

To: Participating Nations willing to upkeep eHealth cross-border services

From: eHealth Network Sub-group for upkeep eHealth cross-border services Chair Henrique Martins

Date: 2014-09-16

Status: Final

Temporary Legal Agreement (TLA) to upkeep epSOS developed cross border eHealth services

1. Objective

The Temporary Legal Agreement (TLA) to upkeep epSOS¹ developed cross border eHealth services aims at providing the legal grounds for interested nations to operate cross-border services from 1st October, 2014 on, as epSOS pilots were until the end of epSOS project (30th of June, 2014). However, no longer as pilots but rather as cross-border services. The usage of the TLA should be considered while there is NOT in place a long term Legal Agreement necessary for Services Operation.

2. Scope

This Agreement is applicable to European Union countries as foreseen in the Article 14 of the Directive 2011/24/EU.

3. Background

Under epSOS (Smart Open Services for European patients) Member States (MS) have co-operated to run a Large Scale Pilot (LSP) involving health data exchange across borders. epSOS issued recommendations for legal sustainability² to be considered by the eHealth Network (eHN) when adopting common data protection and security safeguards.

National and/or Regional eHealth Contact Points (NCPeH) have been set up through legally binding national approaches to carry out the epSOS cross-border pilot services to uphold data sharing to support patient care delivered to European citizens outside their usual state of residence by means of a shareable electronic Patient Summaries and ePrescription/eDispensation services.

NCPeHs (epSOS NCP) have operated in conformance to a set of commonly agreed measures and safeguards, approved by the eHealth Authorities Board of epSOS (PSB). The implementation of these safeguards aims to establish the necessary level of trust to ensure that Health Professionals (Art 3 lit f Directive 2011/24/EU) can rely upon the integrity of the data that will support their decisions, that suitable systems of security exist to ensure that data cannot be accessed by unauthorized parties, and that patients' rights of informed consent to data sharing are duly respected by all parties.

¹ www.epsos.eu

² D2.2.7 Legal Sustainability Recommendations

epSOS Member States have provided information on how the Legal Framework Agreement (FWA)³ was implemented including detailed description of their implementation of the epSOS Baseline Security Policy (BSP).

The diverse national implementations have been peer reviewed by a panel of MS legal and policy experts and assessed against the essential requirements of the epSOS FWA. This learning and experience sharing exercise has reinforced confidence that these requirements are sufficient to maintain trust and at the same time realistic and implementable in diverse however conformant ways.

4. Common legal framework rational

The common legal basis for operating these cross-border services is the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare and the Directive 95/46/EU on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The directive sets forth the need for protection of personal integrity, especially in the context of sensitive data such as data in patients' health and defines "consent" to mean the "freely given specific and informed indication of [one's] wishes."

The Directive 2011/24/EU recognizes the importance of the work on interoperability and respect the division of competences by providing for the Commission and Member States to work together on developing measures which are not legally binding but provide additional tools that are available to Member States to facilitate greater interoperability of ICT systems in the healthcare field and to support patient access to eHealth applications, whenever Member States decide to introduce them. Also encourage Member States to facilitate the establishment of cooperation between healthcare providers, purchasers and regulators of different Member States at national, regional or local level in order to ensure safe, high-quality and efficient cross-border healthcare. Such cooperation may concern joint planning, mutual recognition or adaptation of procedures or standards, interoperability of respective national information and communication technology (hereinafter 'ICT') systems, practical mechanisms to ensure continuity of care or practical facilitating of cross-border provision of healthcare by health professionals on a temporary or occasional basis.

In accordance with Article 14 I(1) and (2) of the Directive 2011/24/EU:

- 1. The Union shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States.*
- 2. The objectives of the eHealth network shall be to: (a) 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 and support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.*

³ http://www.epsos.eu/uploads/tx_epsosfileshare/Framework_Agreement_on_National_Contact_Points_V2.pdf

In June 2014, the eHealth Network has established a subgroup (eHN SG) of those MS willing to maintain cross border eHealth services and the operation of their NCPeHs beyond epSOS.

Since then, the eHN SG has been preparing operation baselines to upkeep the services (the TLA and the services operation restart guide).

The TLA (materialized by this document) is inspired and in close adherence to what has already been agreed in epSOS, namely epSOS Legal Sustainability Recommendations⁴. This TLA presents a simplified but secure approach to legal interoperability baselines needed for Participating Nations to operate Cross-Border eHealth Services.

5. Provision

This TLA can also be adopted by Nations willing to operate cross-border care services accordingly to the eHN requirements.

6. Agreement

The National and/or Regional eHealth Contact Point participating in the upkeep of cross-border services will be delegated by the National Health Administrations. They will subsequently declare their conformance to the terms and conditions of this TLA.

Amendments to the following sections may be triggered by adoptions by the eHealth Network and they shall reflect a common interpretation into practice by the NCPeHs.

7. Legal Conditions

7.1. Duties and obligations

7.1.1. Core Characteristics of the National and/or Regional eHealth Contact Point (NCPeH)

7.1.1.1. The NCPeH is a legal entity which is legally competent to contract with other organisations in order to collaboratively carry out its duties and responsibilities related to eHealth cross border services.

7.1.1.2. Where applicable, the NCPeH shall contract with healthcare providers to provide conformant cross border services.

7.1.1.3. The semantic transformation is performed according to the translation, mapping and trans-coding carried out by designated competent legal entities in the participating countries.

7.1.1.3.1. the responsibility for the *accuracy* and integrity of the process is with each national designated competent legal entity for such semantic processing

7.1.1.3.2. Liability for errors in the semantic mapping is shared between the parties who have been involved in the production of the PS or ePrescription.

7.1.1.3.3. Healthcare providers are not liable for any patient safety adverse events attributed to semantic mapping, save for any contributory negligence in interpreting the data.

⁴ D2.2.7 Legal Sustainability Recommendations

- 7.1.1.4. The NCPeH shall provide a gateway service, a request port and a semantic mapping service in order to enable it to execute the core steps in the cross border eHealth services (see section 2.1.5).
- 7.1.1.5. The NCPeH together with its national contractual partners shall collectively fulfil all technical and organisational requirements for secure and confidential transfer or storage of data necessary to perform the steps outlined above. Specifically the NCPeH shall:
- 7.1.1.5.1. be technically competent to provide a gateway for information transfer;
 - 7.1.1.5.2. be legally recognised as a data controller or data processor in accordance with domestic data protection legislation;
 - 7.1.1.5.3. be legally competent to execute contractual agreements with all domestic partners in compliance with domestic data protection legislation;
 - 7.1.1.5.4. be legally competent to enforce audit and corrective action emerging from audits;
 - 7.1.1.5.5. be technically competent to validate the identity of Patients and patient consent of its territory (acting as country A);
 - 7.1.1.5.6. Maintain the local versions of the semantic value sets and their updates.

7.1.2. General Duties and responsibilities of the NCPeH

- 7.1.2.1. The NCPeH shall establish appropriate security and data protection systems to conform to epSOS recommendations⁵, adopted by the epSOS piloting nations, in addition to all applicable national requirements.
- 7.1.2.2. The NCPeH shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).
- 7.1.2.3. The NCPeH assumes responsibility to ensure that has implemented an appropriate system to validate the identity and accreditation of Health Professionals and Healthcare Providers on its territory who may legally receive data originating from an NCPeH in another nation.
- 7.1.2.4. The NCPeH shall establish the agreed system of audit trail so that records of data collected, processed, translated and transmitted may be duly inspected by official bodies if necessary as well as collected by NCPeH A from all parties concerned and handed over to a patient or a Healthcare Provider requiring such information.
- 7.1.2.5. The NCPeH shall assume responsibility for appropriate data collection for the reporting of such data to its national authorities and share these within the eHealth Network subgroup.
- 7.1.2.6. The NCPeH must ensure that nominative data is not transmitted to parties outside the NCPeH and its partners.

7.1.3. NCPeH duties and responsibilities to other NCPeHs

⁵ D3.7.2 Final Security Services Specifications Definition and its annexes:
http://www.epsos.eu/uploads/tx_epsosfileshare/D3.7.2_epSOS_Final_Security_Services.pdf; ;
http://www.epsos.eu/uploads/tx_epsosfileshare/D3.7.2_SECTION_II_epSOS_Security_Services.pdf;
http://www.epsos.eu/uploads/tx_epsosfileshare/D3.7.2_SECTION_III_epSOS_Suitability_analysis.pdf

- 7.1.3.1. The NCPeH shall be accountable to other NCPeHs for ensuring the security (confidentiality, integrity, availability, non-repudiation and authenticity and auditability) of data processed on their territory.
- 7.1.3.2. The NCPeH shall be accountable to other NCPeHs for guaranteeing that all jointly agreed service specifications and requirements (legal, organisational, semantic and technical) are fulfilled.
- 7.1.3.3. The NCPeH shall be accountable to other NCPeHs, for ensuring, conformance of all national partners to jointly agreed service specifications and requirements.
- 7.1.3.4. The NCPeHs shall collaborate actively to the harmonisation of guidelines and appropriate practices to facilitate the establishment of the trusted domain.

7.1.4. Duties and responsibilities concerning Patient Consent

- 7.1.4.1. The processing of healthcare data must have a clear legal basis. The cross-border exchange of healthcare data is process whilst respecting European Union and national regulations on data protection. For the cross-border exchange of healthcare data is required two-step authorization from the patient: previous explicit consent to access data across border and confirmation of consent at the Point of Care (PoC).
- 7.1.4.2. Where the country of affiliation (A) requests and the country of treatment (B) can make it feasible, it is possible to allow patients to give also their first consent in country B, for instance in a secure way over the Internet.
- 7.1.4.3. Processing of personal and sensitive data can be justified without consent confirmation in country B if it is necessary to protect the vital interests of a data subject or of another person if in the emergency case the data subject is physically or legally incapable of giving his consent, in accordance with the national law.
 - 7.1.4.3.1. In this event the patient should be informed about the override of consent upon leaving the PoC including details of access OR
 - 7.1.4.3.2. Patient should be provided access to audit trails
- 7.1.4.4. The processing of personal data must be strictly limited to the minimum which is necessary for the fulfilment of the cross border healthcare purposes which must be specified, explicit and legitimate.
- 7.1.4.5. Data in the log files is to be stored for the purposes of the service and for litigation purposes up to 5 years unless national laws stand for more.
- 7.1.4.6. Each query about the personal data available should be for a real need of access to specific information related to the care or treatment to be provided or the medicine to be prescribed or dispensed in a particular case.

7.1.5. Steps in the Process

1. Health Professional in country B at a Point of Care accepts patient ID.
2. Health Professional in country B at a Point of Care confirms patient consent to access data in Country A; or Health Professional ticks the override box in cases where consent cannot be obtained because of patient incapacity. A Health Professional's query can be processed only with consent or override duly confirmed.
3. Health Professional in country B sends query to NCPeH in country B.

4. NCPeH in country B authenticates the Health Professional and Point of Care.
5. The NCPeH in country B queries NCPeH in country A for the requested patient data.
6. NCPeH in country A authenticates NCPeH in country B.
7. NCPeH in country A validates patient ID and local prior agreement (if applicable).
8. NCPeH in country A transmits the requested data to NCPeH in country B.
9. NCPeH in country B authenticates NCPeH in country A.
10. NCPeH in country B provides the requested data to Health Professional requestor.

7.2. Security

Members signing this TLA accept to implement security measures as defined by epSOS Deliverable 3.7.2 (refer to Annex 1 of this TLA).

7.3. Liability

Cross border information services offered under this agreement are adjuvant to and do not replace other means of collecting and confirming medical data for medical decision making. Members signing this TLA are responsible for ensuring that health professionals are appropriately informed about the intended use, value and limitations of current eHealth cross border services (Annex 1.4).

Annex 1. epSOS references

A1.1. epSOS Legal and Regulatory perspectives⁶

From a Legal and Regulatory (L&R) perspective, it is important to note that the epSOS Services will be offered on a pilot basis. They will be provided in compliance with the EU regulatory framework, and as such will not require changes to national legislation governing the provision of health services. As a pilot, the primary objective of the initiative is to gather information and evidence in order to provide guidance towards full deployment.

A1.2. epSOS Security Specifications

Final Security Services Specification Summary⁷

- Deliverable 3.7.2: Final Security Services Specification ("Master Document")
 - D3.7.2 Section I: epSOS Security Policies
 - D3.7.2 Section II: Security Services
 - D3.7.2 Section III: Suitability Analysis

A1.3. epSOS Organizational Specifications

Organizational specifications:

- Deliverable D3.8.2 Final National Pilot Set Up and deployment Guide⁸

A1.4. epSOS Privacy Information Notice

1. What is epSOS?

epSOS – Smart Open Services for European Patients – is a large scale pilot project being conducted across several European countries to help European citizens access health services when they are outside their usual country of residence.

[Country/Region] is taking part in epSOS so you, as a citizen of [Country/Region], are entitled to make use of the epSOS services if you need medical care while in another participating country.

2. What are epSOS services

The aim of the epSOS Large Scale Pilot is to demonstrate that it is feasible for citizens of a European country to enjoy the benefits of electronic health services that they receive at home, when they travel abroad without compromising their rights to privacy and confidentiality. The two epSOS services that are offered on a pilot basis have been tested and appropriate safeguards required by European and national law have been taken.

Additionally, [name of NCP-A] guarantees that the level of security and protection of citizens rights to privacy have been ascertained to a level that has been considered appropriate by all

⁶ Legal and Regulatory: http://www.epsos.eu/fileadmin/content/pdf/epSOS_Legal_Perspectives_2013.pdf

⁷ Security Specifications: <http://www.epsos.eu/home/about-epsos/project-structure/work-package-37/d372-final-security-services-specification-definition.html>

⁸ Organizational specifications: http://www.epsos.eu/uploads/tx_epsosfileshare/D3.8.2_National_Pilot_Set-up_and_Deployment_Guide_01.pdf

countries and regions participating in this pilot. *Please consult the epSOS website www.epSOS.eu for a current list of piloting nations and regions.*

Each of these countries and regions, through a designated organisation, have undertaken to ensure that the participating Healthcare Providers and Health Professionals on their territory taking part in the epSOS pilot have adequate information and training about the pilot and the duties and responsibilities which must be assumed when offering these epSOS services. Please refer to the epSOS website for details on the epSOS pilot and the participation of [country name] in it.

3. Your data, Your Consent

The epSOS services will become available to you in participating countries and institutions only if you explicit consent to provide access to your personal Patient Summaries/e-prescriptions to health professionals in the context of providing care to you while you are abroad. Please refer to the epSOS Terms and Conditions⁹ document for details on these services and the terms and conditions for their delivery.

[Here please insert a paragraph about

2. consent to create a PS if needed by your country
3. consent to **opt-in** the epSOS pilot so that your personal Patient Summaries/e-prescriptions can be made accessible for health professionals in participating countries and institutions, and how an opt-in consent can be given if needed by your country
4. any exceptions to providing access in case of emergency (e.g. if prior consent has not been provided)]

When abroad in an actual care situation, the treating physician will need your consent to access your Patient Summaries/ePrescriptions.

If you have not provided your agreement to participate in the epSOS pilot in [country name] it is still possible to provide consent for access to data from the country you are visiting after reading and agreeing to (through signing) the epSOS Terms and Conditions and confirming your consent to the treating physician by confirming the following statement in a country where you require medical care:

'I agree that my [name of electronic document as known in the MS] may be transferred to a registered Health Professional in [COUNTRY OF TREATMENT] for the purposes of providing me with medical care and/or medication.

⁹ http://www.epSOS.eu/uploads/tx_epSOSfileshare/epSOS_TERMS_AND_CONDITIONS.pdf

Annex 2. Glossary and Acronyms

Annex 2.1 Glossary

Term	Definition	Abbrev.
Citizen	An individual in a Participating Nation who can be a patient, a relative of a patient, a carer or any person who may need to have access to healthcare in the future. At its simplest, citizens are represented as the total population of a Participating Nations (EHRI).	
Country A	The country of affiliation. This is the country which holds information about a patient, where the patient can be univocally identified and his data may be accessed.	
Country B	The country of treatment i.e. where cross-border health care is provided when the patient is seeking care abroad. This country is different from country A, in which health care related information about a patient is held.	
Cross-border healthcare	Healthcare provided or prescribed in a country other than the country of affiliation.	
eDispensation, eDispensing	The act of electronically retrieving a prescription and giving out the medicine to the patient as indicated in the corresponding ePrescription. Once the medicine is dispensed, the dispenser shall report via software the information about the dispensed medicine(s).	eD
eHealth	Health care practice which is supported by electronic processes and communication.	
Electronic Health Record	A comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes.	EHR
Episode of care	An interval of care by a health professional for a specific medical problem or condition. It may be continuous or it may consist of a series of intervals marked by one or more brief separations from care, and can also identify the sequence of care (e.g., emergency, inpatient, outpatient), thus serving as one measure of Health Care provided (acc. to http://www.mondofacto.com/dictionary/medical.html)	
ePrescription	A prescription for medicines or treatments, provided in electronic format.	eP
Health Professional	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 Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the country of treatment. epSOS Health Professionals re designated HPs within the epSOS PoCs that are entitled to deliver the epSOS services.	HP
National Connector	Entity that encapsulates the Nation-Specific NCP Components. The National Connector is implemented as a black box having its subcomponents hidden from the NCP	NC
National and/or Regional eHealth Contact Point	National and/or Regional eHealth Contact Point have been set up through legally binding national approaches to carry out the epSOS cross-border pilot services to uphold data sharing to support patient care delivered to European citizens outside their usual state of residence by means of a shareable electronic PS and eP/eD services	NCPeH

Term	Definition	Abbrev.
NCP Gateway	A gateway system under the control of the NCP that manages all epSOS transactions and which connects the National Infrastructure (NI) to the epSOS backbone. It is a point of entry/exit to/from the NCP, acting on behalf of a HP (at a PoC) who requires access to a patient's medical data through epSOS, or acting as service broker of an epSOS data provider	NCP
Participating Nation	A country participating in the eHN SG or on EXPAND, e-SENS or Trillium Bridge projects	PN
Patient Access Service	Enables health professionals and patients to access and understand what has been recorded in the PS, eP or other epSOS documents in a language different from the original language of the PS, eP or other epSOS documents.	PAC
Patient Consent	A patient's freely given explicit and informed agreement provided to the data controller or data processor of his wish to personal data relating to him being processed for a given purpose.	
Patient Summary (document)	A Patient Summary is a concise clinical document that provides an electronic patient health data set applicable both for unexpected, as well as expected, healthcare contact. The epSOS PS is a standardized set of basic health data containing the most important clinical patient data (e.g. allergies, current medical problems, medical implants, or major surgical procedures during the last six months). The epSOS PS does not include a detailed medical history, details on clinical conditions or a full list of all prescriptions and dispensed medicines.	PS
Patients' Rights Directive	Directive 2011/24/EU on the application of patients' rights in cross-border healthcare	PRD
Pharmacists	Health professionals who practice in pharmacy, the field of health sciences focusing on safe and effective medication use	
Point of Care	An epSOS Point of Care is a location where an epSOS patient may seek healthcare services. It can be a hospital, a pharmacy, the practice of a registered health professional or any other point of the health care system of country B which participates in the epSOS pilot. It is designated by its competent Pilot Partner after having demonstrated its capacity to comply with the epSOS requirements.	PoC

Annex 2.2 Acronyms

Acronym	Description
eD	eDispensation
eHN	eHealth Network
eHN SG	eHN Sub Group
EHR	Electronic Health Record
eP	ePrescription
HP	Health Professional
LSP	Large Scale Pilot
MS	Member State
NC	National Connector
NCP	National Contact Point
NI	National Infrastructure
PAC	Patient Access Service
PN	Participating Nation
PoC	Point of Care
PRD	Patients' Rights Directive
PS	Patient Summary

Annex 3. Signing sheet and Signature pages

Signature pages are to be **done in two originals per country**.

Ministry of Health or Regional Health Authority or eHealth Network representative should agree to this TLA and delegate on the Regional Health Authority (when applicable) and NCPeH the authority to sign it on behalf of the Participating Nation. In order to formalize it, the representative should sign the annexed “signing sheet”.

In order to be part of the circle of trust, Regional Health Authority (when applicable) and NCPeH are asked to commit to comply with the requirements above and that undertake to safeguard its continuing conformity to them. To express this commitment, NCPeH signature of this TLA is mandatory.

After printed, signed, stamped and dated by the Ministry of Health or the Regional Health Authority or the eHealth Network representative and by the National or Regional eHealth National Contact Point (NCPeH), the originals should be sent to the eHealth Network Sub Group chair (Henrique Martins), to speed up the process. His secretariat will collect the information, return one original to the signatories, instruct the process and send it to the eHN Secretariat.

The eHN Secretariat will be the faithful depositary of documents signed.

The Temporary Legal Agreement (TLA) for the expressed purposes, i.e., to upkeep epSOS developed cross border eHealth services will result from the set of signed pages received and aggregated by the eHN Secretariat.

Signing sheet

Done in two originals in English

<Please print on headed notepaper of your Ministry>

<Done at>, <day> September, 2014

Temporary Legal Agreement

I, <name of legally representative of Ministry of Health / name of Regional Health Authority / name of eHealth Network representative>, in my function as <title of legal representative> / <eHealth Network representative> and thereby authorized to represent the <Ministry of .../ Regional Health Authority / country> I am pleased to inform that we agree on eHealth Network Subgroup (eHN SG) Temporary Legal Agreement (TLA) statements and requirements and consent that <name of National or Regional eHealth National Contact Point>, represented by <name of legal representative of NCPeH>, established at <address>, <country> to act on our behalf with powers to sign the present TLA for <country name>.

Yours sincerely,

<position>

<signature and stamp>

<name of legal representative of the Ministry/Regional Health Authority/eHN rep>

<Please print on headed notepaper of your organization>

Signature page

Done in two originals in English

**For the Participating Nation /
Region**

Done at:

Name of the legal entity:

Name of legal representative:

Stamp of the organisation (if
applicable)

Signature of legal representative:

Date: 2014-09-