REGERINGEN

Regeringsbeslut **I:21**

2013-12-19 S2010/4937/FS (delvis)

Socialdepartementet

E-hälsomyndigheten
c/o Organisationskommittén
118 60 Stockholm

Uppdrag att vara nationell kontaktpunkt i EU-projekt och bemyndigande att ta ut avgifter

1 bilaga

Regeringens beslut

Regeringen beslutar ge E-hälsomyndigheten i uppdrag att till och med den 30 juni 2014 vara nationell kontaktpunkt för EU-projektet epSOS (Smart Open Services for European Patients). Uppdraget ska genomföras i enlighet med uppdragsbeskrivningen i *bilagan*. För utförandet av uppdraget får E-hälsomyndigheten enligt avtal med Sveriges Kommuner och Landsting (SKL) ta ut en avgift från organisationen. Myndigheten får bestämma storleken på avgiften och disponera avgiftsinkomsten.

Ärendet

Sverige har tillsammans med 24 andra medlemsstater tagit initiativ till EU-projektet epSOS (Smart Open Services for European Patients). Projektets uppdrag är att arbeta fram lösningar för att möjliggöra en säker dataöverföring av känsliga personuppgifter mellan länder. Sverige har rollen som koordinator för projektet, vilken Sveriges Kommuner och Landsting ansvarar för enligt tidigare avtal med regeringen (dnr S2010/4937/FS).

All dataöverföringen av patientuppgifter inom projektet ska ske genom nationella kontaktpunkter (NCP), en per deltagarland, som ska säkerställa och kontrollera att överföringen sker mellan auktoriserade personer och inom säkerställda tekniska lösningar. Förutom den tekniska lösningen ska säkerheten vid överföringen garanteras av att samtliga deltagande länder bygger upp snarlika system och med kontroller genomförda av projektet. Deltagarländer kan antingen fullgöra NCP-funktionen i egen regi eller ingå avtal med en fristående juridisk person. Avtal ska baseras på av projektet framtaget ramavtal Framework Agreement (FWA) med justeringar för den egna nationella rätten. Även i de fall när NCP-funktionen ska genomföras i egen regi ska uppdraget genomföras i enlighet med de bestämmelser som framgår av projektets ramavtal. Socialdepartementet har genom regerings-

Postadress 103 33 Stockholm
Besöksadress Fredsgatan 8
Telefonväxel 08-405 10 00
Telefax 08-723 11 91
E-post: s.registrator@regeringskansliet.se

beslut den 12 maj 2013 ingått avtal med Apotekens Service Aktiebolag varigenom bolaget åtagit sig uppdraget som nationell kontaktpunkt för projekt epSOS. Avtalet löper till och med den 31 december 2013. Inom ramen för ansvaret som koordinator för epSOS har även Sveriges Kommuner och Landsting (SKL) ingått avtal med Apotekens Service Aktiebolag för genomförande av vissa delar av de åtaganden som åligger Sverige.

Den 4 oktober 2013 beslutade epSOS generalförsamling att förlänga projektet sex månader, t.o.m. den 30 juni 2014, för att möjliggöra längre testperiod för pågående aktiva piloter. Sverige har beslutat att delta i projektets förlängning vilket även kräver att en nationell kontaktpunkt för överföring av patientuppgifter upprättas för förlängningsperioden. Regeringen har genom beslut den 19 december 2013 avsatt 4 000 000 kronor som SKL får använda under 2014 för arbeta med gränsöverskridande e-receptslösning med utgångspunkt från Sveriges deltagande i projekt epSOS.

Den 1 januari 2014 bildas den nya E-hälsomyndigheten. I och med bildandet av myndigheten kommer staten i myndighetsform fortsätta att utföra de uppgifter som utgjort verksamheten i Apotekens Service Aktiebolag. Det innebär att Apotekens Service Aktiebolag ska avvecklas. Det är därför lämpligt att även uppdraget som nationell kontaktpunkt för projekt epSOS överförs från bolaget till den nya myndigheten. Det innebär även att E-hälsomyndigheten måste ges möjlighet att samverka med SKL i likhet med vad som tidigare överenskommit via avtal för genomförandet av Sveriges åtaganden.

Uppdraget ska genomföras i enlighet med den uppdragsbeskrivning som framgår av *bilagan*. Uppdragsbeskrivningen överensstämmer i huvudsak med det tidigare ingångna avtalet mellan Staten och Apotekens Service Aktiebolag.

På regeringens vägnar

Göran Hägglund

Henrik Moberg

Kopia till

Justitiedepartementet/L6
Justitiedepartementet/L2
Finansdepartementet/BA
Regeringskansliets förvaltningsavdelning
Utredningen om inrättande av en ny myndighet för hälso- och vårdinfrastruktur (S 2013:03)
Apotekens Service Aktiebolag
Sveriges Kommuner och Landsting

Bilaga till
regeringsbeslut
2013-12-19 nr I:21

Upppdragsbeskrivning

Regeringen har genom beslut den 19 december 2013 gett Ehälsomyndigheten i uppdrag att vara Sveriges nationella kontaktpunkt (fortsättningsvis betecknat NCP) för projekt epSOS. Uppdragsbeskrivningen fastställer villkor för uppdraget.
The Swedish eHealth Agency has been commissioned by the Swedish Government to act as the Swedish national contact point(NCP) for the large scale pilot epSOS. The Instructions (FWA/S) sets down the conditions for the assignment.

Uppdragsbeskrivningen baseras på pilotprojektets mallavtal ”Framework Agreement”(fortsättningsvis betecknat FWA/epSOS) fastställt den 8 juni 2011, bilaga 3.
The FWA/epSOS, annex 3, approved June 8th 2011 has been used as a blueprint for the FWA/S.

Uppdraget gäller enbart för projektets genomförande inom Sverige.
Svensk rätt gäller om konflikt uppstår mellan svensk rätt och mallavtalets, eller andra epSOS-dokuments text och innebörd.
FWA/S is applicable for the realization of the LSP epSOS in Sweden. Swedish national law takes priority in any conflicts between Swedish national law and FWA/epSOS or any other epSOS-documents.

Personuppgiftslagen (1998:204) och specialförfattningar som innehåller bestämmelser om behandling av känsliga personuppgifter gäller för uppdraget. Vidare ligger Europaparlamentets och rådets direktiv 95/46/EG (dataskyddsdirektivet) till grund för projekt epSOS arbete med att säkerställa grundläggande skydd för den personliga integriteten vid behandling av personuppgifter om patienter. Projektet ställer därför krav på att samtycke från patienter ska vara frivilligt, uttryckligt och informerat samt överensstämma med nationell rätt i vårdlandet (land B). För svenska förhållanden finns bestämmelser i personuppgiftslagen (1998:204) och specialförfattningar om krav på uttryckligt samtycke och möjliga undantag från krav på samtycke vid behandling av känsliga personuppgifter. Om konflikt uppstår mellan hanteringen av personuppgifter inom epSOS och hanteringen av sådana uppgifter enligt svensk rätt gäller svensk rätt.
FWA 5.1, 5.2

Ehälsomyndighetens hantering av personuppgifter, vilket inkluderar känsliga personuppgifter inom projekt epSOS ska ske i enlighet med vad som anges ovan. I detta arbete ska Ehälsomyndigheten även beakta de krav som projektet ställer i bilaga 3 a och 3 b i den mån det är möjligt inom ramen för svensk rätt.
FWA 5.1 Annex 3a and 3b

För att möjliggöra jämförelse mellan uppdragsbeskrivning och FWA/epSOS har motsvarande klausul eller text i FWA/epSOS angetts med blå text i direkt anslutning till korresponderande text eller klausul. Översättning och hänvisning har skapats för att underlätta jämförelse mellan dokumenten och utgör ingen garanti för en fullständig överenstämmelse mellan innehållet i uppdragsbeskrivningen och FWA/epSOS.
When possible each provision in the FWA/S has a reference, written in blue, to the corresponding article or text in the FWA/epSOS. The system of cross-references has been created for the easier understanding of the FWA/S and does not guarantee total conformity between the FWA/S and the FWA/epSOS.

1. DEFINITIONER
Definitions

1.1. Definitioner intagna i D2.1.2 utgör del av uppdragsbeskrivningen, se Definitions of concepts and key terms, bilaga 4.
Definitions set out in D2.1.2, annex 4 constitutes an integral part of FWA/S.

1.2. Förkortningar eller kortformer upptagna i D2.1.2 utgör del av uppdragsbeskrivningen, se Abbreviations, bilaga 5.
Abbreviations set out in D2.1.2, annex 5 constitutes an integral part of FWA/S.

1.3. I uppdragsbeskrivningen ska följande begrepp ha följande innebörd:
Definitions to be used in FWA/S are as follows.

Apoteksaktör	avser deltagande apoteksbolag
Apotekspersonal	avser deltagande apotekspersonal, jämför begreppet ”*Health Care Professional*” i bilaga 4, se också ”Health professional” i bilaga 9
ATC-system	avser 1. begreppet "Anatomical Therapeutic Chemical Classification", och avser 2. System för klassificering av läkemedel
Consortium Agreement	avser ingånget konsortialavtal mellan deltagande länder i pilotprojekt epSOS i avsikt att genomföra projektet
D2.1.2	avser dokumentet ”D2.1.2 Legal and Regulatory Constraints on epSOS Design – Participating Member States dated 31 January 2010”, bilaga 2
Deltagarland	avser land som deltar i epSOS, jämför begreppet *Participating Member state* bilaga 4
Deltagande vårdenhet	avser deltagande vårdenheter eller apotek, jämför med begreppet ”*epSOS Point of Care*” såsom det definieras i Definitions, bilaga 4, och ”*PoC*” i Abbreviations, bilaga 5
epSOS	avser projekt ”epSOS Smart Open Services – Open eHealth initiative for a European large scale pilot of patient summary and electronic prescription” – beteckning enligt avtalet ”Consortium Agreement”
epSOS-data	avser personuppgifter som används inom epsos samt uttrycket ”*epsos data*” såsom det används i 5.1 Mallavtalet
epSOS register	avser sammanställning av personuppgifter inhämtade för användning inom epSOS, jämför begreppet ”*epsos record*” såsom

	det används i 5.3 Mallavtalet
epsos patienter	1.avser begreppet ”*epSOS Patients*” såsom definierats i Definitions, bilaga 4 2.avser samtliga individuella deltagare som har för avsikt att utnyttja de tjänster som projekt erbjuder
epSOS Security Policy (SP)	avser epSOS säkerhetspolicy, se bilaga 8
epSOS tjänster	avser uttrycket ”*epSOS services*” eller ”*services*”, såsom det definierats i Glossary, bilaga 9
eRecept	avser recept i elektronisk form, jämför med begreppet ”*ePrescription*” såsom definierats i Definitions, bilaga 4
FWA, FWA/epSOS	avser förkortning för ”*Framework Agreement*”, se även ”*Mallavtalet*”
Land A	avser begreppet ”*country A*” såsom definierats i Definitions, bilaga 4
Land B	avser begreppet ”*country B*” såsom definierats i Definitions, bilaga 4
LSP	avser begreppet ”*large scale pilot*” såsom definierats i Definitions, bilaga 4
Health Care Organisation (HCO)	avser vårdgivare som är juridiska personer såsom definierats i Definitions, bilaga 4
Health Care Provider	avser begreppet vårdgivare såsom definierats i Definitions, bilaga 4
Health Care Professional (HCP)	avser begreppet vårdpersonal såsom definierats i bilaga 4
Health Professional (HP)	avser begreppet vårdpersonal såsom definierats i Glossary, bilaga 9
Mallavtalet	avser ”*Framework Agreement*” eller ”*FWA*” eller ”*FWA/epSOS*” såsom beskrivits i dokumentet D2.1.2, Part II, bilaga 3
Nationell kontaktpunkt	avser 1. utsedd legal enhet med ansvar för överföring av patientdata mellan deltagande länder, och 2. begreppet ”*National Contact Point*” eller ”*NCP*” såsom definierats i Definitions, bilaga 4
NCP/Sverige, NCP/S	avser den svenska nationella kontaktpunkten enligt denna uppdragsbeskrivning
NCP/A	avser NCP som sänder patientdata
NCP/B	avser NCP som tar emot patientdata
Nationell Pilotenhet	avser begreppet ”*epSOS Pilot Site*” såsom definierats i Definitions, bilaga 4
Patientöversikt	avser begreppet ”*Patient Summary*” såsom definierats i Definitions, bilaga 4
Pilotprojekt	avser pilotprojekt epSOS
Participating Nation (PN)	avser deltagarland i epSOS-piloten, jämför definition i Glossary, bilaga 9
PUL	avser personuppgiftslag (1998:204)
Samarbetspartners	avser vårdenheter, vårdgivare, vårdpersonal, apoteksaktörer och

	apotekspersonal samt begreppet ”*epSOS Pilot Partners*” såsom definierats i Definitions, bilaga 4
Samarbetsavtal	avser avtal mellan Apotekens Service i dess roll som NCP/Sverige och svenska samarbetspartners
Semantiskt identifierad informationsmängd	avser identifierade datamängder i t.ex. recept och journal inom epSOS, jämför även med definition i bilaga 9
Semantic interoperability	avser system med förmåga att vid utbyte av information säkerställa att denna information är förståbart för mottagande system, jämför även med definition i bilaga 9
Semantic mapping	avser etablering av samband mellan element som inte tillhör samma system; en process som kopplar ihop koder och gör dem likvärdiga; beskriver hur en kod ska bli en annan i samband med ”transcoding”, jämför även med definition i bilaga 9
Semantic processing	avser översättningsprocessen mellan två språk eller kodsystem
Semantic transformation	avser teknisk översättning eller mapping av identifierade informationsmängder i epSOS, jämför även med ”semantiskt identifierad informationsmängd” och definition i bilaga 9
Semantic translation	avser översättning, inom projektet utvalda semantiska källor översätt mellan olika språk t.ex. översättning av ATC-koden mellan engelska och svenska
Semantic transcoding	avser byte av en kod inom ett system mot en annan kod i ett annat system när samma kodsystem inte används, jämför även med definition i bilaga 9
Semantisk informationshantering	avser ”Semantic interoperability” i bilaga 9
Semantiskt system	avser terminologier, klassifikationer och kodverk
Uppdragsbeskrivning	avser uppdragets innehåll, inklusive bilagor
Value set (se 2.10)	avser följande definition: “A uniquely identifiable set of valid concept representations where any concept representation can be tested to determine whether or not it is a member of the value set. A value set may be a simple flat list of concept codes drawn from a single code system, or it might be an unbounded hierarchical set of possibly post-coordinated expressions drawn from multiple code systems. A Value Set may include a list of zero or more Coded Concepts drawn from a single Code System. A Value Set can represent: all of the Coded Concepts defined in exactly one Code System, a specified list of Coded Concepts that are defined in exactly one Code System, or a set of Coded Concepts represented by another Value Set”, jämför även med definition i bilaga 9
Vårdenhet	avser begreppet ”deltagande vårdenhet”
Vårdgivare	avser begreppet ”*Health Care Provider*” såsom definierats i Definitions, bilaga 4
Vårdspersonal	avser begreppet ”*Health Care Professional*” såsom definierats i Definitions, bilaga 4

2. GRUNDLÄGGANDE KRAV OCH ÅTAGANDEN FÖR DEN SVENSKA NATIONELLA KONTAKTPUNKTEN

2.1 Ehälsomyndigheten ska ingå avtal (samarbetsavtal) med vårdgivare och apoteksaktörer angående tillhandahållande av epSOS-tjänster till patienter. Ett samarbetsavtal ska, i den mån det inte strider mot svensk rätt hålla sig till intentionerna i mallavtalet.
FWA/epSOS 2.2, 7.3

2.2 Ehälsomyndigheten ska ansvara för uppbyggnaden av den semantiska struktur och tillämpning av det semantiska system, vilket även inkluderar systemets tillförlitlighet och integritet, som ska användas inom projekt epSOS.
FWA/epSOS 2.3, 2.3.1

2.3 Ehälsomyndigheten ska tillhandahålla en service- och förfrågningsportal samt tjänster avseende semantisk översättning för att möjliggöra genomförande av utbyte av epSOS-data som beskrivs i dokumentet ”Förfarandesätt vid utbyte av epSOS-data”, bilaga 6.
FWA/epSOS 2.4

2.4 Ehälsomyndigheten ska, i den mån det inte strider mot svensk rätt, uppfylla samtliga tekniska och organisatoriska krav som gäller säker och konfidentiell överföring eller lagring av data i enlighet med de krav som anges i epSOS säkerhetspolicy, bilaga 8.
FWA/epSOS 2.5 regulating only NCP/S as FWA/S is only applicable for the realization of the LSP epSOS in Sweden.

2.5 Ehälsomyndigheten ska ansvara för att bolaget har teknisk kompetens att tillhandahålla en portal för överföring av epSOS-data.
FWA/epSOS 2.5.1

2.6 Ehälsomyndigheten är personuppgiftsansvarig för behandling av personuppgifter som nationell kontaktpunkt för projekt epSOS.
FWA/epSOS 2.5.2

2.7 Ehälsomyndigheten ska, i den mån det överensstämmer med svensk rätt, följa säkerhetspolicyn inom projekt epSOS, bilaga 8.
NCP/S undertakes to apply the epSOS security policy (SP), annex 8, when the provisions of the Security Policy are in accordance with Swedish law. Swedish law takes priority over the FWA/epSOS, the epSOS security policy or any other document or agreement whatever the standing of the document or agreement. See also notification, written in red, in annex 8.

2.8 Ehälsomyndigheten ska i dess egenskap som NCP/A ha teknisk kompetens att kontrollera och säkerställa patients identitet och samtycke.
FWA/epSOS 2.5.5

2.9 Ehälsomyndigheten ska upprätthålla den svenska versionen av det semantiska kodverk som fastställs av projekt epSOS.
FWA/epSOS 2.5.6

3 EHÄLSOMYNDIGHETENS GENERELLA ÅTAGANDEN

FWA 3

3.1 Ehälsomyndigheten ska upprätta ett säkerhets- och dataskyddssystem som både är förenligt med de krav projekt epSOS uppställer och svensk rätt.
FWA/epSOS 3.1

3.2 Ehälsomyndigheten ska upprätta ett säkerhetssystem som säkerställer behandling av personuppgifter (epSOS-data) och vidta nödvändiga åtgärder för att säkerställa skyddet för överföring av alla personuppgifter.
FWA/epSOS 3.2 1st passage

3.3 Ehälsomyndigheten ska ansvara för att överföring av alla former av personuppgifter enbart kan ske till identifierade deltagare i projekt epSOS.
FWA/epSOS 3.3

3.4 Ehälsomyndigheten ska ansvara för att behörigheten för den personal som ska behandla personuppgifter inom projekt epSOS kan säkerställas.
FWA/epSOS 3.2 2nd passage 1 1st sentence

3.5 Ehälsomyndigheten ska upprätthålla en supportavdelning som ska tillhandahålla hjälp och support till vårdpersonal, vårdgivare och apotekspersonal inom Sverige.
FWA/epSOS 3.4

3.6 Ehälsomyndigheten ska ansvara för att inom Sverige upprätthålla kommunikationsmöjligheter mellan Samarbetspartners inom projekt epSOS i Sverige. Ansvaret omfattar även att upprätthålla korrekta länkar till projektets internationella hemsida.
FWA/epSOS 3.5

3.7 Ehälsomyndigheten ska ansvara för att gränsöverskridande utbyte av personuppgifter enligt uppdragsbeskrivningen sker inom ramen för den tekniska lösning som framtagits av projekt epSOS.
The NCP/S undertakes to use the technical solution produced by the LSP epSOS for cross-border exchange of personal data within epSOS.

4 BESTÄMMELSER AVSEENDE PATIENTSAMTYCKE

FWA/EPSOS 5

4.1 Register över Patientöversikt och eRecept får enbart föras under förutsättning att detta överensstämmer med svensk rätt. För utformningen av och innehållet i behövligt patientsamtycke för registrering gäller bestämmelser i personuppgiftslagen (1998:204) och tillämpliga specialförfattningar.
FWA/epSOS 5.3

4.2 Ehälsomyndigheten har möjlighet upprätta ett system som möjliggör för en patient att på förhand lämna ett samtycke till att utländsk vårdpersonal, vårdgivare, vårdenhet eller apotekspersonal får ta del av patientens personuppgifter under förutsättning att den nationella rätten i Land A tillåter ett sådant förfaringssätt.

FWA/epSOS 5.4

4.3 Ehälsomyndigheten får skapa ett system för inhämtande av patientsamtycke för de fall ett föregående samtycke inte har inhämtats i land A, under förutsättning att sådant inhämtande är tillåtet i både land A och Sverige.
FWA/epSOS 5.6

4.4 Ehälsomyndigheten ska skapa ett system som ska kunna tillämpas för nödsituationer när patientsamtycke inte kan inhämtas.
FWA/epSOS 5.7

5 EHÄLSOMYNDIGHETENS ÅTAGANDEN UNDER EPSOS SÄKERHETSPOLICY

FWA/epSOS 6

5.1 epSOS säkerhetspolicy, bilaga 8 utgör ett allmänt ramverk avseende säkerhets- och dataskydd som är anpassat till de behov som finns avseende epSOS informationssystem. epSOS säkerhetssystem ska tillämpas när det överensstämmer med svensk rätt.
FWA/epSOS 6.1.

5.2 Säkerhetspolicyn beskriver samtliga dataflöden som sker inom projekt epSOS, både nationella och gränsöverskridande dataflöden.
FWA/epSOS 6.2

5.3 Ehälsomyndigheten ska uppfylla de krav på säkerhet som finns angivna i epSOS säkerhetspolicy i den mån detta överensstämmer med svensk rätt.
FWA/epSOS 6.3 regulating only NCP/S.

6 EHÄLSOMYNDIGHETENS FÖRHÅLLANDE GENTEMOT SAMARBETSPARTNER

FWA 7

6.1 Ehälsomyndigheten ska möjliggöra för primära och sekundära vårdgivare (allmänpraktiserande läkare och läkarmottagningar respektive sjukhus samt andra vårdgivare som är specialiserade på sekundärvård) och apoteksaktörer (såväl statliga som privata) att delta i projekt epSOS.
FWA 7.2

Bilagor
Annex

Bilaga 1 Annex 1	Beskrivning av pilotprojekt av epSOS Description of the LSP epSOS
Bilaga 2 Annex 2	D2.1.2 Legal and Regulatory Constraints on epSOS Design- Participating Member states
Bilaga 3 Annex 3	epSOS Framework Agreement on National Contact Point – approved 8th June 2011

Bilaga 3a Annex 3a	Annex I epSOS Privacy information notice
Bilaga 3b Annex 3b	Annex II epSOS terms and conditions
Bilaga 4 Annex 4	Definitions of concepts and key terms (from D2.1.2 page 7 - 10)
Bilaga 5 Annex 5	Abbreviations (from D2.1.2 page 11)
Bilaga 6 Annex 6	Förfarandesätt vid utbyte av epSOS-data Endnote – steps in epSOS process
Bilaga 7 Annex 7	Teknisk och organisatorisk kravspecifikation D.3.8.2 National Pilot Set Up and Deployment Guide
Bilaga 8 Annex 8	epSOS Security Policy (epSOS SP)
Bilaga 9 Annex 9	epSOS Glossary – version per 28 January 2013
Bilaga 10 Annex 10	Cross-reference FWA/epSOS and FWA/S, with notifications and comments by Sweden

Kort bakgrundsbeskrivning till projekt epSOS

EU-medborgares rätt till fri rörlighet och tillgång till gränsöverskridande vård är ett prioriterat område för Europeiska kommissionen (Kommissionen). För att ytterligare utveckla den fria rörligheten har Kommissionen genom eHealth action plan[1] fastställt en plan för att möjliggöra ett friare flöde av data över statsgränser, bl.a. mellan nationella sjuk- och hälsosystem inom EU. I syfte att utveckla ett praktiskt tillämpbart ramverk som ska möjliggöra tillgång till och överföring av patientinformation mellan europeiska hälsovårdssystem har Kommissionen tillsammans med ett antal medlemsländer bildat projekt epSOS. Projektets avsikt är att personer bosatta inom EU vid tillfällig vistelse i annat deltagarland ska få tillgång till medicin eller vård på vistelseorten genom att utnyttja existerande eRecept eller patientjournaler i det egna försäkringslandet (country of affiliation). Projektets uppdrag är att arbeta fram lösningar för att möjliggöra en säker överföring av känsliga personuppgifter. Överföringen av patientuppgifter kommer att ske genom nationella kontaktpunkter (NCP), en per deltagarland, som ska säkerställa och kontrollera att överföringen sker mellan auktoriserade personer och inom säkerställda tekniska lösningar. Deltagarländer kan antingen fullgöra NCP-funktionen i egen regi eller ingå avtal med en fristående juridisk person. Detta avtal ska baseras på av projektet framtaget ramavtal ”Framework Agreement” (FWA) med justeringar för den egna nationella rätten.

Projektet har skapat tekniska lösningar för säkert utbyte av patientdata. Avsikten är att allt dataflöde inom epsos ska ske med hjälp av framtagna tekniska lösningar genom överföring mellan nationella kontaktpunkter (NCP). Förutom den tekniska lösningen ska säkerheten vid överföringen garanteras av att samtliga deltagande länder bygger upp snarlika system och med kontroller genomförda av projektet.

Europeiska kommissionen och deltagande länder har ingått följande avtal för genomförande av projektet.
1. Grant Agreement (GA) mellan Europeiska kommissionen samt Sveriges Kommuner och Landsting i egenskap av samordnare (coordinator) och medlemsländerna och övriga deltagare (beneficiaries). Avtalet fastställer de ekonomiska villkoren och det ekonomiska ansvaret för projektet.
2. Annex I - Description of Work (DOW) – Annex till GA som fastställer projektets mål och arbetsprocess.
3. Consortium Agreement (CA) mellan deltagande parter som utgörs av länder och organisationer, samtliga benämnda beneficiaries i GA som anger avtalsparternas rättigheter och skyldigheter, kompletterar GA och fastställer projektorganisationens uppbyggnad och beslutsordning.

[1] E-Health – making healthcare better for European citizens: An action plan for a European e-Health area. COM(2004)356(final)

Sverige har valt att överlämna NCP-funktionen till ett fristående bolag, Apotekens Service Aktiebolag som får i uppdrag att genomföra den svenska NCP-funktionen. Mellan Svenska staten och bolaget har upprättats ett avtal som reglerar förhållandet mellan parterna i anledning av uppdraget. Det svenska avtalet är baserat på projektets FWA med justeringar för svensk rätt vilket inneburit att vissa delar av FWA antingen uteslutits eller justerats för att avtalet ska överensstämma med svensk rätt. Det ingångna avtalet gäller till den 31 december 2013 vilket motsvarar projektets löptid.

Den 4 oktober 2013 beslutade epSOS generalförsamling att förlänga projektet t.o.m. den 30 juni 2014. Sverige har beslutat att delta i projektet under förlängningsperioden vilket kräver att en ny nationell kontaktpunkt upprättas för förlängningsperioden.

Apotekens Service AB har den xx(13?) december 2013 beslutat att försätta sig (term?) i likvidation den 1 januari 2014. Bolagets tidigare verksamhet kommer att överföras till Ehälsomyndigheten. Det är därför lämpligt att även uppdraget som nationell kontaktpunkt för projekt epSOS överförs från bolaget till den nya myndigheten.

Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of

Patient Summary and Electronic Prescription

D2.1.2 Legal and Regulatory Constraints on epSOS Design- Participating Member States

T2.1.2. Standard Contract Terms for MS Document for Engagement of Pilot Sites

January 31st, 2010

Final

Document Information

Project name	Smart Open Services – Open eHealth initiative for a European large scale pilot of Patient Summary and electronic prescription
Author/ person responsible	Zoi Kolitsi, Petra Wilson
Document name	D2.1.2 Standard Contract Terms for MS Document for Engagement of Pilot Sites
Status	in process | final draft | submitted to SC | approved | PUBLIC

Sub-Project Identification

Work Package	WP2.1. Legal and Regulatory Issues
T2.1.1. Analysis and Comparison	T2.1.2. Establishing Legal and Regulatory Framework for Field Trials
Document Owner	*Zoi Kolitsi*

Change History

Version	Date	Type of editing	Editorial
First Draft (ver.1)	Oct 31, 2009	First draft based on previous discussion papers	Petra Wilson, Zoi Kolitsi
Second Draft (ver.2)	Nov 18, 2009	Second draft incorporating comments from WP2.1.	Zoi Kolitsi
Third Draft (ver.3)	Nov 30, 2009	Third draft incorporating the decisions of the WP2.1 meeting Brussels 25_Nov_09	Zoi Kolitsi, Petra Wilson
Fourth draft	Dec 9, 2009	Semi final version -stable draft for comments	Zoi Kolitsi, Petra Wilson
Fifth Draft	January 15, 2009	Final version submitted to QA	Zoi Kolitsi
Final	January 31st	Amended after quality review	Zoi Kolitsi

Acknowledgments

The primary authors wish to thank the colleagues of WP2.1. that have contributed to the authoring of this deliverable. The ideas were developed through productive dialogue, comments and suggestions throughout the process of Task 2.1.2 and we particularly wish to thank the group of WP2 contributors Gerhard Brenner, Jan Cap, Javier Carnicero, Laurence Chamoin, Frederike Diersen, Jana Holland, Lena Jönsson, Karel Neuwirt, George Pangalos, Simone Paolucci , Alain Périé, Jan Petersen, Lars-Åke Pettersson, Cynthia Sanfilipp, Kristina Sykorova, Michèle Thonnet, Rod Tooher and Roberto Zuffada .

Table of Contents

Abstract
D2.1.2 Standard Contract Terms for MS Document for Engaging Pilot Sites is the second contractual deliverable of epSOS WP 2.1. It comprises an epSOS Framework Agreement, foreseen as the common base for establishing national contractual agreements in order to engage national pilot partners in the participating Member States to effectively operate the epSOS services on a pilot basis. The FWA will be used by each Member State to draft a contractual agreement which establishes a legal relationship between the Member State National Authority Beneficiary (NAB) and its epSOS National Contact Point (NCP). Signing of the FWA forms a contractual agreement between NCPs, through their representation in the PSB. The annexes to the Framework Agreement which form an integral part of the national contracts set out the core elements of (i) dealing with patient consent in epSOS and (ii) information regarding rights and responsibilities of patients and healthcare professionals participating in the epSOS trial. The legal approach and the context of application of the framework agreement is presented in the introductory chapters of this document.

Executive summary

In order to establish the framework of trust, the project partners have agreed the epSOS **Framework Agreement (FWA) and its related annexes** set out in Part II of this document. The FWA will govern the co-operative model of data exchange and form the documented basis for the trusted relationships between parties exchanging data. It will also serve as an aid to transparency, so that patients can be reassured that their legal rights to data privacy can be maintained in the cross border care setting. The core purpose of the FWA and its related annexes will be to establish the **epSOS Trusted Domain** which shall be perceived of as an extension beyond a certain national or regional territory where those national/regional ehealth services which are provided within epSOS can be delivered seamlessly to populations travelling to destinations that are "federated" in the epSOS LSP.

Part I of this document provides an overview of the approach and establishes the context within which this Agreement will become operational. The epSOS Framework Agreement itself in Part II is a blueprint which will be reviewed by all MS participating in the pilot and when acceptable it will be signed off by the project PSB. It must then be executed as a contractual agreement between the National Authority Beneficiary (NAB) of each MS which plans to host pilots.

The localization of the FWA is the responsibility of each MS working with its local legal experts and local epSOS teams. As part of this localization, each country will tailor the body of the FWA to create a contract to its own specificities and also its own commitments of piloting the epSOS services.

It is vital that such national contractual agreements are comparable across the whole project (i.e. across all pilot sites) and that they all satisfy the local and EU level legal requirements on issues such as patient consent, data security, patient confidentiality, practitioner liability etc. The existence of NCP contracts in each participating country which are all closely based on the FWA will ensure that collectively the NCPs can co-operate in a trusted domain to deliver their epSOS duties without the need to create direct NCP-NCP contracts.

The legal relationships between NCPs for the pilot phase are established indirectly through their associated National Authority Beneficiaries of the epSOS Grant Agreement. The PSB is the project function established through the Consortium Agreements that ensures that NCP responsibilities are fulfilled by a transparent and independent audit system to be also approved by the PSB.

All the contracts establishing the NCPs nationally and the NCP-HCO contracts will together form the legal basis for the delivery of the epSOS pilot services, since each contract establishing a NCP will contain a contractual obligation to co-operate with other duly established NCPs.

The FWA is to be complemented by D 3.8.2. "National Pilot Set-up and Deployment Guide" which should provide guidance for setting up National Contact Points and deploying the epSOS services at the national pilot sites.

This version reflects our current best knowledge of the challenges that Member States will face when establishing their national accountability framework and allocating responsibilities for running the epSOS pilot in the most beneficial way for the project and in full respect of patients' rights and national legislations.

Predicting all possible hurdles at this phase is not possible, partly because of the large variation of the national organizational environments that collectively address the relevant issues and partly because at this stage many important epSOS requirements have not been

established, such as service level agreements and epSOS services and service delivery specifications.

This document is however considered a sufficient basis for localization of this epSOS blueprint to the national situations. A possible update of this epSOS Framework Agreement will be considered before the launch of the pilots in order to align it to approved "deviations" which may emerge as necessities and have been deemed acceptable during the course of the national localisation experiences.

Definitions of concepts and key terms

Note: These set of definitions concern the usage of terms in this document. Where existing terms are considered insufficient for the purposes of this document they have been adapted accordingly. Explicit notifications to such changes have been provided.

Annex I of the Grant Agreement is annexed to the Grant Agreement and comprises the description of work which forms the contractual obligations taken up jointly by the Beneficiaries of the epSOS project, under the Grant Agreement.

Anonymous data in the sense of the Directive 95/46/EC can be defined as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual, including access to publicly accessible data (e.g. phone books).

Authentication Process to verify the claimed identity of a party before authorising a particular action to be performed.

Authorization Process by which entitlement of a requester, to access or use a given service, is determined.

Country A is the Member State of affiliation, i.e., the state where personal health data of an epSOS patient is stored and where he or she is insured. This is the country where the patient can be unequivocally identified and his or her data may be accessed. [Term from D5.2.1 adapted].

Country B is the Member State of treatment, i.e., where cross-border healthcare is provided when the patient is seeking care abroad. This is a country, different from country A, in which information about a patient is needed to support the provision of healthcare [Term from D5.2.1, adapted].

Data Controller shall mean the 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 [Dir 95/46/EC].

Data Processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the *Data Controller* [Dir 95/46/EC].

eDispensing is defined as 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). [epSOS D3.1.2]

End User is the user of epSOS patient data (e.g. Point of Care, Health Professional, Health Care Organisation, etc.).

ePrescribing is defined as prescribing of medicines in software by a health care professional legally authorized to do so, for dispensing once it has been electronically transmitted, at the pharmacy [epSOS D3.1.2]

ePrescription means a prescription for medicines or treatments, provided in electronic format. A prescription is understood as a set of data such as drug ID, drug name, strength, form, dosage, indication. [Term from D5.2.1, adapted].

epSOS design L&R requirements comprise input into the design of the epSOS services and system components and should normally be addressed fully within the epSOS implementation.

epSOS encounter is any healthcare encounter in country B that makes use of the epSOS services.

epSOS Grant Agreement is the legal contract (including its Annexes) signed between the European Commission and the *Beneficiaries* on the execution of the *epSOS project*.

Beneficiaries are the organisations that participate as partners in the *epSOS project*.

epSOS patients: They are citizens who will seek healthcare at an epSOS PoC and will receive epSOS pilot services. epSOS patients will fit under the following 5 broad categories of cross border mobility:

- temporary visitors abroad;
- people retiring to other countries;
- people in border regions;
- people sent abroad by their home systems (not currently available in epSOS)
- people going abroad to receive care on their own initiative.

epSOS Pilot Partners: Are the national and regional level organizations that enter into partnership in order to deliver the epSOS pilot through delivery of services and the epSOS evaluation. These will normally encompass the epSOS NCP and several local PoCs. Several entities may be established to provide core responsibilities of the NCP if the NCP is not able to fulfill all functions (e.g. national level and regional level co-ordinators).

epSOS Points of Care (PoC): This is a location where an epSOS citizen may seek healthcare services. It may be a hospital, a pharmacy, the practice of a registered healthcare professional or any other point of the health care system of country B, participating in the epSOS pilot. An epSOS PoC is designated as such by the participating Member States after having demonstrated its capacity to comply with the epSOS requirements.

epSOS Pilot Site: It is a cluster of Points of Care, typically with a geographical or an organizational affinity that are designated by a MS to participate in the epSOS large scale pilot. A pilot site can have any number of associated PoC.

epSOS trusted domain is an extension beyond a certain national or regional territory where epSOS ehealth services can be delivered seamlessly to populations travelling to destinations that are federated in the epSOS LSP. The epSOS trusted domain is comprised of epSOS NCPs and their national contractual partners which collectively fulfill all technical, legal and organisational requirements, for safe delivery of epSOS services and secure and confidential transfer or storage of data resulting from healthcare encounters as appropriate, within the epSOS Trusted Domain, according to this framework agreement. The epSOS trusted domain can only be established if compliance to epSOS requirements is secured by audit mechanisms and is supervised by the PSB.

Health Care Professional (HCP) is a person professionally qualified to deliver care; in epSOS the term is used as in Directive 2005/36/EC establishing rules for the mutual recognition of regulated professions. *epSOS Health Care Professionals* are designated HCPs within the epSOS PoCs that are entitled to deliver the epSOS services.

Health Care Organisation (HCO) is any legal entity having legal capacity that relies on the usage of personal health related data in order to fulfill tasks or business purposes notwithstanding whether those tasks have been delegated by law or not. In certain cases a sole practitioner HCP may be both HCP and HCO.

[Note: the acronym represents an adaptation of "HCPO- Health care Provider Organisation" defined in the initial scope and a replacement of the definition "An institution, authorized to provide health care services, unequivocally identified in the set of the Health Care Institutions" (epSOS D3.2.1)]

Health Care Provider is an organization or person who delivers proper health care in a systematic way professionally to any individual in need of health care services.

Identification Assignment of a unique number or string to an entity within a registration procedure which unambiguously identifies the entity. This number or string serves thereafter as an identifier uniquely attached to this entity. (i2-Health_D3.1_1.0)

Information Governance for the purposes of this deliverable is envisaged as incorporating all necessary policies and safeguards for the appropriate use of personal data within epSOS, needed to ensure that personal health information is dealt with legally, securely and to the greatest possible benefit to the epSOS patient in the two epSOS use cases.

Legal entity is an individual or organization which is legally permitted to enter into a contract, and be sued if it fails to meet its contractual obligations.

Legal and Regulatory (L&R) Issues are those issues that emerge from EU and national legal and regulatory frameworks and directly relate to the two epSOS use cases.

Legal and Regulatory profile of epSOS use cases is an integrated view of the legal and regulatory issues that relate to each step of the process in the encounter of a citizen of country A with a Point of Care (PoC) in country B.

Medical Record or *Health Record* is a systematic documentation of a patient's medical history and care. The term 'Medical record' is used both for the physical folder for each individual patient and for the body of information which comprises the total of each patient's health history. Medical records are personal documents and there are many ethical and legal issues surrounding them such as the degree of third-party access and appropriate storage and disposal. Although medical records are traditionally compiled and stored by health care professionals (HCP) and health care organisations (HCO) personal health records maintained by individual patients have become more popular in recent years. All data collected in medical records shall be regarded as sensitive personal data and processed accordingly.

Medication Summary is all prescribed medicine for which the period of time indicated for the treatment has not yet expired, whether they have been dispensed or not. It's a synonymous record of current medication. It contains the following information of each one: active ingredient, strength, pharmaceutical dose form, posology, route of administration, onset date of treatment and duration of treatment. [epSOS D3.2.1]. The medication summary is a part of the PS that can be consulted separately.

*National Contact Point (*epSOS NCP) is an organization delegated by each participating country to act as a bidirectional technical, organisational and legal interface between the existing different national functions and infrastructures. The NCP is legally competent to contract with other organisations in order to provide the necessary services which are needed to fulfil the business use cases and support services and processes. The epSOS NCP is identifiable in both the epSOS domain and in its national domain, acts as a communication gateway and establishes a Circle of Trust amongst national Trusted Domains. The epSOS NCP also acts as a mediator as far as the legal and regulatory aspects are concerned. As such an NCP is an active part of the epSOS environment if, and only if, it is compliant to normative epSOS interfaces in terms of structure, behaviour and security policies.

Participating Member States are the MS' that, according to PSB approval and audit, have met the criteria for joining the epSOS Trusted Domain. They may be MS currently participating in

the project or new MS that have expressed an interest and follow up closely the developments through the CALLepSO NA-SIG (National Authorities Special Interest Group).

Patient consent provided to the data controller or processor means any freely given explicit and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed for a given purpose.

Patient Summary should be understood to be a reduced set of patient's data which provides a health professional with essential information needed in case of unexpected or unscheduled care or planned care [D3.2.1.].

Personal Data is any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [Dir 95/46/EC]. Personal data includes written data, images and audio data stored on any time or medium.

Processing of personal data ('processing') means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction [Dir 95/46/EC].

Restrictions are epSOS constraints that could have implications on the pilots and they will normally concern transactions which will not be allowed to take place. They will be addressed within the drafting of the Recommendations (D.2.3).

Safeguards are primarily measures to be taken during the pilot operation. They shall aim to establish a condition of trust not only amongst epSOS NCPs but they reach down to the level of Points of Care (PoCs) that the mobile citizen will come into contact with. These measures must be implemented by the pilots and they will form a consistent set of requirements reflected in the standard contract terms (D.2.2.). Safeguards will also include special measures for the running of the pilots.

Trust Framework means an integrated framework detailing how trusted relationships may be best implemented between epSOS NCPs at the European interoperability level and incorporating standard legal requirements including those for audit mechanisms to be developed at EU level.

Abbreviations

DPC	Data Protection and Confidentiality
DPD	Personal Data Protection Directive (95/46/EC)
EC	European Commission
EHR	Electronic Health Record
epSOS	epSOS (Smart Open Services for European Patients)
EU	European Union
FWA	Framework Agreement
HCO	Health Care Organisation
HCP	Health Care Professional
CA	Consortium Agreement
IG	Information Governance
L&R	Legal and Regulatory
LSP	Large Scale Pilot
MS	Member State
NA	National Authority
NAB	National Authority Beneficiary
NCP	National Contact Point
PCP	Pilot Co-ordination Point
PD2	Project Domain 2 (Legal and Regulatory Issues)
PoC	Point of Care
PS	Patient Summary
PSB	Project Steering Board established in accordance with Section 4. of the epSOS Consortium Agreement
UC	Use case
WP	Work Package
WP29	Article 29 Data Protection Working Party

Part I - General Information on the epSOS Contractual Agreements Framework

1 Introduction

epSOS is a Large Scale Pilot (LSP) that operates within a complex policy background and focuses on electronic patient record systems, with an initial focus on two cross-border services, i.e., Patient Summary and e-Prescribing/e-dispensing. The aim of the pilot is to demonstrate that it is feasible for any Member State (MS) that already provides these eHealth services to its residents, to create the conditions that will allow it to also offer these services to them when they travel abroad to other Member States taking part in the epSOS pilot.

epSOS has been conceived as a pilot involving initially 10 MS and has been designed to be comprehensive, robust and universally accepted across professions and cultures. The project is also foreseen as a starting point and a stimulus for further cooperation on eHealth development in Europe going well beyond the first two cross-border pilot services between the MS involved in epSOS.

It is important to note that the epSOS services involving Patient Summaries and e-Prescribing/e-dispensing will be offered on a pilot basis and the intention is to gather data and learn from this pilot operation to accelerate wider deployment of these services. The pilots will test the feasibility and acceptance of the overall technical and legal interoperability of the proposed solutions. It is also important to clarify that it is a basic principle of epSOS that the proposed implementation will establish conditions of interoperability of current national solutions. In the same way it is the objective of the project to develop a modus operandi of interoperability between existing legal and regulatory frameworks, rather than to propose new or amendments to existing legislation.

While the long-term operation of the services is out of scope of epSOS the project shall produce and deliver practical guidance and recommendations on how to make the transition from the pilots to normal operation. Therefore, in the short term, the epSOS evaluation will examine the design, development, implementation and operation of the two cross-border interoperability pilot services which constitute the core of epSOS, i.e., Patient Summary, ePrescription and e-Dispensation. In the longer term, it will estimate and forecast the impact that epSOS may have on eHealth in Europe and provide recommendations for further development of cross-border eHealth, including recommendations on any legal and regulatory interventions which may be required for expanding to new cross-border eHealth services and new countries.

The exchange of data which lies at the heart of the epSOS pilot requires that a sound framework of trust is developed between all parties. The framework must ensure that healthcare professionals can rely upon the authenticity of the clinical data on which they will base decisions, that suitable systems of security exist to ensure that data cannot be accessed by unauthorized parties, and that patient rights according to national legislations are e.g. the right of informed consent to data access are duly respected by all parties (authenticity, integrity and confidentiality).

What is federated in epSOS is a number of clinical sites (Points of Care) in epSOS countries (B) where residents of a different country may expect care based on access to their clinical information held in their home country (Country A). There will be numerous such sites and the number of those joining the "confederation" may grow throughout the deployment phase. Due to the potential number of pilot sites, therefore, it is not feasible to build confidence in the epSOS system on a one to one basis. This must instead be established at country to country level. Once a country has become a member of the epSOS trusted domain it can bring on board more and more health care providers, once they have demonstrated conformance to the epSOS requirements according to the NCP and as verified

by audit. Each epSOS country is responsible for the conduct and service quality and conformity to epSOS standards towards the rest of the epSOS community.

A "country" in epSOS is represented by one single legal entity, which then assumes all legal duties and is contractually bound to safeguard the epSOS trusted domain in terms of all national matters. This legal entity is referred to as the **National Contact Point (NCP)**.[1]

The NCP is the focal point. The NCP is a legal entity who is legally competent to contract with other organizations on its territory in order to collaboratively carry out its duties and responsibilities in epSOS, as appropriate in each member state. The NCP will also contract with epSOS health care organisations to provide epSOS services to patients.

The NCP together with its national contractual partners shall collectively fulfill all technical and organisational requirements for secure and confidential transfer or storage of data resulting from healthcare encounters as appropriate, within the epSOS Trusted Domain, according to this framework agreement.

The NCP in each country will also assume the responsibility of ensuring that patient rights according to their national legislation, are appropriately handled and that all epSOS HCPs and designated parties in HCOs are trained with respect to their epSOS duties.

The epSOS NCP takes care of both external and internal - national communication in the epSOS project and the semantic mapping between information on either side[2]. It is therefore at this level that the epSOS Trusted Domain may be established. The epSOS NCPs will be furthermore responsible towards all MS partners in epSOS for securing that the needed processes are properly implemented at their own networks which will be typically points where care is delivered.

In order to establish the framework of trust, the project partners have agreed the epSOS **Framework Agreement (FWA) and its related annexes** which is set out in Part II of this document. The FWA will govern the co-operative model of data exchange and form the documented basis for the trusted relationships between parties exchanging data. It will also serve as an aid to transparency, so that patients can be reassured that their legal rights, including those to data privacy can be maintained in the cross border care setting. The core purpose of the FWA and its related annexes will be to establish the **epSOS Trusted Domain** which shall be perceived of as an extension beyond a certain national or regional territory where those national/regional eHealth services which are provided within epSOS can be delivered seamlessly to populations travelling to destinations that are federated in the epSOS LSP.

From a legal perspective, this means that MS, through their delegated national organizations (NCPs), will enter into national multi-lateral contractual arrangements with HCOs, based as closely as possible on the Framework Agreement as local legislation allows. It is vital that such contractual agreements are comparable across the whole project (i.e. across all pilot sites) and that they all satisfy the local and EU level legal requirements on issues such as patient consent, data security, patient confidentiality, practitioner liability, etc.

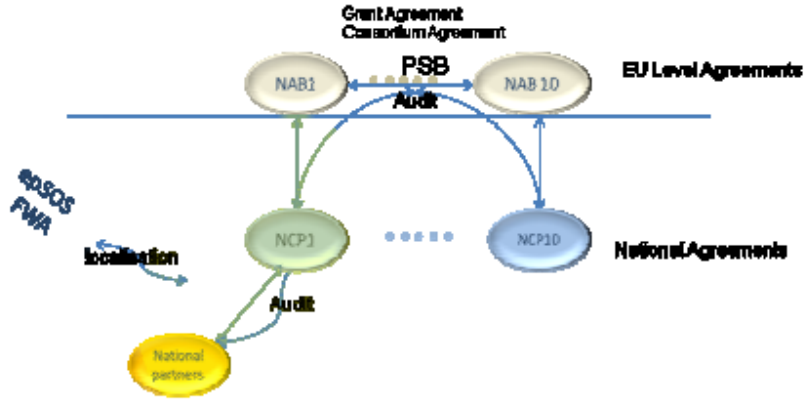
[1] In the present pilot configuration countries with regional devolved administrations have decided to be represented by a single NCP.

[2] See Annex I and epSOS Initial Scope.

2 The Application of the epSOS Framework Agreement

The epSOS Framework Agreement is intended as the common base for two levels of national agreements in order to establish the NCPs and allow the creation of NCP/HCO relationships.

It is envisaged that the contracts creating the NCP in each MS will be based very closely on the FWA. The existence of national NCP contracts in each participating country which are all closely based on the FWA will ensure that collectively the NCPs can co-operate in a trusted domain to deliver their epSOS duties without the need to create direct NCP-NCP contracts.



Once the NCP is established in a MS it will in turn create contracts with HCOs and other organisations as needed, to deliver the epSOS services which will again be closely based on the terms set out in the FWA.

The legal relationships between NCPs at EU level for the pilot phase are established indirectly through their associated National Authority Beneficiaries of the epSOS Grant Agreement. The PSB is the project function established through the Consortium Agreement that ensures that NCP responsibilities are fulfilled by a transparent and independent audit system to be also approved by the PSB.

The epSOS legal approach, described in D2.1.1, envisages that the operation of pilots will become possible through use case specific safeguards for the protection of patients rights, including those for processing of health information with proper balancing of patients' and public health interests that should be guaranteed by all pilot sites. Safeguards are primarily measures to be taken during the pilot operation not only by the NCPs but also by the PoC that the mobile citizen will come in contact with.

Given these expectations we foresee broadly two sets of requirements for PoC: (i) to put in place appropriate measures (processes and procedures, including security measures and safeguards) and (ii) to maintain records and reports demonstrating compliance to such measures, to be used for traceability and audit purposes. Such audit will be external and will involve the NCP. A data protection audit aims at identifying non-compliance issues and detecting weaknesses in data protection management processes applied by HCPs and PoC; and maintaining and ensuring compliance with relevant data protection principles required by the Directive. The security policy will be approved, implemented and periodically audited by epSOS partners represented by the PSB, through an independent party, e,g, through a contracted auditor.

WP3.8. will elaborate guidance on audit practices. At the organizational level, these requirements should be considered in the definition of the necessary procedures for health data exchange between the MS' healthcare organizations and the role of the NCPs. This should be done in a generic way, without imposing specific procedures to the MS, but still setting a basis for mutual recognition and acceptance. In this task the relevant activities of European Standardisation Committee (CEN) and its Workshop Agreements on Personal Data Protection Audit Framework[3] should be consulted. These documents as well as documents issued by some data protection supervisory bodies will be carefully analysed and use as baseline to set up epSOS' Data protection auditing procedures.

The FWA therefore constitutes a contractual agreement between NCP-PSB that allows independent audit and conformance to the FWA. The PSB role as primary arbitrator between NCP (see section 2.2) allows the PSB to act as mediator but also enables the PSB to adopt epSOS performance standards and allow or control variations to FWA.

The collectivity of all the relationships between the NABs at international level as well as the NABs- NCPs and the NCP-HCO nationally will together form the legal basis for the delivery of the epSOS pilot services.

2.1 Establishing National epSOS relationships

A Framework Agreement (FWA) setting out the core tasks and duties of an epSOS NCP is attached in part II of this document. Where required[4], the FWA will be used by each Member State to draft a contractual agreement which establishes a legal relationship between the Member State National Authority Beneficiary (NAB) and its epSOS NCP. Through this agreement the epSOS NCP will establish its duties and responsibilities towards the project in terms of proper execution of the pilot.

The epSOS Framework Agreement in Part II is a blue print which will be reviewed by all participating MS and when acceptable it will be signed off by the PSB. It must then be executed, where necessary as a contractual agreement, between the national authority of each MS which plans to host pilots and the NCP. The contract shall be very closely based on the FWA, but will be localized to comply with national legal and professional requirements.

The annexes to the Framework Agreement set out the core elements of (i) dealing with patient consent in epSOS and (ii) information regarding rights and responsibilities of patients and healthcare professionals participating in the epSOS trial, which should be made available to all such individuals and duly supported by the NCP.

The Framework Agreement and its Annexes, after approval by all Member States participating in the epSOS pilot and its release by the PSB, will therefore become the blue print for the arrangements between National Authorities and epSOS NCPs and their collaborating national pilot partners. The FWA is complemented by D 3.8.2. "National Pilot Set-up and Deployment Guide" which provides guidance for setting up National Contact Points and deploying the epSOS services at the national pilot sites[5].

---

[3] CWA 15499/2006 Personal Data Protection Audit Framework (EU Directive EC 95/46); and CWA 15262/2005 Inventory of Data protection auditing practices

[4] Some member states may not need to establish NCPs by contract if, for example, the national administration provides the service itself.

[5] Expected April 2010

The localization of the FWA is the responsibility of each MS working with its local legal experts and local epSOS teams. As part of this localization, each country will tailor the body of the FWA to its own specificities and also its own commitments of piloting the epSOS services.

All localisation of the FWA must however foresee specific actions and measures in order to implement the pilot:

(i) The epSOS Security Policy[6] with the aim to create a secure operational environment for the pilot service deployment which will be sufficient for protecting the epSOS data and processes, implementable and agreed by all participants. The epSOS security policy provides a secure operational environment for epSOS and is fundamental in establishing the 'circle of trust' among epSOS actors. The security policy will be approved, implemented and periodically audited by all epSOS partners. As such, it shall also provide means of proof and essential checks which give users trust in the given information.

(ii) The epSOS Pilot Strategy, [7] approved by the PSB. The governing principles of how the pilots will be operationalised will be developed and approved as an epSOS level activity to a sufficient detail to provide legal certainty for epSOS NCPs in undertaking such commitments towards epSOS.

(iii) Specific processes, procedures and audit practices which are central to the delivery of the epSOS services to mobile citizens at PoC and at the epSOS NCPs will be developed as part of epSOS WP3.8 and WP 4.2A and B activities.

2.2 Dispute Resolution during the course of the epSOS pilot

It is possible that in the execution of the epSOS pilot, a patient may suffer harm, or that disputes may arise between NCPs as to responsibility or liability for an act, omission or mistake occurring in the operation of the pilot.

Harm to Patients

An epSOS patient who suffers harm while receiving epSOS services abroad, must report and address the issue to the PoC where the harm occured. If the patient or the HCO at the PoC so requires NCP A is obliged to instigate an incident report related to epSOS service performed and NCP B is obliged to fully cooperate. The report shall be given regardless of the patient or the HCO request; no motivation should be required. Both the HCO and the patient are entitled to full information stating summary and conclusion. The official report from NCP A must be clear and consistent if the case is to be brought to court.

According as insofar as an act, omission or mistake causes harm to a patient (real or perceived) the patient shall be entitled to exercise his or her rights in the usual way. This will mean that in most cases the patient will exercise his or her rights in the country where the harm occurred in accordance with Council Regulation (EC) No 44/2001, which states that generally jurisdiction is to be exercised by the Member State in which the defendant is domiciled.

Disputes between NCPs

There will be no formal EU level contractual arrangements between NCPs in the participating Member States. The relationship between the NCPs is deemed to be already sufficiently covered by the epSOS Grant Agreement which has been signed between members of the

[6] epSOS Security Policy in D 3.7.2., "Security Services Specification Definition", Dec 2009
[7] epSOS Pilot Strategy, TF, December 2009

Consortium and the European Commission. This Agreement foresees the obligations of the beneficiaries to execute the epSOS Large Scale Pilot according to the Technical Annex and in respect of applicable national legislations.

The epSOS beneficiaries have specified and supplemented, between themselves, the provisions of the Grant Agreement by means of a Consortium Agreement (CA), which is a legal agreement between its signatories. This CA specifies the organisation of the work between and to be delivered by the Parties, supplements the provisions of the Grant Agreement concerning Access Rights and sets out rights and obligations of the Parties. Start, duration and termination of this Consortium Agreement are identical to the time schedule set by the Grant Agreement. Rules for premature termination are also described (Section 15 of the CA).

Section2.2 of the CA, defines the composition and powers of the Project Steering Board (PSB). The PSB is composed of one duly authorised high-level representative appointed by and from each National Authority participating in epSOS. The PSB is the highest decision making body in epSOS and amongst other duties described in section 4.1.2. of the CA the PSB is in charge of drawing up rules for the participation of new beneficiaries and deciding on any Proposals (4.1.2.e) and conflict resolution when the course of the Project is endangered (4.1.2.f).

The PSB shall act as a primary arbiter of any disputes arising between NCPs. In cases where it proves impossible to settle a dispute between NCPs in the PSB the CA foresees recourse to the European Court of Arbitration in Paris under the rules of arbitration of the International Chamber of Commerce.

2.3 Changes and Updates of the FWA

The current version of the FWA reflects the best current knowledge of the challenges that Member States participating in the pilot will face when establishing their national accountability framework, and allocating responsibilities for running the epSOS pilot in the most beneficial way for the project and in full respect of patients' rights and national legislations.

Predicting all possible hurdles at this phase is not possible, partly because of the large variation of the national organizational environments that collectively address the relevant issues, and partly because at this stage many important epSOS requirements have not been established, for example Service Level Agreements and epSOS services and service delivery specifications.

This document is however considered to be a sufficient basis to engage National Authority beneficiaries into the process of localization of this epSOS blue print to the national situations. Over the next months leading to the launch of the pilot operation, WP2.1. will undertake the task to support Member States in this process, follow up on progress and resolve issues as they arise. Any new elements or needed amendments to this FWA that will emerge a result of this interaction, will be reflected in a possible new version of this deliverable, if necessary, that will be submitted at the end of the site level preparation phase. To quote the external epSOS review panel "epSOS will be remembered by its deliverables" therefore closing the gap between theory and practice. A second edition of the deliverable is considered a necessary additional step not currently foreseen in the Technical Annex.

2.4 Contractual relations beyond the project life time

The epSOS approach described above, based on the designation of NCPs as legal entities with specific duties for the project, relies on an internal mechanism of governance based on guidelines, and represents an adequate solution for offering the epSOS services on a **pilot** basis by a legal EU level entity being the epSOS consortium. The Grant Agreement and its associated Consortium Agreement provide an adequate contractual basis for solving disputes and non compliance to agreements made within the project. Through this approach the project will create accountability of each MS participating in the pilots to prepare appropriately for the epSOS pilot phase, i.e. set up its epSOS NCP and carry out their pilot operations.

This mechanism is however, not sustainable after the end of the project and will need to migrate to a permanent mechanism if the services are to be widely deployed and offered on a routine basis. A useful example can be found in the social security area where there is a legal basis for disputes settling (based Regulation (EC) No 883/2004 of The European Parliament and the Council)[8] and an official body driven by MS has been established. Reference guidelines have been (successfully) used for security questions. Also in the IDABC framework, the MS are the driving force and the European Commission is the facilitator[9]. The present approach with the PSB serving the role of "European Arbitration Service" during the pilot can provide an appropriate ground for further exploration in this direction.

It should however be kept in mind that epSOS operates in an EU environment of Directives rather than Regulations, the implications being that Directives are not directly applicable but transposed into national laws, and thus variations in the transposition of a Directive often arise. Therefore, the establishment of a formal dispute settlement body for eHealth related issues might require national legal adaptations.

These issues will be addressed as part of D2.1.3 (Recommendations), due at the end of the project. The recommendations should include a proposal for the establishment of a European arbitration service as a prerequisite to taking the epSOS services to full deployment.

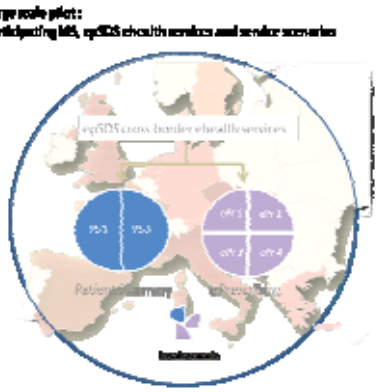
[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:284:0001:0042:EN:PDF
[9] http://ec.europa.eu/idabc/en/document/3473#finalElF

3 Context of Application of the Framework Agreement

3.1 Establishing the epSOS large scale pilot

The epSOS Large Scale Pilot (LSP) is a practical EU level implementation of the two epSOS services in a real life setting. The epSOS LSP presently involves 10 Member States that are working together to establish an epSOS trusted domain involving a number of their local healthcare providers (referred to as epSOS Points of Care (PoC)), together with National Contact Points, in the pilot delivery of these services to patients from other countries.

The epSOS LSP will consist of the pilot delivery of two epSOS ehealth services: *A Patient Summary service* and *an e-Prescribing/eDispensing service.* The workflows of these services are composed of a number of steps or components which in epSOS have been named "scenarios". The configuration of epSOS services to be offered by each Members State is defined by the MS itself. Nevertheless, a local healthcare organisation affiliated to the large scale pilot as an epSOS PoC is expected to be able to execute a sensible and useful service for travelling patients by being able to fulfill a selection of the situations described below:



- ePS1: a treating physician/pharmacist in country B will be provided access to available Patient Summaries/eprescriptions of foreign visitors in the process of providing care to them.
- ePS2: the NCP in country A will receive a request and will make accessible a patient summary of a patient receiving care abroad.
- ePr/eD1: the NCP in country A will receive a request and will make accessible all available prescriptions of a patient receiving care abroad
- ePr/eD2: a treating physician/pharmacists in country B will be provided access to available e-prescriptions of foreign citizens in the process of providing care to them
- ePr/eD3: a pharmacist in country B will send information about the medicines dispensed to the country of affiliation of the foreign visitor
- ePr/eD4: the [national NCP name] will receive send information about the medicines dispensed to a patient receiving care abroad

3.2 Actors and Stakeholders in the epSOS large scale pilot

There are a number of legal entities assigned specific roles in the Large Scale Pilot. The epSOS large scale pilot actors and stakeholders are described below.

1. **Participating Member States:** Are the MS that have met the criteria for joining the epSOS Trusted Domain. They may be MS currently participating in the project or new MS that have expressed an interest and follow up closely the developments through the CALLepSO NA-SIG (National Authorities Special Interest Group)
2. **epSOS Pilot Partners:** Are the national and regional level organisations that enter into partnership in order to carry out the epSOS pilot delivery of services and the epSOS evaluation. These will normally encompass the epSOS NCP (or other national

organizations that will collectively carry out the NCP duties and responsibilities) and Health Care Organisations, ie several local PoCs.

3. **epSOS Points of Care:** are locations where an epSOS patient may seek healthcare services. It may be a hospital, a pharmacy, an emergency vehicle, the practice of a registered healthcare professional or any other point of the health care system of country B, participating in the epSOS pilot. An epSOS PoC is designated as such by the participating Member States after having demonstrated its capacity to comply with the epSOS requirements and have entered into contractual Agreements with the NCP.

   a. **epSOS Health Care Professionals (HCPs):** are designated healthcare practitioners within the epSOS PoCs that are entitled to deliver the epSOS services after e.g receiving proper orientation into epSOS and its specific processes and procedures.

   b. **epSOS patients:** are the mobile citizens who will seek healthcare in one of the epSOS PoC and will receive epSOS pilot services. epSOS patients will fit under the following 5 broad categories of cross-border mobility:

      - temporary visitors abroad;
      - people retiring to other countries;
      - people in border regions;
      - people sent abroad by their home systems (not currently available in epSOS) and
      - people going abroad seeking health care on their own initiative.

3.3 Phases of the Large Scale Pilot

The need for prior establishment of trust is fundamental to the realisation of the pilot.

A major constraint in epSOS is that we cannot commit health care organisations before the needed degree of clarity on their obligations (both legal and organisational) exists. Accordingly, the project will adopt a step by step approach to building the trusted domain:

(i) through an initial collection of intent, epSOS WP4.1. has identified an initial number of national pilot sites which present a clear cross-border business case (Form A)

(ii) the design and specification of the epSOS clinical workflows (WP 4.2 A and B, WP1.2), including parameters and indicators to be assessed in the evaluation of the pilot as well as the procedures to be applied during the evaluation shall ensure sufficient mechanisms for appropriate level of involvement of end users

(iii) during the course of the project, the pilot participation is expected to increase by (a) Member States increasing their own participation in the large scale pilot during the piloting phase; (ii) by inviting additional MS to participate in the epSOS pilot. The initial and subsequent enrollment of national health care organizations will be subject to approval by the PSB.

The Pilot Strategy foresees that national pilot preparations should take the form of a "national project" associated to epSOS, with activities, responsibilities and allocated resources which will be reflected in a document describing the characteristics of the national design and organization of the participation in the epSOS large scale pilot and will reflect preparedness for launching of the services. Each Member State's pilot preparation document will be formally submitted to the PSB for approval. Amendments to the document to reflect additional participants as part of the pilot scalability will be also submitted and approved by the PSB.

The template of this document will be proposed by the epSOS Pilot Strategy Task Force and it will broadly contain:

- Information on the business case pursued, detailing services and scenarios to be piloted as well as type and volumes of cross-border mobility. Such information should be supported by relevant statistics as well as forecasts for contribution to the evaluation sample of epSOS by applying the proposed simulations.
- Information on the organizational, technical and human resources committed to the pilot operation.

3.4 Patient Consent

Patient Consent is the "*freely given specific and informed indication of the patient's wishes by which s/he signifies his agreement to personal data relating to him being processed*". This definition is laid down in Art 2(h) of the Data Protection Directive (1995/46/EC), referred to hereafter as DPD. [10] In transposing the DPD, Member States have introduced or enhanced national systems for regulating access control to patient information, as part of establishing their national trusted domain in ehealth. Such rules typically address the need to establish that access to patient data is limited to accredited healthcare professionals; that access is requested in the context of a care relationship with the patient; and that the requested information verifiably concerns the specific patient. In conformance with the DPD, such systems will also contain rules concerning the nature of information which may be collected and the purposes for which it may be processed - generally the rule is that only data relevant to the care of the patient may be collected and that they may only be processed for patient care. The DPD and national legislation do however provide some exceptions to this rule which allow that certain data may be collected and processed for the purposes of running an efficient and effective health service, and for treating patients when it is impossible to obtain consent, for example where the patient is unconscious.

The European level legislation also gives certain rights to the patient, such as knowing which data are stored and to be given access to the data in order to check that the data are correct and to demand correction of any incorrect data or deletion of any data which the patient does not want to have stored and such data is not necessary for health care purposes.

It is important to note however that there are some significant differences in the transpositions of the Data Protection Directive. There are, for example, differences in the interpretation of 'specific and informed consent'. Some countries allow such consent to be implied from the patient's presence in a consulting room, while others require explicit consent, including written consent. Similarly, some give the patients the right to explicitly restrict or limit access to their information or certain categories of information. For example, a patient may be entitled to exclude certain health care providers or categories of health care providers or certain documents or categories of documents from the healthcare record.

Irrespective of the national approach for consent for creation of a personal data record and access to this information by HCPs within the member state, access to this data from abroad will be executed in accordance to Article 29 WP recommendations in an opt-in mode. This is illustrated taking the example below:

[10] Given that this is a rather precise formulation which has been further clarified in the recitals of the Directive as well as in subsequent opinions of the Data Protection Working Party, the definition and handling of patient consent is not expected to vary significantly across Member States.

In Sweden, consent is provided at the PoC only for adults who are able to provide consent; national law does not require explicit consent in country A prior to processing, due to article 8.3 of the Directive, which is implemented into Swedish national law; " Paragraph 1 (of Article 8 DPD) shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy." The Swedish model for a nationwide PS is created with an "opt out" model.

When a Swedish citizen is being treated in another country, the patient consent will be verified at the point of care in country B. This means that explicit consent is given at the PoC in country B before processing data between NCP A and NCP B takes place, and it is verified by NCP A and interpreted accorded to national law.

3.5 Information on epSOS duties for Patients and Healthcare Professionals

epSOS services will be implemented and delivered on a pilot basis. Parties participating in the pilot must be duly informed of the special conditions on the basis of which these services are offered, and their rights and responsibilities as participants to these trials.

The patient will be informed on the aims of the epSOS LSP, how his/her patient data will be used, on his/her rights and any other circumstances of the processing of his/her data for the epSOS LSP purposes. The patient will be also informed that that his/her consent is free without any consequences if the consent will not be given, and that the collection and further processing of patient's health data solely for providing medical services is a subject of legislation of a country in which medical care is provided.

This core information text is drafted as part of Annex III of the FWA and will be localised in each country, preferably as an addendum to the national standard information provided to patients for acquiring Consent. The information will reside in the epSOS NCP(A) and will be made available as needed to the patient when s/he is in country B.

epSOS healthcare professionals will be called to treat patients from abroad that may have an electronic Patient Summary available in their country of affiliation and which will be made available to them to consult. It is imperative that they understand that the primary application of this Patient Summary is to provide them with a dataset of essential and understandable health information to deliver safer patient care. Furthermore to understand its "value" as a clinical tool i.e., what the Patient Summary is and what it is not, and how it was created.

An important element that needs to be addressed is to clarify that the epSOS patient summary contains only information residing in the country of origin. However, it is possible that more recent health record data has been created in another country. In this phase of the pilot, such information is not used to update the epSOS Patient Summary.

Associated to patient safety is also the need to appreciate that if the patient has decided to hide information in his country, this hidden information will not appear in the epSOS dataset. It has been considered that revealing which types of information have been masked impinges on privacy, therefore there will not be any kind of flag in the PS to alert of this fact.

The health care professional (HCP) must be informed that accepting to offer the epSOS services does not alter obligations to the legal requirements of the country in which s/he

exercises his/her professional practice in order to provide medical services to the epSOS patient. This means that the scope and categories as well as the relevance of personal data (including sensitive data) which the health care professional requires to be collected in the foreign patient's health record created in country B, will fall under the relevant legislation of the country in which the professional practice or Health Care Organisation (HCO) is legally established and operates.

The HCPs that participate in the LSP may use the epSOS e-services to receive health information, related to the patient, from the patient's country of affiliation according to their judgment and complement it with all other needed information collection. The use of these services is therefore not compulsory.

4 Planning Considerations

The localization process should start immediately after approval of the FWA by the PSB and be finalized in good time to allow its operationalisation in each country before the launch of the pilots expected in January 2011.

During this period, WP2.1. will revert to supportive mode and will (i) accept questions and requests for clarifications and provide advice to national teams; (ii) review national solutions and approaches and (iii) follow up on progress. The WP2.1. team will meet three times between January and September 2010 in approximate 3-monthly intervals.

At the end of the localization phase, WP2.1. will issue:

- A recommendation to the PSB for approval of the national approaches
- An amended version of the FWA if necessary.

The process of localization will be followed by any new member state that wishes to join epSOS in the pilot phase. Such localization will be reviewed by WP2.1. and will be approved by the PSB upon recommendation by it.

The diagram in figure 1, depicts major milestones during the next year, associated with development phases of the project.

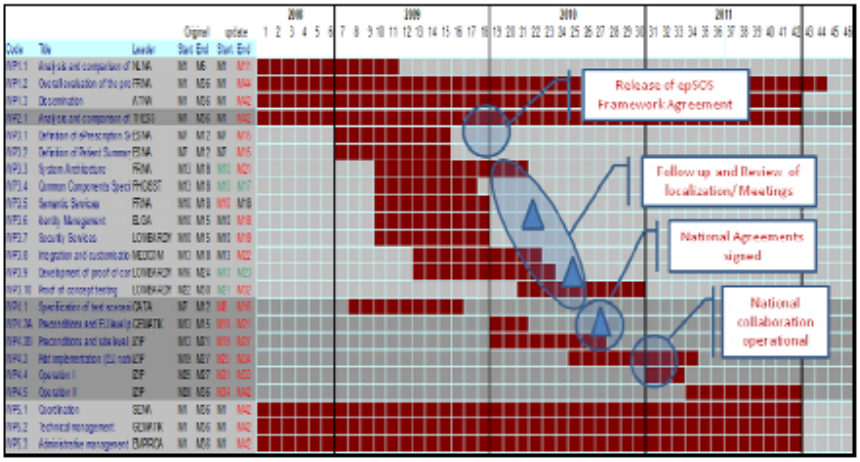


Figure 1. Localisation milestones, associated with development phases of the project.

Part II - epSOS Agreements Framework

Framework Agreement

on

National Contact Points

in the context of the

European Patients' Smart Open Services Project (epSOS)

Preamble

- The epSOS Large Scale Pilot Project has been established to develop and test a pilot system of cross-border data sharing to support patient care delivered to European citizens outside their usual state of residence by means of a shareable electronic patient summary and prescription.
- The Framework Agreement and its annexes is designed to establish the necessary level of trust to ensure that healthcare professionals 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.
- This Framework Agreement provides a blueprint for national level contractual agreements, where required[11], to create a National Contact Point [hereinafter NCP] as a legal entity entitled to process patient data in the context of the epSOS pilot.
- The Framework Agreement also sets out the core duties of the NCP and its partners so that the NCPs, once created, may contract on a common basis with their local partners (healthcare organisations, healthcare professionals and points of care) to deliver the epSOS services to patients.
- The Framework Agreement has 2 annexes which give further guidance on the information to be given to Patients and Healthcare Professionals on their rights and duties within epSOS.
- The articles of the Framework Agreement and its annexes shall be transposed into:
  - (where necessary) Contracts under applicable national law to establish epSOS NCPs
  - (where necessary) Contracts under applicable national law to designate points of care from within existing healthcare provider organisations as epSOS Points of Care
- The terms of this Framework Agreement and its annexes may be modified during transposition into local contracts and guidelines only in so far as it is necessary to do so in order to comply with local law or custom.
- The contractual agreements established at national level to create the NCPs shall be certified as conformant to epSOS principals by the Project Steering Board.

[11] Some member states may not to establish NCPs by contract if, for example, the national administration provides the service itself.

1. **The epSOS pilot – Creation of the epSOS National Contact Point (NCP)**

1.1. The epSOS pilot is an initiative of several European Member States to develop and test a system for access to health data in cross-border situations to support patient care delivered to European citizens outside their usual state of residence by means of a common epSOS electronic patient summary and a common epSOS e-prescription and e dispensation.

1.2. The national and regional Departments of Health and their related eHealth competence centres are beneficiaries of the Grant Agreement number 224991 of the European Commission and parties of its associated Consortium Agreement.

1.3. In accordance with the Grant Agreement the beneficiaries have contracted with the European Commission and each other to ensure that a number of healthcare establishments within their territory will provide one or more test sites for the epSOS Pilot – hereinafter known as a healthcare organisation [HCO]. An HCO may comprise one or more points of care [PoC] or be responsible for one or more points of care.

1.4. Each participating country shall appoint one legal entity to act as NCP. Where this function is federated across several organizations one entity shall act on behalf of the others to be the liaison point for NCPs from other epSOS Countries.

1.5. In the case of regional beneficiaries one NCP will represent all regional beneficiaries[12].

1.6. The NCP in each MS shall be created under local law on the basis of the present framework agreement.

2. **Core Characteristics of the epSOS National Contact Point (NCP) (Terms to be included in all national contracts relating to epSOS)**

2.1. The NCP shall be a legal entity who is legally competent to contract with other organizations in order to collaboratively carry out its duties and responsibilities in epSOS.

2.1.1 The NCP shall contract with epSOS health care organizations to provide epSOS services to patients.

2.2. The epSOS NCP 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 epSOS use cases (see end note).

2.3. The NCP 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 NCP shall:

2.3.1. be technically competent to provide a gateway for epSOS information transfer;

2.3.2. be legally recognised as a data controller or data processor in accordance with domestic data protection legislation;

2.3.3. be legally competent to execute contractual agreements with all domestic partners in compliance with domestic data protection legislation;

2.3.4. be legally competent to enforce audit and corrective action emerging from audits;

2.3.5. be technically competent to validate the identity of patients and patient consent of its territory (acting as country A);

2.3.6. maintain the local versions of the epSOS semantic value sets.

3. **General Duties and responsibilities of the epSOS NCP (terms to be embodied in the national contracts creating the NCPs)**

3.1. The epSOS NCP shall establish appropriate security and data protection systems to conform to epSOS requirements as well as all applicable national requirements.

3.2. The epSOS NCP shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).

3.3. The epSOS NCP shall establish an appropriate system to validate the identity and accreditation of healthcare professionals and HCOs on its territory who may legally receive data originating from an epSOS NCP in another country. The epSOS NCP shall establish an appropriate 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 NCP A from all parties concerned and handed over to a patient or a HCO requiring such information. The epSOS NCP shall assume responsibility for appropriate data collection on the execution of the pilot through the PoCs on its territory and shall assume responsibility for the reporting of such data to the epSOS Project Partner(s) on its territory.

3.4. The epSOS NCP must ensure that nominative epSOS data is not transmitted to parties outside the NCP and its pilot partners.

3.5. The epSOS NCP shall maintain a helpdesk service to support the HCPs and HCOs in its territory.

3.6. The epSOS NCP maintain the communication on epSOS pilots at national level and links to the epSOS website.

4. **epSOS NCP duties and responsibilities to other epSOS NCPs**

4.1. The epSOS NCP shall be accountable to other epSOS NCPs for ensuring the security (confidentiality, integrity, availability, non repudiation and authenticity and auditability) of data processed on their territory.

4.2. The epSOS NCP shall be accountable to other epSOS NCPs for guaranteeing that all epSOS jointly agreed service specifications and requirements (legal, organisational, technical) are fulfilled.

4.3. The epSOS NCP shall be accountable to other epSOS NCPs, represented through the PSB, for ensuring, conformance of all epSOS national pilot partners to jointly agreed service specifications and requirements.

4.4. The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices to facilitate the establishment of the epSOS trusted domain.

4.5. The epSOS NCPs shall adopt the epSOS Information Governance framework that will comprise commonly adopted policies, processes and audit mechanisms.

4.6. The epSOS NCPs must ensure that national agreements with pilot partners include provisions for applying and regularly auditing the epSOS Information Governance framework. Such audit practices applied by NCPs shall be audited by an external independent auditor.

5. **Duties and responsibilities concerning epSOS Patient Consent (terms to be embodied in the national contracts creating the NCPs and contracts between NCPs and their partners as appropriate)**

5.1. No epSOS data shall be collected either directly from the patient or indirectly from healthcare partners (such as laboratories) without the freely given, specific and informed consent of the patient, according to national law of the country where treatment is provided.

5.2. The epSOS pilot shall be conducted on the basis of an opt-in system of consent; accordingly implied consent to epSOS data collection and processing shall not be permitted.

5.3. The epSOS NCP shall ensure (directly or through appropriate contractual agreements with their PoCs) that consent is obtained and documented for the creation of epSOS records (Patient Summary and ePrescription) if required by national law.

5.4. The epSOS NCP can establish a system which allows a patient to give a prior general consent to access to his or her record by a HCP or PoC or HCO abroad. The epSOS NCP shall establish with its partners a process which allows such general prior consent, if required by national law of country A, to be validated at the PoC. Such validation procedures shall be based on epSOS guidance (WP4.2 A and B) e.g. by ticking a box to confirm patients' consent for access to their PS or medication record held in their home country and shall not be disruptive of the clinical workflows.

5.5. The epSOS NCP shall establish a system to allow a Point of Care providing services to an epSOS patient to document the validations of consent for release of data from the NCP to the Point of Care.

5.6. The epSOS NCP shall establish a system for directly obtaining consent from the patient in situations where prior generalised consent has not been provided.

5.7. The epSOS NCP shall establish a consent override procedure to provide for exceptional cases where it is not possible to obtain consent or validation of consent because of the patient's incapacity including consent for minors. The epSOS NCP shall ensure that all the parties concerned with the pilot are able to comply with the requirements of patient consent to epSOS data collection and processing.

6. **Duties and Responsibilities of the epSOS Pilot Partners under the epSOS Security Policy**

6.1. The epSOS security policy creates a general security and data protection framework adapted to the epSOS information system needs.

6.2. The epSOS security policy address all elements of data flows in the pilot including national and cross-border data flows

6.3. The epSOS actors (NCPs, PoCs HCOs and HCPs) shall ensure that they are fully compliant with the security policy as set out in detail in the project documentation.

7. Relationship between NCP and Points of Care, Healthcare Professional and Healthcare Organisations

7.1. A number of partners in the epSOS pilots shall be legally established and recognised. They shall include Points of Care and healthcare professionals, and may also include Healthcare Organisation representing several Points of Care.

7.2. Each Member State will identify a number of Health Care Organisations which will take part in the pilot. These shall include primary care providers (general practitioners and primary care clinics); secondary care providers (hospitals specialist secondary care providers); pharmacies (both public and private).

7.3. The HCO shall sign a contract under local law with the NCP to which it is responsible.

7.4. The HCO/NCP contract shall set out all the minimum requirements of the PoC and shall establish the legal relationship between them.

7.5. The HCO/NCP contract shall set out minimum requirements for epSOS training for all healthcare professionals who shall be active within the pilot.

7.6. The HCO/NCP contract shall detail the duties of both parties with respect to maintaining the security of the epSOS pilot and all data flows.

7.7. The HCO/NCP contract shall detail the duties of both parties with respect to ensuring that patient consent to collecting and processing epSOS data has been duly obtained and documented according to epSOS procedures.

8. Dispute resolution and applicable law

8.1. The co-operation between NCPs shall be ensured through the Grant Agreement.

8.2. Any conflicts arising between NCPs shall, in the first instance, be referred to the PSB. An appeal may be made to the European Court of Arbitration in Paris in the event of any dispute which cannot be resolved at project level.

ENDNOTE - Steps in epSOS Process

1. HCP in country B at a PoC accepts patient ID which may identify the patient as being eligible to take part in epSOS trial
2. HCP in country B at a PoC confirms patient consent to access data in Country A; or HCP ticks the override box in cases where consent cannot be obtained because of patient incapacity. HCP query can be processed only with consent or override duly confirmed
3. HCP in country B sends query to NCP in country B
4. NCP in country B authenticates the HCP and PoC
5. The NCP in country B queries NCP in country A for the requested patient data

6. NCP in country A authenticates NCP in country B
7. NCP in country A validates patient ID and local prior consent (if applicable)
8. NCP in country A transmits the requested data to NCP in country B
9. NCP in country B authenticates NCP in country A
10. NCP in country B provides the requested data to HCP requestor

ANNEX I : PATIENT CONSENT

Concept

It is not the objective in epSOS to establish uniform Patient Consent practices but rather to ensure that travelling Europeans are reassured that their rights of data protection, as provided for in the Data Protection Directive, are fully respected within the epSOS pilots. If not all rights according to data protection law in their countries of affiliation will be transferrable to a cross-border care situation, the patient must be clearly informed of what rights are not maintained. epSOS must ensure that the citizen has the possibility to give *freely given, specific and informed* consent for data processing within the epSOS trusted domain. Such consent may be collected prior to an encounter in the country of origin depending on national requirements and/or collected at the time of the encounter in the country of treatment.

What is epSOS Patient Consent for?

epSOS does not establish new or specific conditions for collection, processing and storage of health data. This data is created and exists in the country of affiliation, irrespective of epSOS. The epSOS project sets up the mechanism to make health data accessible to health care professionals when the patient requires medical service abroad. Thus, epSOS patient's consent is a pre-requisite, not for collecting medical data for the purposes of providing medical care in the Point of Care (PoC) by a health care professional in country B, but for the purpose of accessing already existing data in the country of residence (country A). We must therefore distinguish two processes for which patient consent is needed – one for providing medical service per se, the other for realizing the epSOS "business case" as a specific processing of already existing personal data. Note that where special epSOS records are created outside the normal healthcare setting, consent must also be obtained for the creation of the epSOS record if national law so requires and then further consent for the sharing of the epSOS record in the consent of the epSOS pilot which must be obtained at the PoC in country B according to epSOS procedures.

a) *Consent for collection and processing of patient's data for medical services, treatment, diagnosis, and similar purposes:*

In this process, patient's data are collected and stored in the patient's health record and they are further used for providing health care. Personal data are obtained directly from the patient, or as results of laboratory, diagnostic and other investigations. Patient Consent in this case is regulated by each particular epSOS country and legislation of the country where data is created is applied. This consent does not grant agreement to access to the patient's data from abroad.

b) *Consent for creation of an epSOS summary*

In some MS where the epSOS record is created specifically for the purposes of epSOS out of existing stored records it will be necessary to obtain patient consent locally in Country A for the creation of the epSOS summary. For the purposes of running the epSOS pilot, this will take place as a procedure similar to obtaining consent for patient's attendance in a clinical trial.

c*) Consent for access to patient epSOS patient summary and ePrescriptions from abroad*. In this processes, the consent is the patient's agreement to make accessible his/her epSOS medical data (already existing in his/her medical record, respectively extracted from this

record into the medical summary record) to professionals providing care to the patient abroad.

It must be clear that if, for the purpose of providing care in another country, new health data is created, then this process is equivalent to case (a) above and is subject to country B rules.

Principles for epSOS Patient Consent

The processing of patient's medical data within the epSOS Large Scale Pilot will take the "opt-in" approach, i.e. the patient will be required to provide his/her consent to receive the pilot epSOS services. The patient must provide the consent (i) for creating his/her epSOS Patient Summary in country A (ii) for access to the summary by a HCP from abroad (i.e. from epSOS B countries). The epSOS consent will be a two-step process where the patient gives consent to the creation of the PS in Country A and is duly informed about potential access to his record by a HCP in country B; as a second step consent to access the PS in country B is verified in Country B once the nature of access and purpose is known to the patient. Securing that consent is *freely given, specific and informed* is pursued in the following approach:

I. The consent will be *specific*

- Patient consent is acquired for creation "epSOS patient data", i.e. Patient Summary (including medication record), if the patient's resident country legislation requires it. This action will take place in country A. This is therefore a requirement in each country A associated to the establishment of a PS, which would be needed irrespective of the cross-border exchange.
- Patient's consent is also aquired for access to epSOS patient data abroad under the circumstances specified in the project. This is additional consent that should ideally be incorporated, as an opt-in option in the national patient consent procedure and documentation.
- A provision will be made to ensure that if a patient has not provided his/her consent for access to "patient data" from abroad, s/he still has the right of his/her epSOS patient data to be created (for use in country A only).

II. The consent will be *freely given*.

- The patient has a free choice to participate in the epSOS LSP without any subsequent restrictions or negative influence to receiving all necessary medical treatment or any other medical services if s/he refuses the participation.
- Patient may withdraw his/her consent at any time.

III. The consent will be *informed*.

- The patient will be informed
  - on the aims of the epSOS LSP, how his/her patient data will be used, on his/her rights and any other circumstances of the processing of his/her data for the epSOS LSP purposes.
  - that his consent is free without any consequences if the consent will not be given.
  - that the collection and further processing of patient's health data solely for providing medical services is a subject of legislation of a country in which medical care is provided.

- This information is drafted as part of Annex III of the FWA and will be localised in each country, preferably as an addendum to the national standard information provided to patients for acquiring Consent.
- The information will reside in the epSOS NCP(A) and will be made available as needed to the patient when s/he is in country B

Where is Patient Consent provided?

From a legal and regulatory perspective, in a *trusted domain* environment, consent may be provided in any territory of location within the trusted domain, under auditable, verifiable and conformant to the epSOS Information Governance conditions.

The epSOS NCP shall establish a system which allows a patient to give a prior general consent to access to his or her medical record by a HCP or PoC or HCO abroad. This consent is then confirmed once the patient is *in situ* in country B prior to requesting access to data.

From an organisational perspective, providing consent in country A would be preferable, as it will simplify processes at the epSOS points of care and will reduce technical complexity. Due to the fact that this is not legal in some MS such as Spain on one hand and also because of the pilot nature of the services, prior consent in country A may prove less realistic than expected, while in many cases, especially in unplanned care situations, the likelihood of needing to obtain consent before treatment in country B is high. It is however envisaged that when epSOS has reached a certain level of deployment and it is incorporated in national planning prior consent provided in country A will be generalised for all mobile citizens.

Usually Consent to access data is obtained in country B and

- it must be *freely given, be specific* of the care encounter and *informed* and at the same time *realistic and feasible for PoC to obtain* on site.
- Patients must be duly informed at the time when consent is sought.
- epSOS safeguards for obtaining and recording consent must be uniformly applied.
- epSOS NCP (A) must verify that patient consent has been obtained at the pilot site before data disclosure to an HCP in country B.

Patient information on epSOS must be provided in Country B in appropriate language and in localized version maintained at epSOS NCP (A) (taking account of country legislation and specificities).

For this purpose epSOS will provide a generic formulation which will form Annex IV of its Framework Agreement documentation. This text is then to be transposed to the national environment at the responsibility of each NCP(A) this transposition extending beyond linguistics to also include other specificities that country A would like to make known to its citizens and will be updated at the responsibility of this country as appropriate.

This informative text will be provided to citizens when staying in country B, via the epSOS NCP of country B. Thus, the text transfer to requesting HCP, via epSOS NCP(B) is one of the NCP duties.

If the patient is not able to provide consent in Country B

In some cases the patient will not be able to provide consent because he or she is unconscious, intoxicated and delirious, or has some other cognitive impediment. If this occurs the HCP in country B may access the information in the PS on the provision of a confirmation to the NCP in country A that it is not possible to obtain consent, but in clinical terms it is in the patient's vital interests that the PS is accessed.

How is Patient Consent for transferring patient's epSOS medical data verified?

A positive check of the element demonstrating agreement that information from the patient's health record may be transferred abroad must pre-exist, i.e. no consent/no access to epSOS medical data possible. Notwithstanding the provisions foreseen for the case when patient is not able to provide consent. If the "consent box" is empty, the information shall not be transferred (unless for emergency and vital interest purpose).

Obtaining and recording consent by patients to disclosure of medical data held in their country of usual residence to a healthcare professional at a point of care at an epSOS pilot site in another country must satisfy the following requirements:

- Recognition of the PoC as taking part in epSOS pilots
- Define purpose of disclosure of nominative data for present treatment only
- Record Consent - HCP must tick "consent obtained" box before data request is submitted to NCP, or tick box confirming child care or care of person who cannot consent.
- Patient must confirm consent wherever possible
- HCP may tick alternative box stating that it is not possible to obtain consent, but that access to epSOS Patient Record is needed for emergency situations, when the patient's life is threatened or irrevocable damages may occur.

The onsite processes of obtaining patient consent will be part of the epSOS Information Governance and will be uniformly applied and audited, according to epSOS policies and procedures to be provided by WP3.8.

The patient's wishes to allow access to his/her information must be reflected in his/her patient consent prior to transferring this information from the country A. It is then the task of the NCP in country A to verify that such consent has been duly obtained before initiating a data transfer process.

If the patient is not able to provide consent in Country B, confirmation to the NCP in country A that it is not possible to obtain consent and an emergency situation is at hand will be done by ticking an override box and giving the identification of the HCP concerned. If the NCP in country A is satisfied of the circumstances and if domestic law allows for such emergency access to data (which in is provided for in the Data Protection Directive) then the NCP may transfer the data to country B. A log shall be kept of all such emergency data transfer without patient consent. The possibility of such transfer without consent shall also be explained to the patient at the time when consent to the creation of the PS is obtained.

ANNEX II: INFORMATION FOR EPSOS PATIENTS AND HEALTHCARE PROFESSIONALS

1. About the epSOS services

You are invited to provide/receive electronic services for Patient Summaries and ePrescribing that are offered on a pilot basis and by a small number of institutions and pharmacies.

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 safety considerations and measures required by national law have been taken. Additionally, epSOS 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 countries participating in this pilot: *Austria, France, Region of Lombardy in Italy, Denmark, Germany, Greece, Czech Republic, Slovakia, Sweden and - in Spain- Catalunya, Castilla La Mancha, Andalucia, Balearic island and Comunitat Valenciana.*

Each country, through a designated organisation, undertakes to support the participating health care organisations and Health Care Professional on its territory taking part in epSOS pilot with adequate information training about the pilot and the duties and responsibilities which must be assumed by the epSOS partners.

[country name] participates in the epSOS Large Scale Pilot in the following way:

Health Care Organisation	Services offered*	Contact Information

*Please select from the following

- a [nationality] treating physician/pharmacist will be provided access to available Patient Summaries/eprescriptions of foreign visitors in the process of providing care to them.
- the [national NCP name] will receive a request and will make accessible a patient summary of a [nationality] patient receiving care abroad.
- the [national NCP name] will receive a request and will make accessible an electronic prescription of a [nationality] patient receiving care abroad
- a [nationality] treating physician/pharmacists will be provided access to available e-prescriptions of foreign citizens in the process of providing care to them
- a [nationality] pharmacist will send dispensed medication information to the country of affiliation of the foreign visitor
- the [national NCP name] will receive dispensed medication of a [nationality] patient receiving care abroad.

2. Terms and Conditions [13]

The above services are offered in conformance to epSOS safeguards and procedures, established collectively and with active representation from participating Points of Care. Specifically:

2.1. Terms and Conditions relating to the Patient Summary

1. The purpose for access to information is to enable Health Care Professionals and Pharmacists to make an informed decision and to improve patient care. The project will also enable patients to have e-prescriptions from their country of affiliation available for them in other participating countries, dispensed at designated epSOS pharmacies. The use of these services is not mandatory, but it can provide helpful information for Health Care Professionals and Pharmacists. There is also a need for contribution to the epSOS evaluation.
2. The epSOS Patient Summary (PS) does not hold detailed medical history or details of clinical condition or the full set of the prescriptions and dispensation. The Medication summary, is part of the Patient Summary and can be consulted by the pharmacists as a separate entity under the same terms and conditions.
3. The PS contains a common and agreed structure for all the European countries and reliable information of where the patient is insured. The PS is divided into three main sections: Patient Administrative Data, Patient Clinical Data and Information about the Patient Summary itself.
4. Access is also possible to all "Available ePrescriptions". This does not mean that country A sends all ePs that the patient has left to be dispensed but only those that, under country A responsibility, country A considers that are to be administrated to the patient at that specific moment in time[14]. This means that the pharmacist in country B can dispense, all the medicines shown by country A, for instance, if A sends to B a whole treatment, this means that B can dispense the whole treatment.
5. Each country is responsible for the content of the PS and its creation. Information about how the Patient Summary is generated (*ie by direct human intervention of a HCP; automatically generated using the national data bases; a mixed approach, validated by the human intervention*) is included in the third section of PS.
6. However, it is possible that a more recent health record has been created in another country. In this phase of the pilot, such information is not used to update the epSOS Patient Summary.
7. Only the fields [National healthcare patient ID], [Given name], [Family name/Surname]; [Date of Birth] will be always present in the PS. The rest of the fields are populated according to what data is held by the country where the Patient Summary is generated.
8. It is important to note that, if a patient has decided to hide information in his country, this hidden information will not appear in the epSOS dataset. For legal reasons, there will not be any kind of flag in the PS to alert this fact.

[13] Member states must also inform the patient if the use of epSOS services will be at a cost for the patient. If no cost will occur for the patient, this information is not necessary.

[14] (e.g. in the case of chronic treatments where in some countries an administration pattern is established and automatically controlled by the dispense system.

9. Use of the epSOS services does not alter obligations to fulfill legal requirements of the country in order to provide medical services to the epSOS patients. This means that the scope and categories as well as the relevance of personal data (including sensitive data) required by Health Care Professionals can be created and recorded at the point of care. epSOS services does not include any transfer of medical data to the patient's country of affiliation or the country where the patient is insured.

2.2. Terms and Conditions relating to the Privacy

1. Access to data is allowed provided that patient consent has been granted in accordance with national law, and the purpose of access is to provide medical care for the patient. If the patient decides not to give his consent, this can be recorded either in the country of affiliation or the country where the patient is insured. The patient can also decline the use of epSOS services at the Point of Care, whereas no access is allowed.
2. If consent has not been provided already at the country of affiliation or where the patient is insured, it will be necessary to obtain it on site. In this event it must be *freely given, be specific* of the care encounter and *informed*.

- Consent must always be provided at the point of care, provided that the patient is not a minor or has diminished capacities. These cases must be handled in accordance with national legislation in the country where the health record is stored. Access can also be granted in emergency situations when the patient´s life is at risk or it can be assumed that the patient may suffer a serious health risk if information is not given. The patient must receive information of any emergency access that has taken places as soon as the patient is able to receive such information.
- Patients must be duly informed and provided with the respective information in his/her own language that can be downloaded from the epSOS system.
- Patient consent is recorded and logged electronically before data request is submitted.

3. The DPD, implemented in national law, gives the Patient right to obtain from the Data Controller

(a) without constraint at reasonable intervals and without excessive delay or expense:

i. confirmation as to whether or not data relating to him/her are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

ii. communication to him/her in an intelligible form about the data undergoing processing and of any available information as to their source,

iii. communication to him/her of the concept involved in any automatic processing of data concerning him/her at least in the case of the automated decisions referred to in Article 15 (1) of the DPD;

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

4. Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28 of the DPD, prior to referral to the judicial authority, provisions have been made for the right of every person to a

judicial remedy for any breach of the rights guaranteed him/her by the national law applicable to the processing in question.

5. Provisions have been made that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted according to his/her national legislation is entitled to receive compensation from the controller for the damage suffered.

Any further questions can be addressed to: (Country contact details and national coordinator. Contact details for Data Controller and Data processor.)

Annex III SUPPORTING DOCUMENTS

During the course of the preparation of this document several discussion and in depth legal analysis took place around a number of issues. In Project place a dossier titled D2.1.2. Supporting documents has been created at location https://service.projectplace.com/pp/pp.cgi/0/427368494 . It contains such in depth analysis documents that were used to produce this deliverable and they are addressed to any member of epSOS wishing to explore further specific issues.

a. On patient consent please refer to "Patient Consent in the epSOS Large Scale project"
b. On Information to NCPs please refer to "Information to NCPs"
c. On input from CALLIOPE on the epSOS legal approach please refer to "1st CALLepSO Worskhop Report"
d. Under preparation " Liability in epSOS"

Framework Agreement

on

National Contact Points

in the context of the

Smart Open Services for European Patients Project (epSOS)

(version 2)

CONSENSUS STATEMENT

Since early 2010, PNs have engaged in national contracts, uniformly based on the FWA issued in January 2010 as a formal project deliverable and presented to the PSB. This first version was considered by the PSB to be a sufficient basis to engage National Authority Beneficiaries (NABs) into the process of localization of this epSOS blue print to the national situations. Provision was made at that time that after localization would be complete, this blue print would be reviewed for any needed amendments to better match its implementation. The process of localization indicated that some deviations from the this blue print were necessary, especially around Annex I and II which had to be simplified and clarified with respect to its intent, being in effect to constitute the epSOS Privacy Statement. In addition the PSB-LEG in its June 8th, 2011 second meeting, accepted proposals of WP2.1. and recommended to:

- Append the epSOS Security Policy as an integral part of it (now Annex III);
- Include provisions for its amendment, taking into account consequences for its localization into a separate article 9;
- remove the informative previous Annex I on Patient Consent and together with Duties and Responsibilities endorse them into deployment guidelines;
- add provision for duties, responsibilities and liability around semantic mapping (new article 2.3)
- Align used terminology to that of the cross border directive, in order to improve shareability of this FWA with other EU policy initiatives
- Avoid abbreviations

Amendments to the FWA are limited to implementation of the above

recommendations. Annex III will has been replaced by the final PSB approved version of the epSOS Security Policy.

Framework Agreement

on

National Contact Points

in the context of the

Smart Open Services for European Patients Project (epSOS)

Preamble

- The epSOS Large Scale Pilot Project has been established to develop and test a pilot system of cross-border data sharing to support patient care delivered to European citizens outside their usual state of residence by means of a shareable electronic Patient Summary and ePrescription.
- The Framework Agreement and its annexes is designed 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.
- This Framework Agreement provides a blueprint for national level contractual agreements, where required[2], to create a National Contact Point [hereinafter NCP] as a legal entity entitled to process patient data in the context of the epSOS pilot.
- The Framework Agreement also sets out the core duties of the NCP and its partners so that the NCPs, once created, may contract on a common basis with their local partners (Healthcare Providers [Art 3 lit g Directive 2011/24/EU], Health Professionals and Points of Care) to deliver the epSOS services to Patients (Art 3 lit h Directive 2011/24/EU).
- Annexes I and II of the Framework Agreement give further guidance on the information to be given to Patients and Health Professionals on their rights and duties within epSOS.
- The articles of the Framework Agreement and its annexes shall be transposed into:
    - (where necessary) Contracts under applicable national law to establish epSOS NCPs and
    - (where necessary) Contracts under applicable national law to designate Points of Care from within existing Healthcare Providers as epSOS Points of Care.
- The terms of this Framework Agreement and its annexes may be modified during transposition into local contracts and guidelines only in so far as it is necessary to do so in order to comply with local law or custom.
- The contractual agreements established at national level to create the NCPs shall be certified as conformant to epSOS principals by the Project Steering Board.

[2] Some Participating Nations may not need to establish NCPs by contract if, for example, the national administration provides the service itself.

1. The epSOS pilot – Creation of the epSOS National Contact Point (NCP)

1.1. The epSOS pilot is an initiative of several European Participating Nations to develop and test a system for access to health data in cross-border situations to support patient care delivered to European citizens outside their usual state of residence by means of a common epSOS electronic patient summary and a common epSOS e-prescription.

1.2. The national and regional Departments of Health and their related eHealth Competence Centres are beneficiaries of Grant Agreement number 224991 of the European Commission and its associated Consortium Agreement.

1.3. In accordance with the Grant Agreement the beneficiaries have contracted with the European Commission and each other to ensure that a number of healthcare establishments within their territory will provide one or more test sites for the epSOS Pilot – hereinafter known as a healthcare provider.

1.4. Each participating nation shall appoint one legal entity to act as NCP. Where this function is federated across several organisations one entity shall act on behalf of the others to be the liaison point for NCPs from other epSOS nations.

1.5. In the case of regional beneficiaries one NCP will represent all regional beneficiaries.

1.6. The NCP in each PN shall be created under local law on the basis of the present framework agreement.

2. Core Characteristics of the epSOS National Contact Point (NCP) (Terms to be included in all national contracts relating to epSOS)

2.1. The NCP shall be a legal entity which is legally competent to contract with other organisations in order to collaboratively carry out its duties and responsibilities in epSOS.

2.2. The NCP shall contract with epSOS Healthcare Providers to provide epSOS services to Patients.

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

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

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

2.3.3. Pilot sites are not liable for any patient safety adverse events attributed to semantic mapping, save for any contributory negligence in interpreting the data.

2.4. The epSOS NCP 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 epSOS use cases (see end note).

2.5. The NCP 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 NCP shall:

2.5.1. be technically competent to provide a gateway for epSOS information transfer;

2.5.2. be legally recognised as a data controller or data processor in accordance with domestic data protection legislation;

2.5.3. be legally competent to execute contractual agreements with all domestic partners in compliance with domestic data protection legislation;

2.5.4. be legally competent to enforce audit and corrective action emerging from audits;

2.5.5. be technically competent to validate the identity of Patients and patient consent of its territory (acting as country A);

2.5.6. maintain the local versions of the epSOS semantic value sets.

3. General Duties and responsibilities of the epSOS NCP (terms to be embodied in the national contracts creating the NCPs)

3.1. The epSOS NCP shall establish appropriate security and data protection systems to conform to epSOS requirements as well as all applicable national requirements.

3.2. The epSOS NCP shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).

The epSOS NCP shall establish 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 epSOS NCP in another nation. The epSOS NCP shall establish an appropriate 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 NCP A from all parties concerned and handed over to a Patient or a Healthcare Provider requiring such information. The epSOS NCP shall assume responsibility for appropriate data collection on the execution of the pilot through the Points of Care on its territory and shall assume responsibility for the reporting of such data to the epSOS Project Partner(s) on its territory.

3.3. The epSOS NCP must ensure that nominative epSOS data is not transmitted to parties outside the NCP and its pilot partners.

3.4. The epSOS NCP shall maintain a helpdesk service to support the Health Professionals and Healthcare Providers in its territory.

3.5. The epSOS NCP maintain the communication on epSOS pilots at national level and links to the epSOS website.

4. epSOS NCP duties and responsibilities to other epSOS NCPs

4.1. The epSOS NCP shall be accountable to other epSOS NCPs for ensuring the security (confidentiality, integrity, availability, non repudiation and authenticity and auditability) of data processed on their territory.

4.2. The epSOS NCP shall be accountable to other epSOS NCPs for guaranteeing that all epSOS jointly agreed service specifications and requirements (legal, organisational, semantic and technical) are fulfilled.

4.3. **T**he epSOS NCP shall be accountable to other epSOS NCPs, represented through the PSB, for ensuring, conformance of all epSOS national pilot partners to jointly agreed service specifications and requirements.

4.4. The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices to facilitate the establishment of the epSOS trusted domain.

4.5. The epSOS NCPs shall adopt the epSOS Information Governance framework that will comprise commonly adopted policies, processes and audit mechanisms.

4.6. The epSOS NCPs must ensure that national agreements with pilot partners include provisions for applying and regularly auditing the epSOS Information Governance framework. Such audit practices applied by NCPs shall be audited by an external independent auditor.

5. Duties and responsibilities concerning epSOS Patient Consent (terms to be embodied in the national contracts creating the NCPs and contracts between NCPs and their partners as appropriate)

5.1. No epSOS data shall be collected either directly from the Patient or indirectly from Healthcare Providers without the freely given, specific and informed consent of the Patient, according to national law of the country where treatment is provided.

5.2. The epSOS pilot shall be conducted on the basis of an opt-in system of consent; accordingly implied consent to epSOS data collection and processing shall not be permitted.

5.3. The epSOS NCP shall ensure (directly or through appropriate contractual agreements with their Points of Care that consent is obtained and documented for the creation of epSOS records (Patient Summary and ePrescription) if required by national law.

5.4. The epSOS NCP can establish a system which allows a patient to give a prior general agreement to access to his or her record by a Health Professional or Point of Care or Healthcare Provider abroad. The epSOS NCP shall establish with its partners a process which allows such general prior agreement, if required by national law of country A, to be validated at the Point of Care. Such validation procedures shall be e.g. by ticking a box to confirm patients' consent for access to their Patient Summary or ePrescriptions held in their home country and shall not be disruptive of the clinical workflows.

5.5. The epSOS NCP shall establish a system to allow a Point of Care providing services to an epSOS patient to document the validations of consent for release of data from the NCP to the Point of Care.

5.6. The epSOS NCP may establish a system for directly obtaining agreement from the patient in situations where prior generalised agreement has not been provided in country A, in all cases where country A permits such delegation of responsibility.

5.7. The epSOS NCP shall establish a consent override procedure to provide for exceptional cases where it is not possible to obtain consent or validation of consent because of the patient's incapacity including consent for minors. The epSOS NCP shall ensure that all the parties concerned with the pilot are able to comply with the requirements of patient consent to epSOS data collection and processing.

6. Duties and Responsibilities of the epSOS Pilot Partners under the epSOS Security Policy

6.1. The epSOS security policy creates a general security and data protection framework adapted to the epSOS information system needs.

6.2. The epSOS security policy address all elements of data flows in the pilot including national and cross-border data flows

6.3. The epSOS actors (epSOS NCPs, Health Professionals, Points of Care and Healthcare Providers) shall ensure that they are fully compliant with the Security Policy as set out in detail in Annex III.

7. Relationship between NCP and Points of Care, Health Professionals and Healthcare Providers

7.1. A number of partners in the epSOS pilots shall be legally established and recognised. They shall include Points of Care and Health Professionals, and may also include Healthcare Providers representing several Points of Care**.**

7.2. Each PN will identify a number of Healthcare Providers which will take part in the pilot. These shall include primary care providers (general practitioners and primary care clinics); secondary care providers (hospitals specialist secondary care providers); pharmacies (both public and private).

7.3. The Healthcare Provider shall sign a contract under local law with the NCP to which it is responsible.

7.4. The Healthcare Provider/NCP contract shall set out all the minimum requirements of the Point of Care and shall establish the legal relationship between them.

7.5. The Healthcare Provider/NCP contract shall set out minimum requirements for epSOS training for all health professionals who shall be active within the pilot.

7.6. The Healthcare Provider/NCP contract shall detail the duties of both parties with respect to maintaining the security of the epSOS pilot and all data flows.

7.7. The Healthcare Provider/NCP contract shall detail the duties of both parties with respect to ensuring that patient consent to collecting and processing epSOS data has been duly obtained and documented according to epSOS procedures.

8. Dispute resolution and applicable law

8.1. The co-operation between NCPs shall be ensured through the Grant Agreement.

8.2. Any conflicts arising between NCPs shall, in the first instance, be referred to the PSB. A request for arbitration may be filed with the European Court of Arbitration in the event of any dispute which cannot be resolved at project level.

9. Amendments of the Framework Agreement

9.1. Amendments to this Framework Agreement, its Annexes and any related epSOS policies which have been duly adopted in accordance with project procedure through the epSOS Project Steering Board (PSB), shall be translated and applied to the contracts for epSOS services as provided for in the preamble. The National Authority Beneficiary (NAB) shall give appropriate publicity to the adopted amendments as well as the decision of the PSB not later than 4 weeks after the amendments have been adopted by the PSB.

9.2. Save from the NABs, all parties to the above mentioned contracts shall have the right to rescind the contract during the 16 weeks following the PSB decision.

9.3. Unless otherwise defined by the PSB, the amendments to the above mentioned contracts shall come into effect 16 weeks after the amendments have been adopted by the PSB.

ENDNOTE – Steps in epSOS Process

1. Health Professional in country B at a Point of Care accepts patient ID which may identify the patient as being eligible to take part in epSOS trial.
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 NCP in country B.
4. NCP in country B authenticates the Health Professional and Point of Care.
5. The NCP in country B queries NCP in country A for the requested patient data.
6. NCP in country A authenticates NCP in country B.
7. NCP in country A validates patient ID and local prior agreement (if applicable).
8. NCP in country A transmits the requested data to NCP in country B.
9. NCP in country B authenticates NCP in country A.
10. NCP in country B provides the requested data to Health Professional requestor.

ANNEX I. 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 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 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 Conditions document for details on these services and the terms and conditions for their delivery.

[Here please insert a paragraph about

- consent to create a PS if needed by your country
- 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
- 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 [COUNRTY OF TREATMENT] for the purposes of providing me with medical care and/or medication.

ANNEX II. epSOS TERMS AND CONDITIONS[3]

The epSOS services are offered in conformance to epSOS safeguards and procedures, established collectively and with active representation from participating Points of Care. Specifically:

1. Terms and Conditions relating to the Patient Summary and ePrescription

1.1. The purpose of access to information contained in a Patient Summary is to enable Health Professionals in countries other than the Patient's country of residence to make an informed decision and to improve patient care. The project will also enable Patients to have ePrescriptions from their country of residence dispensed at designated epSOS pharmacies in other participating countries. The use of the epSOS services is voluntary on the part of the Patient. 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.

1.2. The Patient Summary contains a common and agreed structure for all the European countries and reliable information of where the patient is insured. The Patient Summary is divided into three main sections: Patient Administrative Data, Patient Clinical Data and Information about the Patient Summary itself.

1.3. Each country is responsible for the content of the Patient Summary and its creation. Information about how the Patient Summary is generated (ie by direct human intervention of a Health Professional; automatically generated using the national data bases; a mixed approach, validated by the human intervention) is included in the third section of PS.

1.4. When a medical record is created in another country such information is not included into the PS. It will be included into the patients' records in the usual country of residence only if such records are sent back to the Patients' country of residence. Such correspondence is not part of epSOS and happens only in accordance with usual practice at the foreign point of care. Only the fields [National healthcare patient ID], [Given name], [Family name/Surname], [Date of Birth] will be always present in the PS. The rest of the fields are populated according to what data is held in the patient's country of residence where the Patient Summary is generated.

1.5. It is important to note that, if a Patient has decided to hide information in his country, this hidden information will not appear in the epSOS dataset neither will there be any kind of flag in the PS to alert this fact.

1.6. Use of the epSOS services does not alter obligations to fulfill legal requirements existing in the country where medical care is provided to the Patients participating in the epSOS pilot.

1.7. Health data will be recorded and stored in medical records at the point of care according to the regulations applicable in the treating country. epSOS services do not involve any transfer of such medical data to the Patient's country of usual residence.

2. Terms and Conditions relating to the Privacy

[3] Piloting Nations must also inform the patient if the use of epSOS services will be at a cost for the patient. If no cost will occur for the patient, this information is not necessary.

2.1. Access to data is permitted provided that patient consent has been granted in accordance with national law, and the purpose of access is to provide medical care for the Patient. If the Patient decides not to give his/her consent, this can be recorded in the country where the Patient Summary is created. The Patient can also decline the use of epSOS services at the Point of Care, whereas no access is allowed.

2.2. If consent has not been provided already at the country of affiliation or where the Patient is insured, it is still possible to obtain it at a Point of Care in foreign country. In this event such consent must be freely given, must be specific to the care encounter and the Patient must be informed about which data are to be collected and to what purpose they will be put.

2.2.1. Consent must always be confirmed at the Point of Care, provided that the Patient is not a minor or has diminished capacities[4]. Patients will be duly informed and provided with the respective information as needed in their own language at the Point of Care.

2.2.2. Patient consent is recorded and logged electronically before data request is submitted.

2.2.3. Access to information may also be granted by the relevant authority in the country of usual residence in emergency situations[5] when the patient´s life is at risk or it can be assumed that the Patient may suffer a very serious health risk if information is not given. The Patient will receive information of any such access that has taken places as soon as the Patient is able to receive such information.

2.3. The European Data Protection Directive (DPD), implemented in national law, gives the Patient right to obtain from the Data Controller:

"*(a) without constraint, at reasonable intervals and without excessive delay or expense:*

- *confirmation as to whether or not data relating to him[/her] are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*
- *communication to him[/her] in an intelligible form [about] the data undergoing processing and of any available information as to their source,*
- *[communication to him/her of the concept] involved in any automatic processing of data concerning him[/her] at least in the case of the automated decisions referred to in Article 15 (1) [of the DPD];*

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;"

2.4. Provisions have been made that any person who has suffered damage as a result of an unlawful processing operation or of any data processing act incompatible with the national provisions adopted according to his/her national legislation is entitled to receive compensation from the controller for the damage suffered.

---

[4] These cases are excluded from this phase of epSOS pilot services

5 i.e. the cases when data is necessary to avert *life-threatening situation* to someone's health, when the data subject is not able to give consent due e.g. to acute disease or accident. In such cases, the necessity from a medical point of view to collect/handle data, compensates for the requirement of a valid consent, regardless of given or not given prior or concrete consent

2.5. Any further questions can be addressed to: (Country contact details of national coordinator and Data Controller).

ANNEX III. epSOS SECURITY POLICY (epSOS SP)

1. The epSOS Security Policy

1.1. Need and Scope

Security is a critically important issue for epSOS. Without adequate security in place none of the epSOS services can be used in real-life environments. The epSOS Security Policy (epSOS SP) aims to create a secure operational environment for the service deployment which will be sufficient for protecting the epSOS data and processes, implementable and agreed by all participants. The epSOS Security Policy provides a secure operational environment for epSOS, helps develop a 'chain of trust' among epSOS actors and has been developed according to the provisions of the Technical Annex of the project and the contract. The Security Policy also specifies the obligations of service providers and users and must be implemented and periodically audited by all epSOS partners, as described below.

1.2. Principle and Objectives

1.2.1. Principle

All epSOS data and processes must be adequately protected. The network built among the epSOS partners should also not add any unacceptable new risk within any partner organization. Appropriate technologies and procedures must be used to ensure that data is stored processed and transmitted securely over the network built among the epSOS partners and is only disclosed to authorized parties.

Information security is generally characterized as the protection of:

a. Confidentiality (information is protected from unauthorized access or unintended disclosure – only authorized users have access to the information and other system resources),

b. Integrity (information is protected from unauthorized modification) and

c. Availability (resources are available, without unreasonable delay - authorized users are able to access information and the related means when they need it).

The epSOS Security Policy should help to ensure and enforce the above. It should also provide means of proof and essential checks, which establish users' trust in the given information.

1.2.2. Objectives

The objective of the epSOS Security Policy is to establish the basic security provisions that must be satisfied in order to ensure the security of data and system continuity and to prevent and minimise the impact of security incidents by implementing a stable, reliable and secure infrastructure.

More specifically, the epSOS Security Policy objectives are:

a. To make epSOS actors sensitive in the operated means of protection and in the risks which they cover.

b. To create a general security framework adapted to the epSOS information system needs, which should be observed by those in charge of epSOS processes; it should be implemented by putting in place measures and procedures in order to ensure the epSOS information and epSOS information system and infrastructure security.

c. To promote cooperation between various epSOS actors in order to jointly elaborate and put in place those measures, instructions and procedures.

d. To enhance user and Patient' trust in the information system.

e. To ensure that the information system in place respects the National and European legislation on privacy and data protection in force.

The epSOS security policy is constructed under the principle of well-proportioned answer to the incurred risk.

1.3. **Security Rules**

The following general security rules are required and apply for the epSOS data exchange model:

SR 1	epSOS data flows must be adequately protected, as specified in the ISO 27000 series international standards or equivalent.
SR 2	End users must be unambiguously identified by national infrastructure before being provided access to the system.
SR 3	Mutual authentication between End Users and the national infrastructures' identity providers is needed when connecting to the system.
SR 4	End user identification and authentication procedures in place must be audited according to the epSOS security audit policy.
SR 5	The epSOS security audit policy must be implemented. Audit policy is defined by the epSOS PSB
SR 6	Mutual Authentication between national contact point providers (NCPs) of different Member State is needed when initiating a trans European (cross border) information flow.
SR 7	Non-repudiation procedures must be implemented between the User-Originator and the User-Receiver of documents and messages
SR 8	All epSOS actors in a Country B must ensure that any medical document is forwarded only to the user that has been authorized to access the document.
SR 9	The software used to implement the NCP gateway must conform to the technical specifications of epSOS architecture and common components (D3.3.2, D3.4.2 and D3.9.1)

Rules SR2, SR3 and SR4 are national (national level) competency, while rules SR5, SR6, SR7, and SR8 are a pan European (epSOS level) competency.

In addition, epSOS actors and processes must also take into account the relevant security provisions of the security recommendations of the Commission Recommendation on cross-border interoperability of electronic health record systems (Rec. 2008/594/EC).

1.4. Security Audit

A security audit must be conducted yearly to audit the systems by ISO/IEC 17799 or ISO/IEC 27001, or equivalent level standards, according to the above listed requirements and the guidelines provided in D3.8.2. in this respect. Audit will be based on the epSOS Security Audit policy, described in Chapter 2 of this Security Policy.

1.5. Document update policy

A Security Expert Group (SEG) set up and operating within the TPM function of epSOS, will continually follow-up and propose revisions of the security policy to WP2.2. Proposed amendments will be placed on the PSB agenda twice a year or as otherwise deemed necessary.

Clear and justified proposals for Security Policy review arising from the implementation activities need to be accompanied by an assessment of their impact on the rest of the work packages.

1.6. References

[D3.7 MD] "WP3.7_D3.7.2_ Security Service_V04.pdf", REGLOM, epSOS 2010

[epSOS Annex I] epSOS Annex I – "Description of Work", EMP/S.O.S. LSP-eHealth team, 2008-06-30

[FWA] D2.1 Legal and regulatory constraints on epSOS, WP2.1, epSOS, 2009-01-31

1.7. Further Requirements and Recommendations

All epSOS actors must respect the provisions of this Security Policy.

The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices for the epSOS Security Policy and its implementation[6].

2. The epSOS Security Audit Policy

2.1. Objectives

In compliance with the provisions of the epSOS Security Policy (SP), the epSOS Security Audit shall observe the following general requirements:

- It shall cover both the epSOS Security Policy and the ISO 27000/2 standard requirements.

[6] According to FWA clause 4.4.

- The epSOS Security Audit shall focus on confidentiality and integrity needs more so than availability needs.
- The epSOS Security Audit shall include an assessment of compliance to national legislation.
- The epSOS Security Audit Procedure is conducted by national auditors, using ISO based procedures.
- Each national epSOS NCP must pass successfully annual security audits.
- Successful completion of the Initial Audit shall certify that data and privacy protection procedures are in place as a pre-requisite to entering the Operation Phase of the Pilot.
- Besides the NCP infrastructure also the epSOS Central Services need to be audited.

2.2. **Basic Provisions for the Audit Procedure**

The epSOS security audit procedure is based on the following provisions:

- An internal audit process will be followed, where the National Authority Beneficiary (NAB) selects its own auditor. The audit should be performed by an auditor that is certified to international standards and accredited by national law. The ISO 27002 standard shall provide the framework for epSOS audit.
- In case of a serious non-conformity or dispute an escalation process will be carried out by the PSB, which may include the delegation of an epSOS independent certified auditor to perform an independent audit in the MS in question.
- The PSB will appoint a group of security experts in the legal and technical domain, that will coordinate and review the Member States implementation of the Security Policy.
- This process will be mainly desktop review of audit reports provided in a standardized epSOS Audit Report format and may include onsite visits which will in addition be part of learning and exchange of good practices in epSOS.

ANNEX I. epSOS PRIVACY INFORMATION NOTICE

Notification

- **The epSOS Annex I epSOS Privacy information notice can only be used when it is in accordance with Swedish national law.**
- **In conflicts between Swedish law and the epSOS Privacy information notice Swedish national law takes priority. Swedish law also takes priority over FWA or any other agreements or documents, whatever the standing of the document.**

4. 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.

5. 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 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.

6. Your data , Your Consent

The epSOS services will become available to you in participating countries and institutions only if you 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 Conditions document for details on these services and the terms and conditions for their delivery.

[Here please insert a paragraph about

- consent to create a PS if needed by your country

- 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
- 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 [COUNRTY OF TREATMENT] for the purposes of providing me with medical care and/or medication.

ANNEX II. epSOS TERMS AND CONDITIONS[7]

Notification

- **The epSOS Annex II - epSOS epSOS terms and conditions can only be used when it is in accordance with Swedish national law.**
- **In conflicts between Swedish law and the epSOS Annex II Swedish national law takes priority. Swedish law also takes priority over FWA or any other agreements or documents, whatever the standing of the document.**

The epSOS services are offered in conformance to epSOS safeguards and procedures, established collectively and with active representation from participating Points of Care. Specifically:

3. Terms and Conditions relating to the Patient Summary and ePrescription

1.8. The purpose of access to information contained in a Patient Summary is to enable Health Professionals in countries other than the Patient's country of residence to make an informed decision and to improve patient care. The project will also enable Patients to have ePrescriptions from their country of residence dispensed at designated epSOS pharmacies in other participating countries. The use of the epSOS services is voluntary on the part of the Patient. 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.

1.9. The Patient Summary contains a common and agreed structure for all the European countries and reliable information of where the patient is insured. The Patient Summary is divided into three main sections: Patient Administrative Data, Patient Clinical Data and Information about the Patient Summary itself.

1.10. Each country is responsible for the content of the Patient Summary and its creation. Information about how the Patient Summary is generated (ie by direct human intervention of a Health Professional; automatically generated using the national data bases; a mixed approach, validated by the human intervention) is included in the third section of PS.

1.11. When a medical record is created in another country such information is not included into the PS. It will be included into the patients' records in the usual country of residence only if such records are sent back to the Patients' country of residence. Such correspondence is not part of epSOS and happens only in accordance with usual practice at the foreign point of care. Only the fields [National healthcare patient ID], [Given name], [Family name/Surname], [Date of Birth] will be always present in the PS. The rest of the fields are populated according to what data is held in the patient's country of residence where the Patient Summary is generated.

1.12. It is important to note that, if a Patient has decided to hide information in his country, this hidden information will not appear in the epSOS dataset neither will there be any kind of flag in the PS to alert this fact.

[7] Piloting Nations must also inform the patient if the use of epSOS services will be at a cost for the patient. If no cost will occur for the patient, this information is not necessary.

1.13. Use of the epSOS services does not alter obligations to fulfill legal requirements existing in the country where medical care is provided to the Patients participating in the epSOS pilot.

1.14. Health data will be recorded and stored in medical records at the point of care according to the regulations applicable in the treating country. epSOS services do not involve any transfer of such medical data to the Patient's country of usual residence.

4. Terms and Conditions relating to the Privacy

2.6. Access to data is permitted provided that patient consent has been granted in accordance with national law, and the purpose of access is to provide medical care for the Patient. If the Patient decides not to give his/her consent, this can be recorded in the country where the Patient Summary is created. The Patient can also decline the use of epSOS services at the Point of Care, whereas no access is allowed.

2.7. If consent has not been provided already at the country of affiliation or where the Patient is insured, it is still possible to obtain it at a Point of Care in foreign country. In this event such consent must be freely given, must be specific to the care encounter and the Patient must be informed about which data are to be collected and to what purpose they will be put.

2.7.1. Consent must always be confirmed at the Point of Care, provided that the Patient is not a minor or has diminished capacities[8]. Patients will be duly informed and provided with the respective information as needed in their own language at the Point of Care.

2.7.2. Patient consent is recorded and logged electronically before data request is submitted.

2.7.3. Access to information may also be granted by the relevant authority in the country of usual residence in emergency situations[9] when the patient´s life is at risk or it can be assumed that the Patient may suffer a very serious health risk if information is not given. The Patient will receive information of any such access that has taken places as soon as the Patient is able to receive such information.

2.8. The European Data Protection Directive (DPD), implemented in national law, gives the Patient right to obtain from the Data Controller:

"*(a) without constraint, at reasonable intervals and without excessive delay or expense:*

- *confirmation as to whether or not data relating to him[/her] are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*
- *communication to him[/her] in an intelligible form [about] the data undergoing processing and of any available information as to their source,*

[8] These cases are excluded from this phase of epSOS pilot services

9 i.e. the cases when data is necessary to avert *life-threatening situation* to someone's health, when the data subject is not able to give consent due e.g. to acute disease or accident. In such cases, the necessity from a medical point of view to collect/handle data, compensates for the requirement of a valid consent, regardless of given or not given prior or concrete consent

- *[communication to him/her of the concept] involved in any automatic processing of data concerning him[/her] at least in the case of the automated decisions referred to in Article 15 (1) [of the DPD];*

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;"

2.9. Provisions have been made that any person who has suffered damage as a result of an unlawful processing operation or of any data processing act incompatible with the national provisions adopted according to his/her national legislation is entitled to receive compensation from the controller for the damage suffered.

2.10. Any further questions can be addressed to: (Country contact details of national coordinator and Data Controller).

Definitions of concepts and key terms

Note: These set of definitions concern the usage of terms in this document. Where existing terms are considered insufficient for the purposes of this document they have been adapted accordingly. Explicit notifications to such changes have been provided.

Annex I of the Grant Agreement is annexed to the Grant Agreement and comprises the description of work which forms the contractual obligations taken up jointly by the Beneficiaries of the epSOS project, under the Grant Agreement.

Anonymous data in the sense of the Directive 95/46/EC can be defined as any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual, including access to publicly accessible data (e.g. phone books).

Authentication Process to verify the claimed identity of a party before authorising a particular action to be performed.

Authorization Process by which entitlement of a requester, to access or use a given service, is determined.

Country A is the Member State of affiliation, i.e., the state where personal health data of an epSOS patient is stored and where he or she is insured. This is the country where the patient can be unequivocally identified and his or her data may be accessed. [Term from D5.2.1 adapted].

Country B is the Member State of treatment, i.e., where cross-border healthcare is provided when the patient is seeking care abroad. This is a country, different from country A, in which information about a patient is needed to support the provision of healthcare [Term from D5.2.1, adapted].

Data Controller shall mean the 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 [Dir 95/46/EC].

Data Processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the *Data Controller* [Dir 95/46/EC].

eDispensing is defined as 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). [epSOS D3.1.2]

End User is the user of epSOS patient data (e.g. Point of Care, Health Professional, Health Care Organisation, etc.).

ePrescribing is defined as prescribing of medicines in software by a health care professional legally authorized to do so, for dispensing once it has been electronically transmitted, at the pharmacy [epSOS D3.1.2]

ePrescription means a prescription for medicines or treatments, provided in electronic format. A prescription is understood as a set of data such as drug ID, drug name, strength, form, dosage, indication. [Term from D5.2.1, adapted].

epSOS design L&R requirements comprise input into the design of the epSOS services and system components and should normally be addressed fully within the epSOS implementation.

epSOS encounter is any healthcare encounter in country B that makes use of the epSOS services.

epSOS Grant Agreement is the legal contract (including its Annexes) signed between the European Commission and the *Beneficiaries* on the execution of the *epSOS project*.

Beneficiaries are the organisations that participate as partners in the *epSOS project*.

epSOS patients: They are citizens who will seek healthcare at an epSOS PoC and will receive epSOS pilot services. epSOS patients will fit under the following 5 broad categories of cross border mobility:

- temporary visitors abroad;
- people retiring to other countries;
- people in border regions;
- people sent abroad by their home systems (not currently available in epSOS)
- people going abroad to receive care on their own initiative.

epSOS Pilot Partners: Are the national and regional level organizations that enter into partnership in order to deliver the epSOS pilot through delivery of services and the epSOS evaluation. These will normally encompass the epSOS NCP and several local PoCs. Several entities may be established to provide core responsibilities of the NCP if the NCP is not able to fulfill all functions (e.g. national level and regional level co-ordinators).

***epSOS Points of Care (PoC)*:** This is a location where an epSOS citizen may seek healthcare services. It may be a hospital, a pharmacy, the practice of a registered healthcare professional or any other point of the health care system of country B, participating in the epSOS pilot. An epSOS PoC is designated as such by the participating Member States after having demonstrated its capacity to comply with the epSOS requirements.

epSOS Pilot Site*:* It is a cluster of Points of Care, typically with a geographical or an organizational affinity that are designated by a MS to participate in the epSOS large scale pilot. A pilot site can have any number of associated PoC.

epSOS trusted domain is an extension beyond a certain national or regional territory where epSOS ehealth services can be delivered seamlessly to populations travelling to destinations that are federated in the epSOS LSP. The epSOS trusted domain is comprised of epSOS NCPs and their national contractual partners which collectively fulfill all technical, legal and organisational requirements, for safe delivery of epSOS services and secure and confidential transfer or storage of data resulting from healthcare encounters as appropriate, within the epSOS Trusted Domain, according to this framework agreement. The epSOS trusted domain can only be established if compliance to epSOS requirements is secured by audit mechanisms and is supervised by the PSB.

Health Care Professional (HCP) is a person professionally qualified to deliver care; in epSOS the term is used as in Directive 2005/36/EC establishing rules for the mutual recognition of

regulated professions.

epSOS Health Care Professionals are designated HCPs within the epSOS PoCs that are entitled to deliver the epSOS services.

Health Care Organisation (HCO) is any legal entity having legal capacity that relies on the usage of personal health related data in order to fulfill tasks or business purposes notwithstanding whether those tasks have been delegated by law or not. In certain cases a sole practitioner HCP may be both HCP and HCO.

[Note: the acronym represents an adaptation of "HCPO- Health care Provider Organisation" defined in the initial scope and a replacement of the definition "An institution, authorized to provide health care services, unequivocally identified in the set of the Health Care Institutions" (epSOS D3.2.1)]

Health Care Provider is an organization or person who delivers proper health care in a systematic way professionally to any individual in need of health care services.

Identification Assignment of a unique number or string to an entity within a registration procedure which unambiguously identifies the entity. This number or string serves thereafter as an identifier uniquely attached to this entity. (i2-Health_D3.1_1.0)

Information Governance for the purposes of this deliverable is envisaged as incorporating all necessary policies and safeguards for the appropriate use of personal data within epSOS, needed to ensure that personal health information is dealt with legally, securely and to the greatest possible benefit to the epSOS patient in the two epSOS use cases.

Legal entity is an individual or organization which is legally permitted to enter into a contract, and be sued if it fails to meet its contractual obligations.

Legal and Regulatory (L&R) Issues are those issues that emerge from EU and national legal and regulatory frameworks and directly relate to the two epSOS use cases.

Legal and Regulatory profile of epSOS use cases is an integrated view of the legal and regulatory issues that relate to each step of the process in the encounter of a citizen of country A with a Point of Care (PoC) in country B.

Medical Record or ***Health Record*** is a systematic documentation of a patient's medical history and care. The term 'Medical record' is used both for the physical folder for each individual patient and for the body of information which comprises the total of each patient's health history. Medical records are personal documents and there are many ethical and legal issues surrounding them such as the degree of third-party access and appropriate storage and disposal. Although medical records are traditionally compiled and stored by health care professionals (HCP) and health care organisations (HCO) personal health records maintained by individual patients have become more popular in recent years. All data collected in medical records shall be regarded as sensitive personal data and processed accordingly.

Medication Summary is all prescribed medicine for which the period of time indicated for the treatment has not yet expired, whether they have been dispensed or not. It's a synonymous record of current medication. It contains the following information of each one: active ingredient, strength, pharmaceutical dose form, posology, route of administration, onset date of treatment and duration of treatment. [epSOS D3.2.1]. The medication summary is a part of

the PS that can be consulted separately.

National Contact Point (epSOS NCP) is an organization delegated by each participating country to act as a bidirectional technical, organisational and legal interface between the existing different national functions and infrastructures. The NCP is legally competent to contract with other organisations in order to provide the necessary services which are needed to fulfil the business use cases and support services and processes. The epSOS NCP is identifiable in both the epSOS domain and in its national domain, acts as a communication gateway and establishes a Circle of Trust amongst national Trusted Domains. The epSOS NCP also acts as a mediator as far as the legal and regulatory aspects are concerned. As such an NCP is an active part of the epSOS environment if, and only if, it is compliant to normative epSOS interfaces in terms of structure, behaviour and security policies.

Participating Member States are the MS' that, according to PSB approval and audit, have met the criteria for joining the epSOS Trusted Domain. They may be MS currently participating in the project or new MS that have expressed an interest and follow up closely the developments through the CALLepSO NA-SIG (National Authorities Special Interest Group).

Patient consent provided to the data controller or processor means any freely given explicit and informed indication of his/her wishes by which the data subject signifies his/her agreement to personal data relating to him/her being processed for a given purpose.

Patient Summary should be understood to be a reduced set of patient's data which provides a health professional with essential information needed in case of unexpected or unscheduled care or planned care [D3.2.1.].

Personal Data is any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [Dir 95/46/EC]. Personal data includes written data, images and audio data stored on any time or medium.

Processing of personal data ('processing') means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction [Dir 95/46/EC].

Restrictions are epSOS constraints that could have implications on the pilots and they will normally concern transactions which will not be allowed to take place. They will be addressed within the drafting of the Recommendations (D.2.3).

Safeguards are primarily measures to be taken during the pilot operation. They shall aim to establish a condition of trust not only amongst epSOS NCPs but they reach down to the level of Points of Care (PoCs) that the mobile citizen will come into contact with. These measures must be implemented by the pilots and they will form a consistent set of requirements reflected in the standard contract terms (D.2.2.). Safeguards will also include special measures for the running of the pilots.

Trust Framework means an integrated framework detailing how trusted relationships may be best implemented between epSOS NCPs at the European interoperability level and incorporating standard legal requirements including those for audit mechanisms to be

developed at EU level.

Abbreviations

DPC	Data Protection and Confidentiality
DPD	Personal Data Protection Directive (95/46/EC)
EC	European Commission
EHR	Electronic Health Record
epSOS	epSOS (Smart Open Services for European Patients)
EU	European Union
FWA	Framework Agreement
HCO	Health Care Organisation
HCP	Health Care Professional
CA	Consortium Agreement
IG	Information Governance
L&R	Legal and Regulatory
LSP	Large Scale Pilot
MS	Member State
NA	National Authority
NAB	National Authority Beneficiary
NCP	National Contact Point
PCP	Pilot Co-ordination Point
PD2	Project Domain 2 (Legal and Regulatory Issues)
PoC	Point of Care
PS	Patient Summary
PSB	Project Steering Board established in accordance with Section 4. of the epSOS Consortium Agreement
UC	Use case
WP	Work Package
WP29	Article 29 Data Protection Working Party

Förfarandesätt vid utbyte av epSOS-data

ENDNOTE – steps in epSOS process

1. Vårdpersonalen eller apotekspersonal vid en Vårdenhet i Land B godtar patient-ID som kan identifiera en Patient såsom behörig att medverka i epSOS.
Endnote 1.

2. Vårdpersonal eller apotekspersonal vid en Vårdenhet i Land B bekräftar Patientens samtycke att behandla datainformation i Land A. En förfrågan från Vårdpersonalen om att få ta del av patientinformation kan enbart behandlas om Patienten lämnat samtycke till detta.
Endnote 2.

3. Vårdpersonalen eller apotekspersonal i Land B sänder en förfrågan till NCP/Land B.
Endnote 3.

4. NCP/Land B verifierar Vårdpersonalen och Vårdenheten.
Endnote 4.

5. NCP/Land B begär efterfrågad patientinformationen från NCP/Land A.
Endnote 5.

6. NCP/Land A verifierar NCP/Land B.
Endnote 6.

7. NCP/Land A bekräftar aktuell patients identifikation samt om Patienten eventuellt på förhand har lämnat sitt samtycke.
Endnote 7.

8. NCP/Land A översänder den efterfrågade informationen till NCP/Land B.
Endnote 8.

9. NCP/Land B verifierar NCP/Land A.
Endnote 9.

10. NCP/Land B tillhandahåller den efterfrågade informationen till den begärande vård- eller apotekspersonal.
Endnote 10.

epSOS SECURITY POLICY

Notification

- **As stated by Sweden at the meeting on June 8th 2011 in Stockholm, Sweden is not in agreement with the articles, provisions etc. set down in the epSOS Security Policy (hereinafter SP) as the SP to great extent is in conflict with Swedish law and the Swedish legal system.**
- **The SP can therefore only be used when it is fully in accordance with Swedish national law and custom including the Swedish legal system with its principle of delegation to public authorities to issue legally binding regulations.**
- **At the meeting on June 8th 2011 Sweden also declared that the epSOS "circle of trust" and the epSOS "trusted domain"have no legal standing and cannot take precedence over Swedish law or the Swedish legal system.**

Priority

- **In conflicts between Swedish law and the SP Swedish national law will always take priority. Swedish law also takes priority over FWA or any other epSOS agreements or other epSOS documents, whatever the standing of the document.**
- **Swedish security systems in force, whether based on law or other regulations will take priority over provisions in SP.**

3. The epSOS Security Policy

3.1. Need and Scope

Security is a critically important issue for epSOS. Without adequate security in place none of the epSOS services can be used in real-life environments. The epSOS Security Policy (epSOS SP) aims to create a secure operational environment for the service deployment which will be sufficient for protecting the epSOS data and processes, implementable and agreed by all participants. The epSOS Security Policy provides a secure operational environment for epSOS, helps develop a 'chain of trust' among epSOS actors and has been developed according to the provisions of the Technical Annex of the project and the contract. The Security Policy also specifies the obligations of service providers and users and must be implemented and periodically audited by all epSOS partners, as described below.

3.2. Principle and Objectives

3.2.1. Principle

All epSOS data and processes must be adequately protected. The network built among the epSOS partners should also not add any unacceptable new risk within any partner organization. Appropriate technologies and procedures must be used to ensure that data is stored processed and transmitted securely over the network built among the epSOS partners and is only disclosed to authorized parties.

Information security is generally characterized as the protection of:

a. Confidentiality (information is protected from unauthorized access or unintended disclosure – only authorized users have access to the information and other system resources),

b. Integrity (information is protected from unauthorized modification) and

c. Availability (resources are available, without unreasonable delay - authorized users are able to access information and the related means when they need it).

The epSOS Security Policy should help to ensure and enforce the above. It should also provide means of proof and essential checks, which establish users' trust in the given information.

3.2.2. Objectives

The objective of the epSOS Security Policy is to establish the basic security provisions that must be satisfied in order to ensure the security of data and system continuity and to prevent and minimise the impact of security incidents by implementing a stable, reliable and secure infrastructure.

More specifically, the epSOS Security Policy objectives are:

f. To make epSOS actors sensitive in the operated means of protection and in the risks which they cover.

g. To create a general security framework adapted to the epSOS information system needs, which should be observed by those in charge of epSOS processes; it should be implemented by putting in place measures and procedures in order to ensure the epSOS information and epSOS information system and infrastructure security.

h. To promote cooperation between various epSOS actors in order to jointly elaborate and put in place those measures, instructions and procedures.

i. To enhance user and Patient' trust in the information system.

j. To ensure that the information system in place respects the National and European legislation on privacy and data protection in force.

The epSOS security policy is constructed under the principle of well-proportioned answer to the incurred risk.

3.3. Security Rules

The following general security rules are required and apply for the epSOS data exchange model:

SR 1	epSOS data flows must be adequately protected, as specified in the ISO 27000 series international standards or equivalent.
SR 2	End users must be unambiguously identified by national infrastructure before being provided access to the system.
SR 3	Mutual authentication between End Users and the national infrastructures' identity providers is needed when connecting to the system.
SR 4	End user identification and authentication procedures in place must be audited according to the epSOS security audit policy.

SR 5	The epSOS security audit policy must be implemented. Audit policy is defined by the epSOS PSB
SR 6	Mutual Authentication between national contact point providers (NCPs) of different Member State is needed when initiating a trans European (cross border) information flow.
SR 7	Non-repudiation procedures must be implemented between the User-Originator and the User-Receiver of documents and messages
SR 8	All epSOS actors in a Country B must ensure that any medical document is forwarded only to the user that has been authorized to access the document.
SR 9	The software used to implement the NCP gateway must conform to the technical specifications of epSOS architecture and common components (D3.3.2, D3.4.2 and D3.9.1)

Rules SR2, SR3 and SR4 are national (national level) competency, while rules SR5, SR6, SR7, and SR8 are a pan European (epSOS level) competency.

In addition, epSOS actors and processes must also take into account the relevant security provisions of the security recommendations of the Commission Recommendation on cross-border interoperability of electronic health record systems (Rec. 2008/594/EC).

3.4. **Security Audit**

A security audit must be conducted yearly to audit the systems by ISO/IEC 17799 or ISO/IEC 27001, or equivalent level standards, according to the above listed requirements and the guidelines provided in D3.8.2. in this respect. Audit will be based on the epSOS Security Audit policy, described in Chapter 2 of this Security Policy.

3.5. **Document update policy**

A Security Expert Group (SEG) set up and operating within the TPM function of epSOS, will continually follow-up and propose revisions of the security policy to WP2.2. Proposed amendments will be placed on the PSB agenda twice a year or as otherwise deemed necessary.

Clear and justified proposals for Security Policy review arising from the implementation activities need to be accompanied by an assessment of their impact on the rest of the work packages.

3.6. **References**

[D3.7 MD] "WP3.7_D3.7.2_ Security Service_V04.pdf", REGLOM, epSOS 2010

[epSOS Annex I] epSOS Annex I – "Description of Work", EMP/S.O.S. LSP-eHealth team, 2008-06-30

[FWA] D2.1 Legal and regulatory constraints on epSOS, WP2.1, epSOS, 2009-01-31

3.7. Further Requirements and Recommendations

All epSOS actors must respect the provisions of this Security Policy.

The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices for the epSOS Security Policy and its implementation[10].

4. The epSOS Security Audit Policy

4.1. Objectives

In compliance with the provisions of the epSOS Security Policy (SP), the epSOS Security Audit shall observe the following general requirements:

- It shall cover both the epSOS Security Policy and the ISO 27000/2 standard requirements.
- The epSOS Security Audit shall focus on confidentiality and integrity needs more so than availability needs.
- The epSOS Security Audit shall include an assessment of compliance to national legislation.
- The epSOS Security Audit Procedure is conducted by national auditors, using ISO based procedures.
- Each national epSOS NCP must pass successfully annual security audits.
- Successful completion of the Initial Audit shall certify that data and privacy protection procedures are in place as a pre-requisite to entering the Operation Phase of the Pilot.
- Besides the NCP infrastructure also the epSOS Central Services need to be audited.

4.2. Basic Provisions for the Audit Procedure

The epSOS security audit procedure is based on the following provisions:

- An internal audit process will be followed, where the National Authority Beneficiary (NAB) selects its own auditor. The audit should be performed by an auditor that is certified to international standards and accredited by national law. The ISO 27002 standard shall provide the framework for epSOS audit.
- In case of a serious non-conformity or dispute an escalation process will be carried out by the PSB, which may include the delegation of an epSOS independent certified auditor to perform an independent audit in the MS in question.
- The PSB will appoint a group of security experts in the legal and technical domain, that will coordinate and review the Member States implementation of the Security Policy.

[10] According to FWA clause 4.4.

- This process will be mainly desktop review of audit reports provided in a standardized epSOS Audit Report format and may include onsite visits which will in addition be part of learning and exchange of good practices in epSOS.

Cross-reference FWA/epSOS and FWA/Sweden
Notification and comments by Sweden on FWA/Sweden

Framework Agreement

on
National Contact Points
in the context of the
Smart Open Services for European Patients Project (epSOS)
(version 2)

CONSENSUS STATEMENT

Since early 2010, PNs have engaged in national contracts, uniformly based on the FWA issued in January 2010 as a formal project deliverable and presented to the PSB. This first version was considered by the PSB to be a sufficient basis to engage National Authority Beneficiaries (NABs) into the process of localization of this epSOS blue print to the national situations. Provision was made at that time that after localization would be complete, this blue print would be reviewed for any needed amendments to better match its implementation. The process of localization indicated that some deviations from the this blue print were necessary, especially around Annex I and II which had to be simplified and clarified with respect to its intent, being in effect to constitute the epSOS Privacy Statement. In addition the PSB-LEG in its June 8th, 2011 second meeting, accepted proposals of WP2.1. and recommended to:

- Append the epSOS Security Policy as an integral part of it (now Annex III);
- Include provisions for its amendment, taking into account consequences for its localization into a separate article 9;
- remove the informative previous Annex I on Patient Consent and together

with Duties and Responsibilities endorse them into deployment guidelines;

- add provision for duties, responsibilities and liability around semantic mapping (new article 2.3)
- Align used terminology to that of the cross border directive, in order to improve shareability of this FWA with other EU policy initiatives
- Avoid abbreviations

Amendments to the FWA are limited to implementation of the above recommendations. Annex III will has been replaced by the final PSB approved version of the epSOS Security Policy.

Framework Agreement

on

National Contact Points

in the context of the

Smart Open Services for European Patients Project (epSOS)

Notification, comments and explanation on FWA/Sweden

eHealth

- **eHealth, including ePrescriptions and computerized patient file systems, have been used for a long time by the Swedish National Health Service. The Swedish legal system has correspondingly been developed and adapted for the use of computerized systems for health and medical care.**
- **National Health Service, including patients safety and integrity, is regulated by law decided by the Swedish Parliament which can chose to delegate some of its rights to the Swedish Government which can also delegate some of its rights to Governmental Agencies.**
- **Cross-border exchange of patient data within EU is regulated by the directive 95/46/EG of the European parliament and of the Council of the European Union.This principle also applies to cross-border exchange of patient data within the LSP epSOS and therefore is at the regulating principle for the FWA/Sweden.**

FWA/Sweden

- **The Swedish eHealth Agency has been appointed to act as the Swedish National Contact Point (hereinafter NCP/S or NCP/Sweden).**
- **Articles in FWA which are not in coherence with Swedish legislation have been excluded or, when possible, rewritten to be in accordance with Swedish national law.**
- **Any provisions, articles, sections etc. in FWA which sets out any kind of commitments for third parties have been excluded.**
- **FWA/S is applicable for NCP/S in its execution of the epSOS-services in Sweden.**
- **FWA/S can not set out any commitments for third parties.**
- **For the sake of comparision between the FWA and the FWA/S a cross-reference, written in blue, is noted under each section or article. A cross-reference is not a guarantee for full correspondence between the FWA and the FWA/S.**

Circle of trust

The "circle of trust" and "trusted domain" as used in D2.1.2 and FWA has no legal standing and cannot take precedence over Swedish law or the Swedish legal system.

Priority of interpretation

In any conflicts arising out of this agreement the Swedish national law takes priority over the FWA or any other epSOS agreements or other documents, whatever the standing of the document.

Preamble

Excluded in FWA/S as it contains the general epsos policy and is not applicable to the FWA/S. Information and policies which are in correspondence with the FWA/S are noted below each corresponding passage.

- The epSOS Large Scale Pilot Project has been established to develop and test a pilot system of cross-border data sharing to support patient care delivered to European citizens outside

their usual state of residence by means of a shareable electronic Patient Summary and ePrescription.
The FWA/S has similar information, see bilaga 1 (Annex 1).

- The Framework Agreement and its annexes is designed 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.
  Sweden does not recognize the existens of a legally binding level of trust and all references to this are excluded in the FWA/S.

- This Framework Agreement provides a blueprint for national level contractual agreements, where required[11], to create a National Contact Point [hereinafter NCP] as a legal entity entitled to process patient data in the context of the epSOS pilot.

- The Framework Agreement also sets out the core duties of the NCP and its partners so that the NCPs, once created, may contract on a common basis with their local partners (Healthcare Providers [Art 3 lit g Directive 2011/24/EU], Health Professionals and Points of Care) to deliver the epSOS services to Patients (Art 3 lit h Directive 2011/24/EU).

- Annexes I and II of the Framework Agreement give further guidance on the information to be given to Patients and Health Professionals on their rights and duties within epSOS.
  The FWA, Annex I and II are included in the FWA/S as Annexes 3a and 3b.

- The articles of the Framework Agreement and its annexes shall be transposed into:
  - (where necessary) Contracts under applicable national law to establish epSOS NCPs and
  - (where necessary) Contracts under applicable national law to designate Points of Care from within existing Healthcare Providers as epSOS Points of Care.
- The terms of this Framework Agreement and its annexes may be modified during transposition into local contracts and guidelines only in so far as it is necessary to do so in order to comply with local law or custom.
- The contractual agreements established at national level to create the NCPs shall be certified as conformant to epSOS principals by the Project Steering Board.

[11] Some Participating Nations may not need to establish NCPs by contract if, for example, the national administration provides the service itself.

2. The epSOS pilot – Creation of the epSOS National Contact Point (NCP)

Excluded in FWA/S, but the gist of this section is equivalent to the "Ingress (A)" and Annex 1 (bilaga 1) in FWA/Sweden.

9.4. The epSOS pilot is an initiative of several European Participating Nations to develop and test a system for access to health data in cross-border situations to support patient care delivered to European citizens outside their usual state of residence by means of a common epSOS electronic patient summary and a common epSOS e-prescription.

9.5. The national and regional Departments of Health and their related eHealth Competence Centres are beneficiaries of Grant Agreement number 224991 of the European Commission and its associated Consortium Agreement.

9.6. In accordance with the Grant Agreement the beneficiaries have contracted with the European Commission and each other to ensure that a number of healthcare establishments within their territory will provide one or more test sites for the epSOS Pilot – hereinafter known as a healthcare provider.

9.7. Each participating nation shall appoint one legal entity to act as NCP. Where this function is federated across several organisations one entity shall act on behalf of the others to be the liaison point for NCPs from other epSOS nations.

9.8. In the case of regional beneficiaries one NCP will represent all regional beneficiaries.

9.9. The NCP in each PN shall be created under local law on the basis of the present framework agreement.

10. Core Characteristics of the epSOS National Contact Point (NCP) (Terms to be included in all national contracts relating to epSOS)

FWA/S 2.

10.1. The NCP shall be a legal entity which is legally competent to contract with other organisations in order to collaboratively carry out its duties and responsibilities in epSOS.
FWA/S 2.1 The requirement to "collaboratively carry out duties" is excluded in the FWA/S. Contracts binding third parties are not in accordance with the Swedish legal system.

10.2. The NCP shall contract with epSOS Healthcare Providers to provide epSOS services to Patients.
FWA/S 2.1

10.3. The semantic transformation is performed according to the translation, mapping and transcoding carried out by designated competent legal entities in the epSOS countries
FWA/S 2.2

10.3.1. the responsibility for the *accuracy* and integrity of the process is with each national designated competent legal entity for such semantic processing
FWA/S 2.2

10.3.2. liability for errors in the semantic mapping is shared between the parties who have been involved in the production of the PS or ePrescription.
Excluded in FWA/S - FWA/S regulates only the NCP/S

10.3.3. Pilot sites are not liable for any patient safety adverse events attributed to semantic mapping, save for any contributory negligence in interpreting the data.
Excluded in FWA/S

10.4. The epSOS NCP 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 epSOS use cases (see end note).
FWA/S 2.5

10.5. The NCP 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 NCP shall:
FWA/S 2.4 regulating only responsibilities for the NCP as the FWA/S.

10.5.1. be technically competent to provide a gateway for epSOS information transfer;
FWA/S 2.6

10.5.2. be legally recognised as a data controller or data processor in accordance with domestic data protection legislation;
FWA/S 2.6

10.5.3. be legally competent to execute contractual agreements with all domestic partners in compliance with domestic data protection legislation;
Excluded in FWA/S – NCP/S is a governmental body

10.5.4. be legally competent to enforce audit and corrective action emerging from audits;
Excluded in FWA/S

10.5.5. be technically competent to validate the identity of Patients and patient consent of its territory (acting as country A);
FWA/S 2.8

10.5.6. maintain the local versions of the epSOS semantic value sets.
FWA/S 2.9

11. General Duties and responsibilities of the epSOS NCP (terms to be embodied in the national contracts creating the NCPs)
FWA/S 3

11.1. The epSOS NCP shall establish appropriate security and data protection systems to conform to epSOS requirements as well as all applicable national requirements.
FWA/S 3.1

11.2. The epSOS NCP shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).
FWA/S 3.2 1st sentence

The epSOS NCP shall establish 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 epSOS NCP in another nation.

FWA 3.4

The epSOS NCP shall establish an appropriate 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 NCP A from all parties concerned and handed over to a Patient or a Healthcare Provider requiring such information. The epSOS NCP shall assume responsibility for appropriate data collection on the execution of the pilot through the Points of Care on its territory and shall assume responsibility for the reporting of such data to the epSOS Project Partner(s) on its territory.

Excluded in FWA/S as the provision is not in accordance with Swedish legislation.

11.3. The epSOS NCP must ensure that nominative epSOS data is not transmitted to parties outside the NCP and its pilot partners.
FWA/S 3.3

11.4. The epSOS NCP shall maintain a helpdesk service to support the Health Professionals and Healthcare Providers in its territory.
FWA/S 3.5

11.5. The epSOS NCP maintain the communication on epSOS pilots at national level and links to the epSOS website.
FWA/S 3.6

12. epSOS NCP duties and responsibilities to other epSOS NCPs

The entire chapter is excluded in FWA/S.

12.1. The epSOS NCP shall be accountable to other epSOS NCPs for ensuring the security (confidentiality, integrity, availability, non repudiation and authenticity and auditability) of data processed on their territory.

12.2. The epSOS NCP shall be accountable to other epSOS NCPs for guaranteeing that all epSOS jointly agreed service specifications and requirements (legal, organisational, semantic and technical) are fulfilled.

12.3. **T**he epSOS NCP shall be accountable to other epSOS NCPs, represented through the PSB, for ensuring, conformance of all epSOS national pilot partners to jointly agreed service specifications and requirements.

12.4. The epSOS NCPs shall collaborate actively to the harmonisation of guidelines and appropriate practices to facilitate the establishment of the epSOS trusted domain.

12.5. The epSOS NCPs shall adopt the epSOS Information Governance framework that will comprise commonly adopted policies, processes and audit mechanisms.

12.6. The epSOS NCPs must ensure that national agreements with pilot partners include provisions for applying and regularly auditing the epSOS Information Governance framework. Such audit practices applied by NCPs shall be audited by an external independent auditor.

13. Duties and responsibilities concerning epSOS Patient Consent (terms to be embodied in the national contracts creating the NCPs and contracts between NCPs and their partners as appropriate)

FWA/S 4

13.1. No epSOS data shall be collected either directly from the Patient or indirectly from Healthcare Providers without the freely given, specific and informed consent of the Patient, according to national law of the country where treatment is provided.
FWA/S introduction

13.2. The epSOS pilot shall be conducted on the basis of an opt-in system of consent; accordingly implied consent to epSOS data collection and processing shall not be permitted.
FWA/S introduction

13.3. The epSOS NCP shall ensure (directly or through appropriate contractual agreements with their Points of Care that consent is obtained and documented for the creation of epSOS records (Patient Summary and ePrescription) if required by national law.

FWA/S 4.1 – the article har been exteneded and applies to any records that may be created during the execution of the epSOS LSP.

13.4. The epSOS NCP can establish a system which allows a patient to give a prior general agreement to access to his or her record by a Health Professional or Point of Care or Healthcare Provider abroad.
FWA/S 4.2

The epSOS NCP shall establish with its partners a process which allows such general prior agreement, if required by national law of country A, to be validated at the Point of Care. Such validation procedures shall be e.g. by ticking a box to confirm patients' consent for access to their Patient Summary or ePrescriptions held in their home country and shall not be disruptive of the clinical workflows.
FWA/S – excluded but is partly covered by the provision in FWA/S 2.1 and 4.3

13.5. The epSOS NCP shall establish a system to allow a Point of Care providing services to an epSOS patient to document the validations of consent for release of data from the NCP to the Point of Care.
FWA/S – excluded but is partly covered by the provision in FWA/S 2.1 and 4.3

13.6. The epSOS NCP may establish a system for directly obtaining agreement from the patient in situations where prior generalised agreement has not been provided in country A, in all cases where country A permits such delegation of responsibility.
FWA/S 4.3

13.7. The epSOS NCP shall establish a consent override procedure to provide for exceptional cases where it is not possible to obtain consent or validation of consent because of the patient's incapacity including consent for minors. The epSOS NCP shall ensure that all the parties concerned with the pilot are able to comply with the requirements of patient consent to epSOS data collection and processing.
FWA/S – 4.4

14. Duties and Responsibilities of the epSOS Pilot Partners under the epSOS Security Policy

FWA/S 5

14.1. The epSOS security policy creates a general security and data protection framework adapted to the epSOS information system needs.
FWA/S 5.1

14.2. The epSOS security policy address all elements of data flows in the pilot including national and cross-border data flows.
FWA/S 5.2

14.3. The epSOS actors (epSOS NCPs, Health Professionals, Points of Care and Healthcare Providers) shall ensure that they are fully compliant with the Security Policy as set out in detail in Annex III.
FWA/S 5.3 regulating NCP/S

15. Relationship between NCP and Points of Care, Health Professionals and Healthcare Providers

FWA/S 6. – the majority of the articles are excluded in the FWA/S as it is not possible to set down binding obligations for third parties in the FWA/S.

15.1. A number of partners in the epSOS pilots shall be legally established and recognised. They shall include Points of Care and Health Professionals, and may also include Healthcare Providers representing several Points of Care.
excluded in FWA/S – Health providers in Sweden are always legally established and recoginised. All health providers acting in Sweden can by choice participate in the LSP epSOS.

15.2. Each PN will identify a number of Healthcare Providers which will take part in the pilot. These shall include primary care providers (general practitioners and primary care clinics); secondary care providers (hospitals specialist secondary care providers); pharmacies (both public and private).
FWA/S 6.1 but the identification will be done by the NCP/S.

15.3. The Healthcare Provider shall sign a contract under local law with the NCP to which it is responsible.
FWA/S 2.1 – The NCP/S undertakes to regulate its cooperation with Pilot Partners through through legally bindig contracts. The contracts shall, when possible, be in accordance with the FWA/epSOS.

15.4. The Healthcare Provider/NCP contract shall set out all the minimum requirements of the Point of Care and shall establish the legal relationship between them.
Excluded in FWA/S

15.5. The Healthcare Provider/NCP contract shall set out minimum requirements for epSOS training for all health professionals who shall be active within the pilot.
exclude in FWA/S

15.6. The Healthcare Provider/NCP contract shall detail the duties of both parties with respect to maintaining the security of the epSOS pilot and all data flows.
exclude in FWA/S

15.7. The Healthcare Provider/NCP contract shall detail the duties of both parties with respect to ensuring that patient consent to collecting and processing epSOS data has been duly obtained and documented according to epSOS procedures.
exclude in FWA/S

16. Dispute resolution and applicable law

FWA/S – section 14

Sweden only recognizes the Grant Agreement (GA) as a contract specifying the financial contribution by the Community, represented by the Commission, to the consortium. The Consortium Agreement (CA) specifies the organisation of work between parties and to be delivered by the parties. It is made to fulfil the obligations of the beneficiaries to the contract (GA). The CA also sets out the rights and obligations of the parties. Grant Agreement , Annex I – Description of Work specifies (among other clauses) the overarching goal, operational objectives and key measurable outputs. None of these documents includes any obligations for PNs to implement the result of the Work Packages deliverables or decisions by PSB regardless of national law or any other objections. National law, in this case Swedish law will always have precedence in case of any legal conflict.

16.1. The co-operation between NCPs shall be ensured through the Grant Agreement.
FWA/S – excluded

16.2. Any conflicts arising between NCPs shall, in the first instance, be referred to the PSB. A request for arbitration may be filed with the European Court of Arbitration in the event of any dispute which cannot be resolved at project level.

FWA/S – excluded

17. Amendments of the Framework Agreement

FWA/S – excluded

17.1. Amendments to this Framework Agreement, its Annexes and any related epSOS policies which have been duly adopted in accordance with project procedure through the epSOS Project Steering Board (PSB), shall be translated and applied to the contracts for epSOS services as provided for in the preamble. The National Authority Beneficiary (NAB) shall give appropriate publicity to the adopted amendments as well as the decision of the PSB not later than 4 weeks after the amendments have been adopted by the PSB.

17.2. Save from the NABs, all parties to the above mentioned contracts shall have the right to rescind the contract during the 16 weeks following the PSB decision.

17.3. Unless otherwise defined by the PSB, the amendments to the above mentioned contracts shall come into effect 16 weeks after the amendments have been adopted by the PSB.

ENDNOTE – Steps in epSOS Process

FWA/S – annex 6

11. Health Professional in country B at a Point of Care accepts patient ID which may identify the patient as being eligible to take part in epSOS trial.
12. 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.
13. Health Professional in country B sends query to NCP in country B.
14. NCP in country B authenticates the Health Professional and Point of Care.
15. The NCP in country B queries NCP in country A for the requested patient data.
16. NCP in country A authenticates NCP in country B.
17. NCP in country A validates patient ID and local prior agreement (if applicable).
18. NCP in country A transmits the requested data to NCP in country B.
19. NCP in country B authenticates NCP in country A.
20. NCP in country B provides the requested data to Health Professional requestor.