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16.1.2001, p. 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0044:EN:html (last visited: Nov. 16th, 2011).

EFTA member states and last but most important the Brussels I regulation, supplanting more or less the Brussels Convention. Due to its EFTA relevance and in contrast to the Brussels Convention, the **Lugano Convention** is still crucial in cases relating to EFTA states, as for example Norway in the context of epSOS.

4.4.2 Choice of law

4.4.2.1 EU Member States

The choice of law is governed within the European Union by the Rome I and II regulations (see below chapters 4.4.5, Rome I Regulation (Rome I), p. 42 and 4.4.6, Rome II Regulation (Rome II), p. 43). Denmark is the only EU Member State not being bound by Rome II (Art. 1 para. 4 Rome II) thus having to apply its own (national) choice of law provisions. Nonetheless, due to the principle of universality (Art. 3 Rome II), the courts of EU Member States might have to apply Danish law.

4.4.2.2 Norway

Norway is neither bound by Rome I nor Rome II regulations. Hence, Norwegian courts will use Norwegian international private law to decide which law is to be applied. For some areas, Norway has implemented specific provisions relating to the choice of law through acts of the parliament. When no such specific provisions exist, the court will use the doctrine (developed through decisions by the Supreme Court) that the court will apply the law from the country to which the case has the **closest connection** to.

Regarding contractual obligations, specific provisions exist for some areas. Regarding non-contractual obligations, Norway is neither bound by the Rome II regulation nor is the choice of law regulated by Norwegian law. The Norwegian courts will therefore decide on the choice of law according to principles of Norwegian international private law, and will use the doctrine as mentioned above. Still, the Norwegian Supreme Court has stated that unless it has been decided otherwise by acts or secondary law, the solution from the EU-countries in relation to Rome II should be emphasized when deciding on the choice of law (RT-2009-1537).

4.4.2.3 Turkey

Both Rome Regulations are not to be applied by Turkish courts due to not being EU Member State. Applicable law to legal relationship with foreignness factor and related cases is regulated by the Law on International Private Law and Procedure Law, no. 5718 dated 12.12.2007.

For private law matters, EU has adopted special legislation for its members. Conventions dated 1968 were only open to participation of members of the European Union which were later on replaced by regulations which are kind of EU secondary legislation. Due to these explanations it is impossible for Turkey to join the mentioned EU conventions or to implement EU regulations. Therefore questions concerning “jurisdiction, applicable law and enforcement” of private law issues between Turkey and EU countries are solved according to bilateral or multilateral agreements which have been signed between Turkey and EU countries. One should examine the existence of an agreement in the mentioned fields and each case should be examined separately. The Council of Europe which Turkey is a member leads signature of agreements in the field of civil and private law matters. The list of agreements and position of Turkey can be found on the website of the Council of Europe[41].

4.4.3 Foreign judgements

The recognition and enforcement of foreign judgements in civil and commercial matters is regulated by several international agreements. Among them there are:

[41] See http://www.coe.int (last visited: Nov 6th, 2011).

- the Brussels Regime,
- the Hague Convention[42] with Albania, Cyprus, Kuwait, Portugal and the Netherlands as parties as well as
- the Agreement on the recognition and enforcement of judicial decisions and settlements in civil and commercial matters, UNTS no. 31488.

4.4.3.1 EU Member States

Recognition and enforcement of foreign judgments among EU Member States is subject to the Brussels I regulation, discussed in more detail below (chapter 4.4.4, Brussels I Regulation (Brussels I), p. 41).

4.4.3.2 Norway

Recognition and enforcement of foreign judgements in civil and commercial matters are regulated by the Lugano Convention, which is implemented in Norwegian law by being referred to in the *Act relating to mediation and procedure in civil disputes*, paras. 4 to 8, and is added as an annex to this legislation. Hence, regarding recognition and enforcement for foreign judgements, Norway is bound by the Lugano Convention which for most part contains the same rules as for EU Member States through the Brussels Regime.

4.4.3.3 Switzerland

The same holds true for Switzerland, which is also party to the Lugano Convention.

4.4.3.4 Turkey

Recognition and enforcement of foreign judgment in Turkish Law is regulated by International Private Law and Procedure Law, no. 5718 dated 12.12.2007. In addition, Turkey is a party of international treaties signed by some of the epSOS countries. In this scope, New York Convention which regulates recognition and enforcement of foreign arbitral awards and La Haye Convention on recognition and enforcement of maintenance orders are the main examples of Turkey's participation to agreements as a party. Reciprocity shall be required in the approval process of foreign judgments according to International Private and Procedure Law, no. 5718. An agreement or treaty which provides reciprocity with all of the epSOS countries is not applicable in this matter. However, there is reciprocity between Turkey and England, Germany, Switzerland, France, Italy, The Netherlands and Austria in terms of enforcement of foreign judgment.

4.4.4 Brussels I Regulation (Brussels I)

The Brussels I Regulation[43] lays down rules governing the jurisdiction of courts in civil and commercial matters. "*A judgment given in an European Union (EU) country is to be recognised without special proceedings, unless the recognition is contested. A declaration that a foreign judgment is enforceable is to be issued following purely formal checks of the documents supplied. The regulation lists grounds for non-enforcement; however, courts are not to raise these of their own motion. The regulation does not cover revenue, customs or administrative matters. Neither does it apply to:*

- *the status or legal capacity of natural persons, matrimonial matters, wills and succession,*

[42] Convention of 1 February 1971 on the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters, http://www.hcch.net/index_en.php?act=conventions.text&cid=78 (last visited: Nov 6th, 2011).

[43] Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L 12, 16.1.2001, p. 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:012:0001:0023:EN:PDF (last visited: Nov. 15th, 2011).

- *bankruptcy,*
- *social security,*
- *arbitration.*"

The basic principle is that jurisdiction is with the EU country in which the defendant – who is most probably to be either the epSOS NCP or the epSOS healthcare provider – is domiciled, regardless of the defendant's nationality. Domicile is determined in accordance with the domestic law of the EU Member State where the matter is brought before a court. In the case of legal persons or firms, domicile is determined by the country where they have their statutory seat, central administration or principal place of business.

4.4.5 Rome I Regulation (Rome I)

Regulation Rome I[44] determines – in contrast to the Brussels regime, that deals with place of venue and enforcement matters – which law is to be applied in cross-border cases. Rome I deals with contractual obligations, whereas Rome II is related to non-contractual obligations.

Out of the regulation's scope are for example revenue, customs or administrative matters (Art. 1 para. 1 Rome I). Also excluded are "arbitration agreements and agreements on the choice of court" (Art. 1 para. 2 lit. e Rome I), which could effect epSOS, as Art. 8.2 FWA designates the European Court of Arbitration as arbitration court. Nonetheless this provision has to be interpreted in a narrow sense as the contract as a whole is supposed to be decisive and not one single provision. Also excluded are "*questions governed by the law of companies and other bodies, corporate or unincorporated, such as the creation, by registration or otherwise, legal capacity, internal organization or winding-up of companies and other bodies, corporate or unincorporated, and the personal liability of officers and members as such for the obligations of the company or body*" (Art. 1 para. 2 lit. f Rome I).

Therefore Rome I needs to be applied to the whole FWA, except for its Art. 8.3 and questions concerning legal status of epSOS.

Basically the selection of law according to Rome I is done in the following order:

1. law either explicitly expressed or clearly demonstrated chosen (Art. 3 para. 1 Rome I),
2. law according to Art. 4 para. 1 Rome I governing special types of contracts as for example contracts for the provision of services, which "*shall be governed by the law of the country where the service provider [ann.: epSOS healthcare providers could be regarded service providers within the meaning of this provision] has his habitual residence*" (Art. 4 para. 1 lit. b Rome I),
3. law of the habitual residence of that party, whose performance is characteristic for the contract (Art. 4 para. 2 Rome I) and
4. as a fallback option – the "*law of the country with which [the contract] is most closely connected*" (Art. 4 para. 4 Rome I).

A reference to the choice of law is made within some provisions of the FWA, when it refers to "national law", as for example in the preamble, Art. 5.1 or Annex I heading 2.

Also relevant for the purposes of epSOS is Art. 6 Rome I on the applicable law regarding consumer contracts. According to that provision a contract "*shall be governed by the law of the country where the consumer [ann.: in the context of epSOS this would be the epSOS patient] has his habitual*

[44] Regulation (EC) 593/2008 on the law applicable to contractual obligations (Rome I), OJ L 177, 4.7.2008, p. 6, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0016:En:PDF (last visited: Nov. 14th, 2011).

residence, provided that the professional [ann.: in the context of epSOS this would be the epSOS healthcare provider]:

(a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or

(b) *by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities.*"

The "*direction of such activities*" to the epSOS patient's country (Art. 6 para. 1 lit. b Rome I) does not refer to the "*mere fact that contact details and an e-mail address are given on a website, […] since this kind of information is obligatory under Article 5(1) of Directive 2000/31/EC on electronic commerce.*"[45] For the purposes of epSOS this means that law suits arising from treatment received in country B are subject to country B's law, save that the healthcare provider clearly directs his services to country A patients, e.g. by providing country A specific information, country A specific contact details and/or information in language A.[46]

4.4.6 Rome II Regulation (Rome II)

The Rome II Regulation deals with non-contractual obligations, i.e. primarily tort issues and culpa in contrahendo (= fault in conclusion of a contract), excluding non-contractual obligations arising out of:

- family relationships and connected obligations regarding property (Art. 1 para. 2 lit. a and b Rome II),
- negotiable instruments, like bills of exchange, cheques, … (Art. 1 para. 2 lit. c Rome II),
- the law of companies (Art. 1 para. 2 lit. d Rome II) or
- the relations connected to trusts created voluntarily (Art. 1 para. 2 lit. e Rome II).

In the event of tort in an EU Member State, excluding Denmark (Art. 1 para. 4 Rome II) the applicable law is determined by Rome II. The universality of both Rome regulations (Art. 2 Rome I and Art. 3 Rome II) may even result in the application of third country law for law suits within the European Union. The general rule governing applicable law defines that the law applicable "*shall be the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur*" (Art. 4 para. 1 Rome II).

For the purposes of epSOS *the country in which the damage occurs* will usually be country B safe from cases where the injury occurs delayed, as for example taking the pills falsely prescribed by healthcare provider B not abroad (country B) but at home (country A).

4.4.7 Conclusion

The provisions of international private law will be especially relevant in damages cases, resulting from both maltreatment (caused or not by wrong/missing data) as well as infringements of privacy. Among the EU Member States these issues are harmonized and covered by the Brussels Regime. Regarding third countries the Lugano Convention governs at least jurisdiction and enforcement and recognition of judgement for some, whereas the choice of law will in most cases be regulated by national laws. As a detailed analysis cannot be provided in the course of this deliverable, the rule of thumb will be that claims have to be filed at the residence of the infringing entity (e.g.: maltreating healthcare provider) according to the national law the infringing entity is subject to.

[45] *Calliess*, Art 6 Rome I in *Calliess* (ed) Rome Regulations – Commentary on the European rules of the conflict of laws, p. 144.

[46] *Calliess*, Art 6 Rome I in *Calliess* (ed) Rome Regulations – Commentary on the European rules of the conflict of laws, p. 144.

4.5 Medical Device Directive (MDD)

Purpose of the Directive 93/42/EEC concerning medical devices (Medical Device Directive – MDD)[47] is to guarantee and harmonize the safety and health protection of patients, users and, where appropriate, other persons, with regard to the use of medical devices in order to guarantee the free movement of such devices within the internal market.

According to Art. 1 para. 2 lit. a MDD a medical device is defined as "*any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:*

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,*
- *investigation, replacement or modification of the anatomy or of a physiological process,*
- *control of conception,*

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means"

It is not yet clear whether epSOS is a medical device in the terms of the new formulation of software as a medical device. This issue needs further analysis, most probably by WP2.2.

[47] Directive 93/42/EEC concerning medical devices, OJ L 169, 12.7.1993, p. 1 as amended, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:EN:PDF (last visited: Nov. 11th, 2011).

ANNEX I: Terminology

cross-border healthcare means healthcare provided or prescribed in a Member State other than the Member State of affiliation (Art. 3 lit. e PRD).

data controller means a natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law (Art. 2 lit. d DPD).

data exporter in accordance with the European Commission's Decisions on Standard Contractual Clauses, means the data controller who transfers personal data to a data imrporter established in a third country (Art. 3 lit. d EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC and Art. 3 lit. c EC Decision 2010/87/EU).

data importer means the controller (Art. 3 lit. e EC Decision 2001/497/EC as amended by EC Decision 2004/915/EC) or processor (Art. 3 lit. d EC Decision 2010/87/EU) established in a third country who agrees to receive from the data exporter personal data intended for processing on the data exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a third country's system ensuring adequate protection within the meaning of Art. 25 para. 1 DPD.

data processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Art. 2 lit. e DPD).

eDispensation (acronym: electronic Dispensation) is defined as the act of electronically retrieving a prescription and administering medicine to the patient as indicated in the corresponding ePrescription. Once the medicine is administered, the dispenser sends an electronic report on the dispensed medicine(s).

ePrescription (acronym: eletronic Prescription, abbreviation: eP) means a medicinal prescription, i.e. a set of data like drug ID, drug name, strength, form, dosage and/or indication(s), provided in electronic format.

epSOS National Contact Points (NCP) are organizations delegated by each Participating Nation, acting as a bidirectional way of interfacing between the existing different national functions provided by the national IT infrastructures and those provided by the common European infrastructure, created in epSOS. The epSOS National Contact Point takes care of external and internal national communication and functions in epSOS and the semantic mapping (if necessary) between information on either side. The epSOS NCP also acts as a kind of mediator as far as the legal and regulatory aspects are concerned. The epSOS NCP creates the conditions (by supporting trust, data protection and privacy) for a trusted relationship with other countries' epSOS NCPs.[48]

healthcare shall mean health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices (Art. 3 lit. a PRD).

health care activity period (deprecated term: contact) means the continuous period of time during which health care activities are performed for a subject of care (CONTsys)

NOTE In EN 13940-1 : 2007 the term contact was used for this concept.

[48] Cf. D. 5.2.1.

health care commitment (Synonym: care commitment) is the outcome of a needs assessment where a health care provider commits to provide health care activities according to a health care mandate (CONTsys)

NOTE 1 The health care commitment is the promise by the health care provider to perform health care activities. This also means that the health care provider accepts and confirms the pending health care mandate issued through the proposed care plan. It is only once the health care commitment has been stated, that an effective health care mandate does exist and will be the legal framework for all health care activities of the subsequent health care process.

NOTE 2 Implicitly, a health care commitment results from a dialogue with the subject of care or someone on behalf of the subject of care within a needs assessment

health care mandate (Synonym: health care commission) menas the commission based on a commitment and either a consent given by the subject of care (or by their representative) or an authorisation by law, defining the scope and limits of the specific role assigned to one health care actor and delineating its role in a health care process (CONTsys)

NOTE 1 A health care mandate can be explicit or implicit

NOTE 2 Information about new health care mandates and changes that have occurred regarding existing health care mandates should be made available for concerned health care parties via recordings in electronic health records.

health care process [Synonym: care process] process where a subject of care and health care actors interact aiming to directly or indirectly influence the health state of that subject of care(CONTsys)

NOTE 1 The main kind of a health care process is the clinical process which has a health state as input and output and is defined by the comprehensiveness of activities in relation to one or more specified health issues.;

NOTE 2 Any health care process is dependent on management and supporting resources.

NOTE 3 A health care process that aims to influence the health state should also influence its perception (the subject of care's health conditions)

NOTE 4 A health care process is not by definition restricted to one health care provider or any other organisational unit borders .

health professional refers to a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Art. 3 para. 1 lit. a D 2005/36/EC, or a person considered to be a health professional according to the legislation of the Member State of treatment (Art. 3 lit. f PRD).

healthcare provider is any natural or legal person or any other entity legally providing healthcare on the territory of a Member State (Art. 3 lit. g PRD).

insured person means (i) persons, including members of their families and their survivors, who are covered by Art. 2 of Regulation (EC) No 883/2004 and who are insured persons within the meaning of Art. 1 lit. c Reg (EC) No 883/2004; and (ii) nationals of a third country who are covered by Reg (EC) No 859/2003 or Reg (EU) No 1231/2010, or who satisfy the conditions of the legislation of the Member State of affiliation for entitlement to benefits (Art. 3 lit. b PRD).

language A means language (of country A) used for the original documents (on which the epSOS Patient Summary and electronic Prescription are based) created and stored by country A.

language B means language different from language A, into which the PS or eP are translated by an epSOS service.

medical records covers all the documents containing data, assessments and information of any kind on a patient's situation and clinical development throughout the care process (Art. 3 lit. m PRD).

medication related overview is a certain overview regarding medication created by some Participating Nations, that consists of relevant aspects for patient care, especially for safety reasons.

Implementations vary widely from country to country, and also the content of this overview might vary from user to user: prescribers and pharmacists do not have the same overview in all countries.

Member State of affiliation would refer to the country where the insurance of a patient is established (Art. 3 lit. c PRD).

Member State of treatment or **country B** means the Member State on whose territory healthcare is actually provided to the patient. In the case of telemedicine, healthcare is considered to be provided in the Member State where the healthcare provider is established (Art. 3 lit. d PRD).

Member State of usual residence or **country A** is the country where the patient is most likely to have his medical records updated due to long term stay for work, studying etc. This may be a different country than the Member State of affiliation, where the patient is insured.

National Contact Point the institution/institutions, which are designated by each Member State for cross-border healthcare (Art. 6 PRD). The name of them and contact details have to be communicated to the Commission and should be publicly available. Member States shall ensure that the National Contact Points consult with patient organisations, healthcare providers and healthcare insurers. National Contact Points shall facilitate the exchange of information and shall cooperate closely with each other and with the European Commission. National Contact Points shall provide patients on request with contact details of National Contact Points in other Member States.

patient is any natural person who seeks to receive or receives healthcare in a Member State (Art. 3 lit. h PRD).

prescription means a prescription for a medicinal product or for a medical device issued by a member of a regulated health profession within the meaning of Art. 3 para. 1 lit. a D 2005/36/EC who is legally entitled to do so in the Member State in which the prescription is issued (Art. 3 lit. k PRD).

process means set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2000, 3.4.1] (CONTsys)

> NOTE Inputs to a process are generally outputs of other processes. In that sense, because their output can be used as an input to another process, activities may sometimes be considered as resources in a process.

subject of care (Synonyms: subject of health care, patient, client, service user) means a person seeking to receive, receiving, or having received health care

> NOTE 1 In some previous standards, a subject of care has sometimes been defined as a "person or defined group of people having received, receiving, or to receive health care". A subject of care may be a group of people, for example a family, a therapy group, a population based group etc. However, this International Standard restricts this concept to an individual person.
>
> In this International Standard, 'subject of care' is definitely restricted to an individual. It is assumed that in those cases where a health care activity addresses a group of more than one individual (e.g. a family, a community) and where a single health record is used to capture the health care activities provided to the group, each individual within the group will be referenced explicitly within that health record.
>
> NOTE 2 In the real world, a subject of care may be designated by different professions using different names, for instance "a patient", "a client" etc.
>
> NOTE 3 A fœtus, when receiving health care, is to be considered as a subject of care.
>
> EXAMPLES A treated patient, a client of a physiotherapist, each particular member of a target population for screening, each particular member of a group of diabetic people attending a session of medical education, a person seeking a health advice.