Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of Patient Summary and Electronic Prescription

D3.8.2 Final National Pilot Set Up and Deployment Guide

Version 1.1

WORK PACKAGE	**WP 3.8**
DOCUMENT VERSION	**1.1**
DATE	**17/09/2010**

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	D3.8.2 v1.1
Distribution level	**Public**
Status	Final
Author(s): **Organisation:**	**Digital Health**

Dissemination level: PU = Public, PP = Restricted to other programme participants, RE = Restricted to a group specified by the consortium, CO = Confidential, only for members of the consortium.

ABSTRACT
Document name: D3.8.2 Final National Pilot Set Up and Deployment Guide WP3.8 “Integration and customisation” creates a Pilot Setup Guide supporting the Competence Centres and national experts in setting up their National Contact Points.

History of Alteration				
Version	**Date**	**Status Changes**	**From**	**Review**
V0.1	2010-06-24	Draft based on D3.8.1	Digital Health	
V0.2	2010-07-15	Input from beneficiaries	Digital Health	
V0.3	2010-07-22	Sequential Implementation Guidelines updated	Digital Health and beneficiaries	Internal review
V0.4	2010-07-27	Including comments from internal review	Digital Health	
V0.5	2010-07-28	Corrections after TCON	Digital Health	
V0.6	2010-07-29	With status as “Public Draft”	Digital Health	Quality review
V0.7	2010-08-31	After quality review	Digital Health	
V0.7	2010-09-08	Minor editorial adjustments	Digital Health	
V0.8	2010-09-13	Adjustments after final tcon	Digital Health	
V1.0	2010-09-13	Editorial changes	Digital Health	
V1.1	2010-09-17	Changes from Fredrik Linden	Digital Health	

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 7
2 INTRODUCTION 10
2.1 Scope and Goal of WP 3.8 10
2.2 Timing and expected outputs 11
2.3 Overview (Birds perspective) 12
2.4 Reading instruction for Guidelines 12
2.4.1 Structure of the Document 12
2.4.2 Use of drawings in the Document 13
2.5 Relationship with other WPs 14
3 WORKING METHODOLOGY 15
3.1 Progress in WP3.8 15
3.2 Writing guidelines 15
Main Contacts 16
3.3 Timeline of the WP3.8 17
GUIDELINES 18
4 Technical Issues 18
4.1 Functional & Technical Content References to WP3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, JWG 18
4.2 Architecture of epSOS 20
4.2.1 Overall Structure and Components 20
4.2.2 Interoperability 20
4.2.3 Interfaces 20
4.3 Setting up a NCP 21
4.3.1 NCP Components in Common 21
4.3.2 NCP Customisation 23
4.4 Technical Aspects of epSOS 23
4.4.1 Interconnectivity 23
4.4.2 Patient Identification 24
4.4.3 Patient Consent 24
4.4.4 HCP Authentication 24
4.4.5 Semantic Services 25
4.4.6 Patient Summary Service 25
4.4.7 ePrescription/eDispensing Service 26
4.4.8 Consistent Time 27
4.4.9 Platforms 27
4.5 Central Services 27
4.5.1 Example of possible solution (a virtual central service) 27
4.6 Test Procedures 29
5 Legal Issues 30
5.1 *Contractual aspects* 30
5.1.1 Framework Agreement 30
5.1.1.1 Forming local variations of the Framework Agreement 30

5.1.1.2 Process for agreeing on local variations of the FWA 30
5.1.1.3 Signing of FWA 30
5.1.2 Legal Establishment of NCP 31
5.1.3 Legal relationship between NCPs 31
5.1.4 Legal recognition of Point of Care and Healthcare Organisation 32
5.2 *Clinical Aspects* 32
5.2.1 General Information 33
5.2.2 Data availability/integrity/confidentiality 35
5.2.3 Patient Consent – Information to be Provided, Processes for Confirming and Documenting Consent 35
5.2.3.1 Information on epSOS duties for Patients and Healthcare Professionals 36
5.3 *National and European Rules, Laws and Directives* 36
5.3.1 The effect of different laws 37
5.3.2 EU Directives 37
5.4 Liability 38
6 Organisational Issues 39
6.1 Establishment of NCP organisation 39
6.1.1 General NCP Organisation 39
6.1.2 Description of Organisational NCP Roles 39
6.1.2.1 Organisational issues stemming from the NCP's functional behaviour 39
6.2 NCP Operating Organisation (Selected Processes) 40
6.2.1 Support Organisation. 40
6.2.1.1 Incident Management 40
6.2.1.2 Problem Management 41
6.2.1.3 Change Management 42
6.2.1.4 Service Level Management 42
6.2.1.5 Configuration Management 45
6.2.1.6 Security Management 45
6.3 Security Organisation 46
6.4 Auditing Organisation 47
6.5 Central Services 47
6.6 Organising the Test Procedures 47
6.6.1 Gazelle 47
6.6.1.1 Simulators 48
6.6.1.2 Test Data 48
6.6.2 Lab Tests 48
6.6.2.1 Test of Common Components of FET 48
6.6.2.2 Test of National Connector within MS 48

6.6.2.3 Tests from/to National Connector from/to NCP 48
6.6.3 Projectathon (PAT) Pre-Tests 49
6.6.4 Projectathon 49
6.6.5 Pre-Pilot 49
6.7 NCP Roles 49
7 Practicalities 52
7.1 Manual processes 52
7.1.1 How to run the NCP in daily use 52
7.1.2 How to handle epSOS at the PoC 53
7.2 Manual regulations to run the NCP 54
7.2.1 Servers to be used for the NCP – virtual/dedicated 54
7.2.2 Securing the server room and servers 55
7.2.3 Training System administrators and other support staff 55
7.2.3.1 Objectives 55
7.2.3.2 Training Process 55
7.2.4 Nondisclosure agreement for system administrators 56
7.3 Marketing Activities 57
7.3.1 Hospitals and GPs 58
7.3.2 Citizens/Patients 58
7.3.2.1 Country A, target group 1: Citizens and residents 59
7.3.2.2 Country A, target group 2: National Patients 60
7.3.2.3 Country B, target group 3: epSOS patients 60
7.3.3 Public Information Policy 61
7.4 Communication Structures 62
7.4.1 NCP as Communication Centre 62
7.4.2 Single Point of Contact 63
7.5 Semantic Services (MVC and MTC) 64
7.5.1 Transcoding and Mapping 64
7.5.2 Translation 65
7.5.3 Semantic safety issues 66
7.5.4 MTC Maintenance 66
8 Guidelines for epSOS pilot evaluation 68
8.1 Introduction: Scope and Intended Audience 68
8.2 General Guidelines 69
8.3 Contextualisation Guidelines 69
8.4 Interaction Guidelines 70
9 Step-by-Step Description 71
10 GLOSSARY 75
11 ABBREVIATIONS 79
12 LIST OF FIGURES 81
13 Annex I: Security 82

14 Annex II: Sequential Implementation Guidelines 83
Annex III: Danish example (per 15 July 2010) of using the Sequential Implementation Guidelines 89
15 Annex IV: Austrian Example 95
16 Annex V: Visualisation of the Sequential Implementation Guidelines 96
17 Annex VI: Requirements and Recommendations - checklist 97
18 Annex VII: NCP Customisation 98
18.1 Danish NCP Example 98
18.1.1 Overview of Data Source and Selected Integrations 98
18.2 Security Authentication & Audit Traceability 99
18.3 Spanish NCP Example 99
18.3.1 Motivations and State of the Project 99
18.3.2 Functional Architecture 100
18.3.3 Lessons Learned 102

1 EXECUTIVE SUMMARY

This is the Final Guidelines for National Pilot Set Up and Deployment produced by WP3.8. The document has the project related administrative chapters in the beginning. The history of the document shows the decision of WP3.8 to describe how to set up the NCP and base the document upon deliverables and output from other WPs, and not to be involved in each single Member States (MS). Guidelines are mostly directed at the relevant professionals in the MS. Guidelines are referring to all previous and current WPs. Latest agreed time schedules for D3.8.1 and D3.8.2 show delays in relation to Annex 1, caused by the delay of other WPs and delayed decisions.

After the administrative chapters come the actual guidelines in chapter 4, 5, 6, 7, 8 and 9. Glossary, abbreviations and list of figures is found in chapter 10-12. Seven annexes have been added in the end of the Guideline document.

In chapter 4, you will find a reference structure which will guide readers to content of the technical deliverables (WP3.1 to WP3.7, WP3.9 and HLDD). The epSOS architecture and components are based on a SOA paradigm with SOAP for information exchange, using epSOS backbone (the internet). The architecture, components, security, etc. are from technical WPs. The epSOS architecture shows NCP A with “Common Component” design and NCP B, where also a Portal is included. A minimal central service structure is included in the epSOS technical/organisational solution. The interfacing between the National Infrastructure and Common Components is, as part of the National Connector, described in the separate High Level Design Document, and will also be described in specification from Fraunhofer – ELGA – Tiani (FET). The Danish example in Annex VII shows integration between the Danish data sources and epSOS. A Spanish example is also included in Annex VII.

In chapter 5, legal relationships have been described. Legal input is mostly from WP2.1 and therefore you will find footnotes to D2.1.2. In relation to D2.1.2, chapter 5 is intended to be practical for better understanding by the MSs. In Contractual aspects is explained how to localise the Framework Agreement (FWA) which could be agreements/contracts between Points of Care/Pilot sites and the epSOS NCP. Such agreements/contracts must be signed with copy to PSB. It is explained how Grant Agreement/Consortium Agreement connect the national NCP organisations. In Clinical Aspects the Security aspects you will find that it is the epSOS Security Policy together with the FWA which constitute the agreement structure to be audited, and which give responsibility in a MS towards the rest of the epSOS community. The Commission decision that the System owners bear responsibility and the Data Protection Directive must be recognised. Availability, Integrity, Confidentiality and Patient content are part of the epSOS Security Policy, and must be followed. The Security Policy document can be found in Annex I in the Guidelines. In National and European Rules, laws and Directives 5 important EU Directives/Rules are listed, but it is important to note, that the guiding principle of epSOS is that a patient travelling is treated according to country B (the foreign country). In Liability it is pointed out, that at present no specific legislation of eHealth liability at EU level exist. Any person who suffers harm may claim compensation. Liability is also concerning design and implementation. Pilot partners have analysed the situation.

Chapter 6 is the chapter for organisational issues. The main topic is organisational setting up of the NCP and here the reader will be informed about NCP organisation, NCP operating organisation and related issues, security organisation and auditing organisation. MSs must care for setting up the necessary NCP organisation. This means that MS must have epSOS Incident Management, Problem Management, Change Management, Service level management with SLA according to epSOS demands, Service Desk SLA according to epSOS demands, Configuration Management and Security Management. In epSOS there must be formed a Security and Auditing Organisation guaranteeing to fulfil the Security policy with Security Baseline Document.
The demands concerns i.e. servers, server rooms, Non Disclosure Agreements, Back-ups and many other issues, (detailed description in Annex I). To perform the test procedures for NCP and

Point of Care (PoC) in epSOS is a major task for the MS. It also implies participation in Projectathon and the preparation. MS must recognise the Central services, which the organisation must be able to handle. The many NCP Roles should be studied by MS to ensure compliance.

Chapter 7 concerns practical activities needed for setting up and running the NCP. It is about how MSs should run the NCP in daily use, how the NCP servers should be secured and how to handle marketing activities. You will also find a chapter about communication structures and a chapter about semantic services. It is up to the MS to decide how to run the epSOS business in its country as long as the procedures comply with epSOS' rules. Nevertheless, setting up organisation and hiring staff is necessary and so is managing staff. Procedures in Pharmacies, Hospitals and GP Clinics on how to handle epSOS correctly must be described. Training of staff in the MS is mentioned as an important part of the needed practically manual procedures to be performed. Marketing epSOS is advisory explained for the MS. It concerns marketing for professionals as well as for the citizens in a particular country. Citizens should preferably be informed before travelling and therefore before health care is needed. epSOS has proposed a Communication structure with Single Point of Contacts for being able to ensure communication during and after Pilots as well as during the preparation of the Pilots. Each MS must set up the needed catalogues (MVC and MTC) before start of epSOS and have a practical and secure solution to maintaining the Semantic Services. Find description in these Guidelines and in referred documents.

Chapter 8 has mostly been written by members of WP1.2. By reading this chapter, the reader obtains knowledge about evaluation activities in epSOS. As epSOS is a large scale pilot project, evaluation is an important task, and therefore it is of great value to explain the evaluation structure to the MSs. The evaluation Guidelines must be followed by the MS. MS should have an evaluation team for working with the evaluation template. The evaluation plan in MS must be an adoption of the epSOS evaluation plan. This plan or guidelines will contain: Technical parameters, Use of parameters/indicators, plan for Doctors and for Administrative staff. MS must appoint evaluation staff at NCP and at Pilot level, and staff for managing the evaluation in the country.

In chapter 9 you find a step-by-step description of the patient and information flow between countries (A and B). In this process description you will find all important steps, as i.e. the consent process.

Annex I consists of three documents. The first, which is attached below (and original version can be found in the D3.8.2 folder on ProjectPlace or here: (https://service.projectplace.com/pp/pp.cgi/r492884389) is the NCP Security Policy. The second, called NCP BSP details-compact.pdf can be found in the D3.8.2 folder on ProjectPlace (or by using this link: https://service.projectplace.com/pp/pp.cgi/r495440632) and the third is the security ncp bsp checklist.xls which can be found in the D3.8.2 folder on ProjectPlace (or by using this link: https://service.projectplace.com/pp/pp.cgi/r492869378).

Annex II is "Sequential Implementation Guidelines" which is a help to the MS for implementing the NCP and prepare the pilot sites. The main steps in implementing epSOS (NCP) are described. It gives MS and WP 4.2 a tool to use when planning the implementation.

Annex III is a Danish example of using the "Sequential Implementation Guidelines" in Annex II.

Annex IV is Austrian example of Implementation planning.

Annex V is Visualisation of Sequential Implementation Guidelines. The graphics shows how some of the steps can be understood. There are conditionally steps and alternative steps.

Annex VI is Requirements and Recommendations. This living document is a part of D3.8.2. It is placed at ProjectPlace and https://service.projectplace.com/pp/pp.cgi/r511702212 is a link to the document. The Requirement and Recommendations is a general checklist for the "D3.8.2 The

Final national Pilot Set Up and Deployment Guide" with possibilities of sorting the subjects into different criteria. The list can be extended over time.

2 INTRODUCTION

According to Annex I and the original plan for the work of WP3.8, the outcome of this WP should have been slightly different than it is now.

Originally, one of the tasks for WP3.8 (T3.8.1) was to form a workgroup with participants from national pilots, competence centres and industry which should compare relevant existing infrastructures and pilot IT systems which could be used in the participating national pilots. As part of this task, WP3.8 planned to perform gap analyses in all piloting countries. During the kick off meeting in Rome in September 2009, however, it was agreed that the gap analysis was a national issue and not a task for WP3.8. In general, the national side of the NCP is left for the MS to handle themselves together with local experts. Consequently, the second task (T3.8.2) which was supposed to build on the national descriptions from T3.8.1 and develop common guides and models for integration and customisation local IT systems, was not relevant anymore. Rather than building on national descriptions, WP3.8 builds upon deliverables and output from other WPs. The last task of WP3.8, according to Annex I is to describe how MS set up their NCP. This is what this document is doing.

At one point, it was the intention that everybody, regardless of background, should be able to read and understand the guidelines. However, in order for the guidelines to be useful, it was decided that the different chapters in the document should be directed at the relevant people and hence, written in a language and level of detail that is useful for that particular target group. Furthermore, as this guide is in English, it is the job of the national epSOS team to make sure that the national pilot teams and experts understand the guidelines.

2.1 Scope and Goal of WP 3.8

WP3.8 “Integration and customisation” creates a Pilot Setup Guide supporting the Competence Centres (CC) and national experts in setting up their National Contact Points (NCP).

In WP3.3 to WP3.7 the common technical specifications and modules and the overall European architecture in epSOS are defined. In order to help the MSs implement their NCP based on the work done in WP2.1 and WP3.1-3.7, WP3.8 provides these guidelines.

In epSOS, the national pilot IT systems are integrated and customised to be able to exchange ePrescriptions and Patient Summaries with pilot sites in the other European countries. How this integration and customisation is done differs between the different national pilots, depending on the national IT infrastructure in the actual pilot.

The important task for WP3.8 is to obtain substantial and sufficient knowledge from WP2.1 and WP3.1-3.7 and the work carried out in the Joint Working Group WP3.8/3.9 (JWG) in order to be able to capture all technical, organisational and legal requirements needed to set up a NCP. Information from WP3.9, concerned with developing the epSOS pilot system should also be included. Further information about testing and testing tools from WP3.9 shall be used for writing guidelines for test tools and test plans for the NCP. WP3.8 also coordinates with WP4.2 and provides input for their pilot template.

In short, the following should be achieved by WP3.8:
Write up a set of Guidelines for setting up NCP both related to:
a) Organisational/Legal/Practical/Evaluation matters, and
b) Technical matters

2.2 Timing and expected outputs

Milestones		
Date	**Deliverable**	**Description**
End Aug 09		Initiation Document, WP plan and TOC
Mid Sep 09		F2F Kick Off meeting
End Jun 10	D3.8.1	Draft National Pilot and Deployment Guide
Mid Sep 10	D3.8.2	Final National Pilot and Deployment Guide

Figure 1: Milestones

Deliverables		
D-No.	**D-Title**	**Description**
Unofficial	Overview of Guidelines	Table of Contents
Unofficial	Requirements	Requirements for technical Issues (From High Level Design Document from Joint Working Group WP3.8/3.9)
D3.8.1	Draft National Pilot SetUp and Deployment Guide	Practical guide describing how to customise the pilot infrastructure to fit with the common European epSOS framework (Legal Issues, Organisational Issues, Practicalities and Evaluation Matters). This version has gaps due to open issues in epSOS.
D3.8.2	Final National Pilot SetUp and Deployment Guide	Final guide; reviewed, quality assured and approved.

Figure 2: Deliverables

2.3 Overview (Birds perspective)

The guidelines are based on material and deliverables from other WPs. The figure below gives an overview of what deliverables and other input from working groups are used as basis for the different chapters in this deliverable.

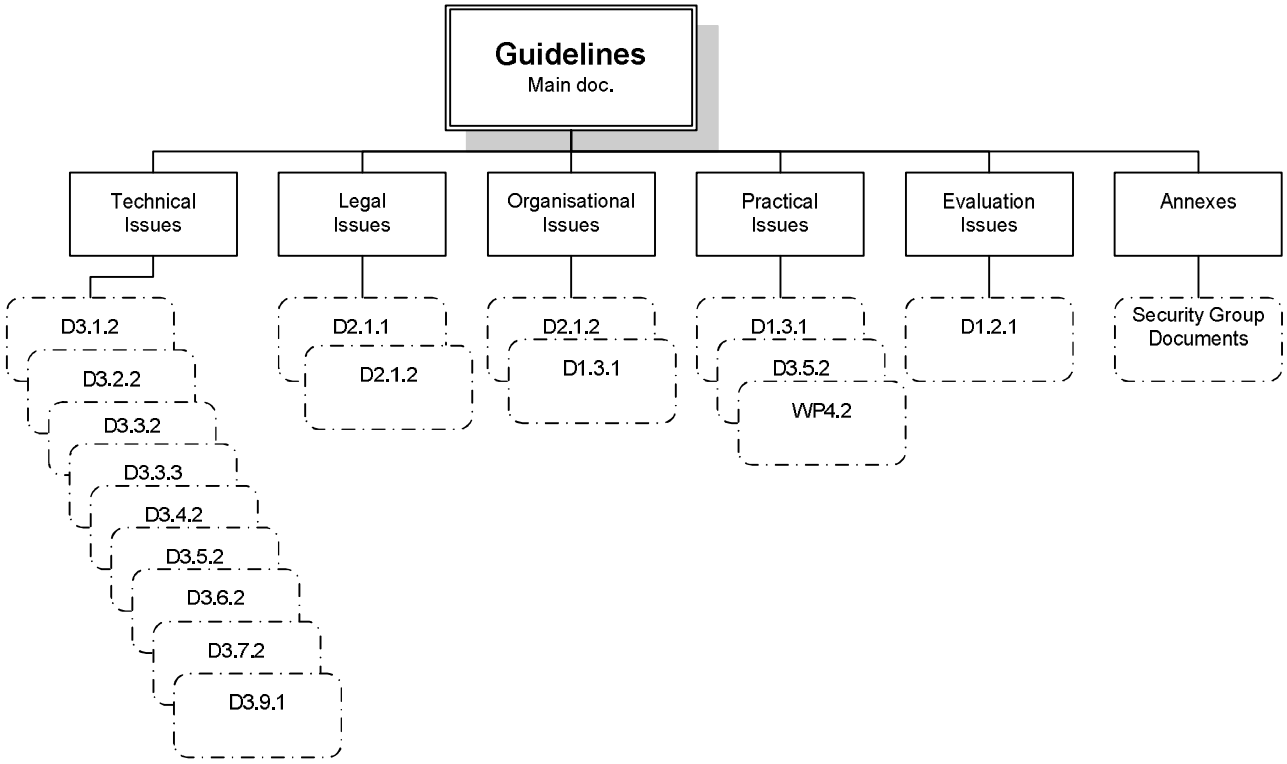


Figure 3: Bird's perspective

2.4 Reading instruction for Guidelines

This chapter is meant to help the reader understand how this document is build up and in which way it can best be read.

2.4.1 Structure of the Document

The main structure of the document is illustrated below.

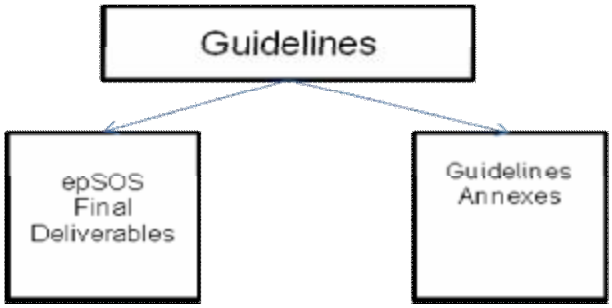


Figure 4: Structure of the document

The Guidelines are here the part of this document which contains the operational chapters: Technical Issues, Legal Issues, Organisational Issues, Practicalities and Evaluation.

The Guidelines will refer to either the final deliverables from the different WPs in the epSOS documentation or to Annexes in this document. The WP documents can be found at ProjectPlace and, when they have been finally approved, at the epSOS website.

In the WP documents the reference will primarily point at a page number or at a certain chapter. If the subject cannot refer to such precise point, the whole epSOS document will be the reference.

In the Cover and Control page you will find a useful versioning of the guideline document.
The Guideline document is structured with useful information about the background for the Guideline document and about the document itself in main chapter 2 and 3. The *Executive Summary* is placed in Chapter 1.

Chapter 4-9 are the operational chapters of the Guidelines. Subjects are placed in one of the 4 main-chapters best possible, however, as some subjects belong to more than one main chapter, sometimes it will be necessary for the reader to refer to several chapters/sections of the document. For instance, you will find all legal subjects in chapter 5, *Legal Issues*, but it has been more appropriate to place “Nondisclosure agreement” in the main chapter 7 Practicalities, as it also concerns system administration.

In all sections (second level) you will find an introduction to the chapter. It gives a brief description of what is in the chapter, and if the chapter is dedicated to a certain professional group in epSOS. Chapters in the Guidelines can be read by all, but a certain chapter can be more valuable for one or more professional group.

It has been decided to use a “Road Map” structure for chapter 4, *Technical Issues*. It would be pointless to rewrite the output from the technical WPs, as the final documents from the WPs should be read and understood in their totality. Consequently, chapter 4 lists relevant subjects for the technical setup of the NCP and references are made to relevant technical documents.

The design for a ‘NCP-in-a-box’ developed by the JWG (WP3.8/3.9) is documented in the High-Level Design Document (HLDD) which is now part of D3.9.1. The design is not normative, but is used in the “Road Map” – chapter 4 as examples of possible implementation

Operative chapters are followed by auxiliary chapters: Glossary, Abbreviations etc. (Chapter 10-12).

Three annexes are included: Annex I “Security”, Annex II: “Sequential Implementation Guidelines” and Annex III: “Danish example of Sequential Implementation Guidelines”.

An important part of the guidelines is the checklist which is a living document in Excel form and can therefore not be added physically to this document. The newest version of the checklist can be found in the D3.8.2 folder on ProjectPlace [https://service.projectplace.com/pp/pp.cgi/r498254036].

Important note:
Please note that chapters 1-3 are practical epSOS related and methodological information whereas chapter 4-9 are the actual guidelines which should be used for implementation of the NCP.

2.4.2 Use of drawings in the Document

Drawings in this document are illustrative. Where normative content is necessary it is expressed in text.

2.5 Relationship with other WPs

It is important not to refer to documents which are not stable, as it could cause misunderstandings if references points to wrong parts of a document.
The tables below depict the necessary inputs and outputs required from and to other WPs.

Work Package/ Task	Required Input
WP1.2	D1.2.1 Project Evaluation Methodology and Plan
WP2.1	Legal requirements for NCP D2.1.2 Legal Standard Contract Terms for engagement of pilot sites
WP 3.1 and 3.2	D3.1.2 and D3.2.2 Definitions and service requirements for ePrescription and Patient Summary
WP3.3	D3.3.2 epSOS System technical specifications D3.3.3 Interoperability Framework
WP3.4	D3.4.2 Common components specification
WP3.5	D3.5.2 Semantic service specifications
WP3.6	D3.6.2 Identity management specification
WP3.7	D3.7.2 Security service specification
WP3.9	D3.9.1 epSOS Pilot System Components Specifications D.3.9.2 Testing Methodology, Test Plan and Tools
JWG	HLDD
SEG	Security Group documents

Figure 5: Required inputs from other epSOS WP

Work Package/ Task	Expected Output	Date
WP1.2	Input to evaluation of pilots	August 2010
WP4.2	Input to pilot template and checklists to help monitor the pilot implementation progress.	August 2010
WP4.3 and WP4.4	Pilot SetUp Guide is to be used by the national pilot for precondition preparation and site level preparations and pilot implementation.	September 2010

Figure 6: Outputs to other WPs

3 WORKING METHODOLOGY

This chapter explains the working methodology for writing the guidelines, including the participants in WP3.8 and a timeline.

3.1 Progress in WP3.8

The work which has taken place in WP3.8 prior to writing the guidelines is shortly outlined here:

August 2009 – Preparing Initiation document – including preliminary table of contents

September 2009 – Kick off meeting in Rome

October 2009 – Creation of working groups:
- Management
- Technical Group
- Joint Working Group (JWG) with WP3.9
- Legal and Organisational Group
- Editorial Group

October 2009 to April 2010 – Work in JWG

November 2009 – WGD revises table of contents for the legal and organisational part of the guidelines.

February 2010 – Revision of table of contents and assignment of tasks within the organisational and legal part of the guidelines.

June 2010 – finalisation of D3.8.1.

July 2010 – D3.8.2 gone through internal review and released as Public Draft in order to provide MSs with necessary information to be able to start pilot preparation.

September 2010 finalisation of D3.8.2 and closure of WP3.8.

3.2 Writing guidelines

In order to write coherent and useful guidelines without duplicating the work of previous WPs, a set of rules and an agreed method has been used. It is important to follow the same method for writing the different parts of the guidelines.

The guidelines should be based on the deliverables from WP2.1 and the whole of Project Domain 3 in epSOS.

When writing the Guidelines the following rules have been used:
1. Find all epSOS requirement related to the section in question.
2. Find the epSOS documents(s)/deliverable(s) where these requirements are dealt with, including the output from the joint working group.
3. New demands and ways to understanding or working within epSOS should not be proposed by WP3.8 *if good text is already available* in approved documents (mostly found in the Legal and Technical WPs). Based on these documents, we should write *short and understandable text and refer to chapters in the approved documents*. Where *no text is available* we should guide and advise MS. It will mostly be relevant in Organisational and Practical chapters.

4. Nevertheless, check if parts of available documents/deliverables can be used for Organisational Issues, Practical Issues etc.
5. In the guidelines, refer to the appropriate sections of documents/deliverables by name, chapter and page of the epSOS document
6. Make clear what are *requirements* and what are *recommendations*.
7. Identify missing key points, include them in the guidelines if possible, and make Work Package Leaders (WPL) aware of the lack.
8. Pure Legal text should be at Legal chapters, Organisational text in Organisational chapters and so on. Exceptions can be needed.

It is important to keep in mind that the guidelines should be readable and understandable for people who have not been part of epSOS' development. This might be people who will be part of developing epSOS components for the nation side of the NCP.

Main Contacts

MM	Beneficiary	Country	Contact name	e-mail address
16,0	**MedCom /Digital Health**	Denmark	Per Loubjerg Rasmus Melgaard Mie H. Matthiesen	pel@sdsd.dk rme@sdsd.dk mima@sdsd.dk
3,0	**ASIP Sante**	France	Alain Périé Elie Lobel	Alain.PERIE@sante.gouv.fr elie.lobel@sante.gouv.fr
5,4	**ELGA**	Austria	Gottfried Heider Tobias Pass	gottfried.heider@elga.gv.at tobias.pass@elga.gv.at
5,4	**IZIP**	Czech Republic	Milan Ruzicka	milan.ruzicka@izip.cz
5,4	**LOMBARDY**	Italy	Marcello Melgara Claudio Beretta Roberto Zuffada Natalia Allegretti	Marcello.Melgara@cnt.lispa.it claudio_beretta@regione.lombardia.it roberto.zuffada@cnt.lispa.it natalia.allegretti@cnt.lispa.it
5,4	**NICTIZ**	The Netherlands	Michiel Sprenger	sprenger@nictiz.nl
5,4	**SALAR**	Sweden	Eva Leach Elfgren Lena Jönsson	eva.leach@skl.se Lena.C.Jonsson@ltdalarna.se
5,1	**NHIC**	Slovakia	Andrej Fandak	andrej.fandak@beset.sk
4,0	NHS	UK	Jeremy Thorp	
3,0	THESS	Greece	Zoi Kolitsi Yiannis Salmatzidis	kolitsi@vivodinet.gr
2,7	ANDA	Spain	Marta Bonilla Grande	marta.bonilla.sspa@juntadeandalucia.es
2,0	Gematik	Germany	Anna Wolfe	anna.wolfe@gematik.de
1,6	CLM	Spain	Celia Varela Jose Sacristán	cvarela@externas.sescam.jccm.es jsacristan@sescam.org
1,5	INDUSTRY	EU	Ilia Fortunov Petra Wilson Nikos Kyriakoulakos Berler Alexander	epsos-industry-team-work-package-38@googlegroups.com
1,1	ESNA	Spain	Juan Fernando Muñoz	jfmunoz@msc.es
1,0	FHGISST	Germany	Sören Bittins	soeren.bittins@isst.fraunhofer.de
0,8	CATA	Spain	Montse Meya Carlos Gallego Perez	montse.meya@ticsalut.cat cgallego@ticsalut.cat

3.3 Timeline of the WP3.8

Guidelines D3.8.1

2010	2010																										
Month	January				February				March					April				May			June					July		
Week number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	16	19	20	21	22	23	24	25	26	27	28	29
Possible time schedule																			*		Δ								
WP3.8 - Integration and customisation																			*		Δ								
Total document *Issue 1*																			*		Δ								
Internal review																			*		Δ								
Quality Review D3.8.1																			*		Δ								
WG E - Editorial group																			*		Δ								

Meetings concerning Legal and Organisational, Practical and Evaluation:
TCON about homogenised D3.8.1: 12 May *
TCON about final draft of D3.8.1: 27 May Δ
Release of D3.8.1: 23 June
Lifetime of WP3.8
Intensive and planned work

Figure 7: Time schedule D3.8.1

Guidelines D3.8.2

2010	2010																
Month	June				July				August					September			
Week number	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
Possible time schedule			∞											Δ			
WP3.8 - Integration and customisation			∞											Δ			
Input to D3.8.2			∞											Δ			
Internal review			∞											Δ			
Quality Review D3.8.2			∞											Δ			
WG E - Editorial group			∞											Δ			

* technical chapter, liability, end-to-end, security, auditing, central services, Medical Device Directive, NCP roles and responsibilities

Important dates
PSB meeting 21 June - decision about liability (end-to-end), security, auditing, central services ∞
10 September - Release of Guidelines Issue 2 Δ

Figure 8: Time schedule D3.8.1

GUIDELINES

Important note:
This is where the actual guidelines begin.

4 Technical Issues

As part of the work in the defining the technical guidelines, the work package decided that guidelines should be composed of references to current work packages. The epSOS work is still unfinished and future work is relevant in this guideline, but the timely planning & execution of WPs only permit forward references to these.

WP deliverables	Deliverable	Description
WP3.9	Technical Specification (part of D3.9.1)	This deliverable is planned to contain a detailed technical specification of the NCP design provided in the High-Level Design (HLD) from the JWG, which will be an annex to D3.9.1
WP3.9	Testing strategy and tools (D3.9.2)	This deliverable is planned to contain the epSOS testing strategy, test plan and test tools description, together with guidelines on the Projectathon the epSOS interoperability testing event

The technical guidelines must be used as a roadmap to other primary sources, where the information is rightfully described. The following sections (sections in Chapter 4) will split the technical guidelines in sensible areas and provide references to the primary source of information on the subject. Information is in a lot of case in epSOS listed in many places, so an information index has therefore been seen valuable. Moreover, the sections can be used as a checklist for the MS implementers, for checking their design, planning & post implementation checking.

4.1 Functional & Technical Content References to WP3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, JWG

WP deliverables	Deliverable	Description
WP3.1	D3.1.2	This deliverable contains the functional definition of the ePrescription (eP) & eDispensing (eD) use cases. A description of the medical documents needed for eP & eD as well as the information needed inside. The dataset for the medical document needed for e/eD/PS was also defined.
WP3.2	D3.2.2	This deliverable contains the functional definition on the Patient Summary (PS) use cases. A description of the medical document needed for PS as well as the information needed inside. The dataset for the medical document needed for e/eD/PS was also defined.

WP deliverables	Deliverable	Description
WP3.3	D3.3.2 D3.3.3	These deliverables contain a high-level architectural view on the epSOS gateway – National Contact Point (NCP). As well as the system application architecture, a service design for the epSOS interface is defined.
WP3.4	D3.4.2	This deliverable contains the technical profiles of the epSOS interface as well as transactions hereof. This can be seen as a mapping of the security, business & architectural views on actual international standards.
WP3.5	D3.5.2	This deliverable contains the medical document defined in 3.1 and 3.2, but adapted to the standards chosen, as well as semantics. Information coding & rules on translation, transcoding and transformation of medical information in the NCP gateway.
WP3.6	D3.6.2	This deliverable contains the description of HCP Identification and Authentication, Patient Identification, Patient Consent and Confirmation of Patient
WP3.7	D3.7.2	This deliverable contains the security requirements & rules for epSOS. Views on network, service, business security for epSOS, and rules & guides on national security likewise.
JWG	HLDD (not official document according to Annex I. It has been fully integrated in D3.9.1))	This deliverable is a joint work between WP3.8 & WP3.9 and is a suggested design of a NCP-in-a-box emphasising commonly developed components within epSOS. The design is high-level and depending on the development strategies for the components a detail design can be done from here.

4.2 Architecture of epSOS

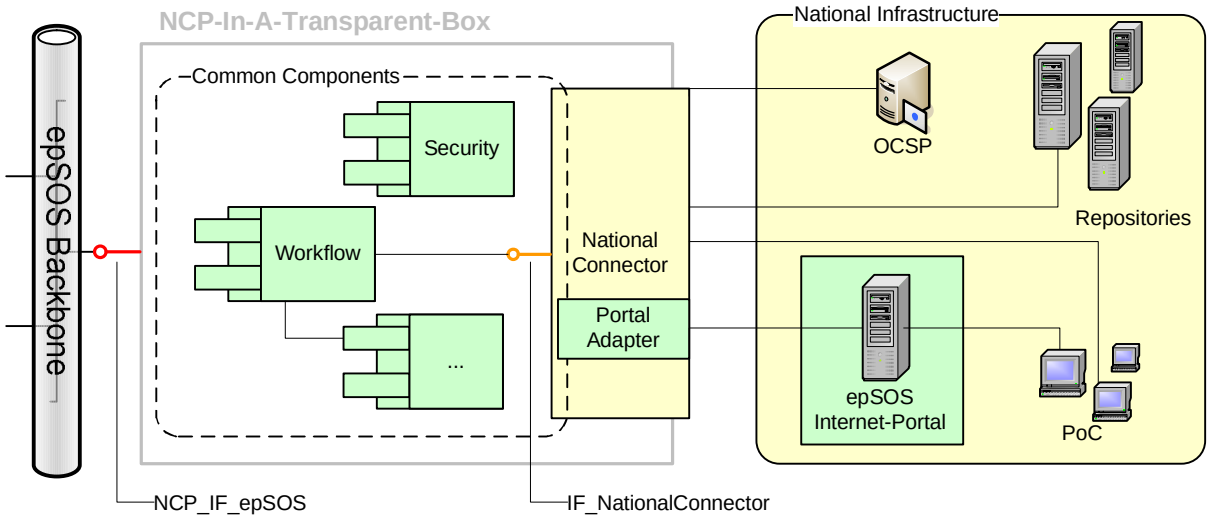


Figure 9: Conceptual Architecture of epSOS NCP Gateway

One of the main objectives of epSOS is to ensure the interoperability between individual NCPs. Section 6 of D3.3.2 (pp. 77-135) is dedicated to providing a high-level architectural description of an NCP that should serve as a reference for a detailed specification documents as well as for development planning process.

4.2.1 Overall Structure and Components

SOA paradigm with SOAP chosen for an information exchange was chosen as a basis for NCPs interoperability. Section 6.3 of D3.3.2 (pp. 80-83) provides a technical overview of the epSOS service architecture. The architectural view on the components is given in D3.3.2, section 6.4, pp. 83-112.

4.2.2 Interoperability

The different aspects of interoperability are summarised in D3.3.3, the Interoperability framework. D3.3.3 has been designed as a guide to the standards and protocols that are used to support the interoperability between the MSs.
à See D3.3.3

The interoperability framework identifies four main categories of interoperability which are legal, organisational, semantic and technical aspects of interoperability. Technical interoperability is achieved with the stipulations in D3.3.2 and 3.4.2 regarding standards and interfaces between NCPs.
à See D3.3.2 (Technology view) for the basic decisions regarding interfaces and standards
à See D3.4.2 for the detailed specification of the interfaces.

4.2.3 Interfaces

The one normative interface in epSOS is the interface of an NCP gateway towards the epSOS backbone (NCP_IF_epSOS, coloured in red in Figure 9). In D3.3.2, the interface is described in the Technology View. It is deduced from the epSOS transactions which are analysed in Business View and Information System View.
à See D3.3.2 (Technology View)

The detailed specification of the WebService interface including WSDL and XML Schema can be found in D3.4.2
à See D3.4.2 (epSOS common message format; wsdl)

The other important interface of the NCP gateway is not normative according to the epSOS specification but becomes relevant if a MS makes use of the design approach as described in the High Level Design Document (HLDD). It is the interface of the national connector towards the "common components" part of the NCP (IF_NationalConnector, coloured in orange in Figure 9). Aim and conditions of that interface are defined in HLDD.
à See JWG Deliverable HLDD

The detailed specification of the interface IF_NationalConnector can be found in technical specification (appendix A) of the D3.9.1.
à See D3.9.1

4.3 Setting up a NCP

This section covers only technical aspects of setting up a NCP. The guidelines on organisational preconditions and recommendations can be found in Chapter 6 and 7 and include establishment of NCP organisation described in Section 6.1 (Establishment of NCP organisation), definition of NCP key roles described in chapter 6.7 and testing strategy described in chapter 6.6.

It is up to each MS to obtain the appropriate hardware and software for NCP and to perform the ICT installation, however epSOS requirements on security described in Annex I of this document (NCP baseline security profile) and in D3.7.2 must be followed. Some requirements and recommendations on servers for NCP are described in Section 7.2 (Manual regulations to run the NCP) and recommendations on operating systems, platforms and libraries are in Section 4.5.12 (Platforms and Technical issues). The system must be configured according to epSOS requirements described in D3.7.2 and D3.4.2.

The NCP components will be provided by MS implementer and/or Common component developer along with the installation instructions. These instructions will also include information on how to configure the NCP using the central configurations provided by epSOS. For more details about the central configurations see Section 6.2.1.5 (Configuration Management).

After the NCP components have been successfully installed, configured and tested, they need to be connected to the national infrastructure to services for identifications and authentication of patients and HCPs and for obtaining the documents to be transferred to another country (Patient Summary, ePrescription, etc.). Connecting the NCP to the national infrastructure is MS responsibility and is out of scope of these guidelines.

Each NCP MUST describe its service addresses and certificates in a location table that complies to the epSOS Trusted Service List (TSL) format specified in D3.4.2, section 4.4 (epSOS Trusted Service List) and make this list available to other NCPs via a centrally managed table (see Section 6.2.1.5.2 and 6.5).

4.3.1 NCP Components in Common

The epSOS project has proposed a common design specifying common components that can be developed in common. To achieve high interoperability and conformity between the different NCP installations, these common components will be developed for epSOS and the MSs by the F.E.T. (Frauenhofer institute & ELGA Team: the consortium composed by the two Beneficiaries and vendors of the Industry Team - Tiani-Spirit et al.).the F.E. (Frauenhofer institute & ELGA) and vendors' consortium (Tiani-Spirit et al.). The work of design and specifying the High-Level Design

for the components and interfaces has been done in the JWG between WP3.8 & WP3.9, and these are documented in the HLDD. The HLDD will be formally
à See HLDD for design of commonly developed components

Note: FET design document will be available at a later date/FET design is subject to change.

The F.E.T. consortium has provided the following design for the NCP-A & NCP-B:

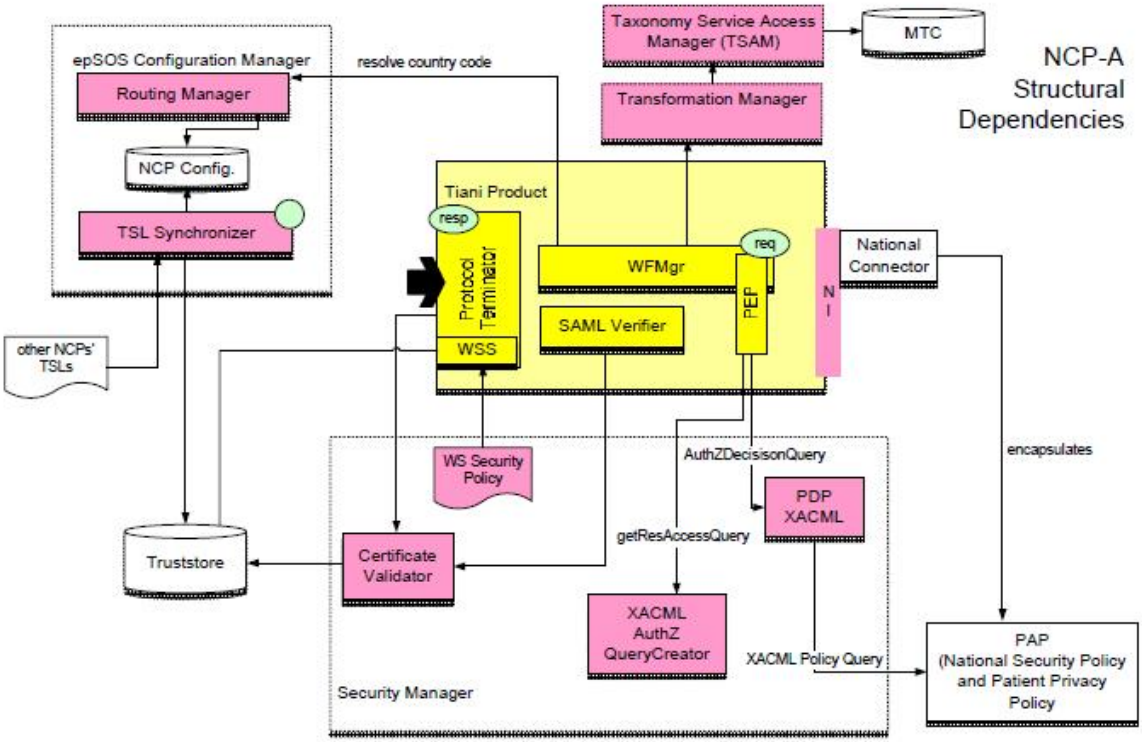


Figure 10: F.E.T. Design for NCP-A common components

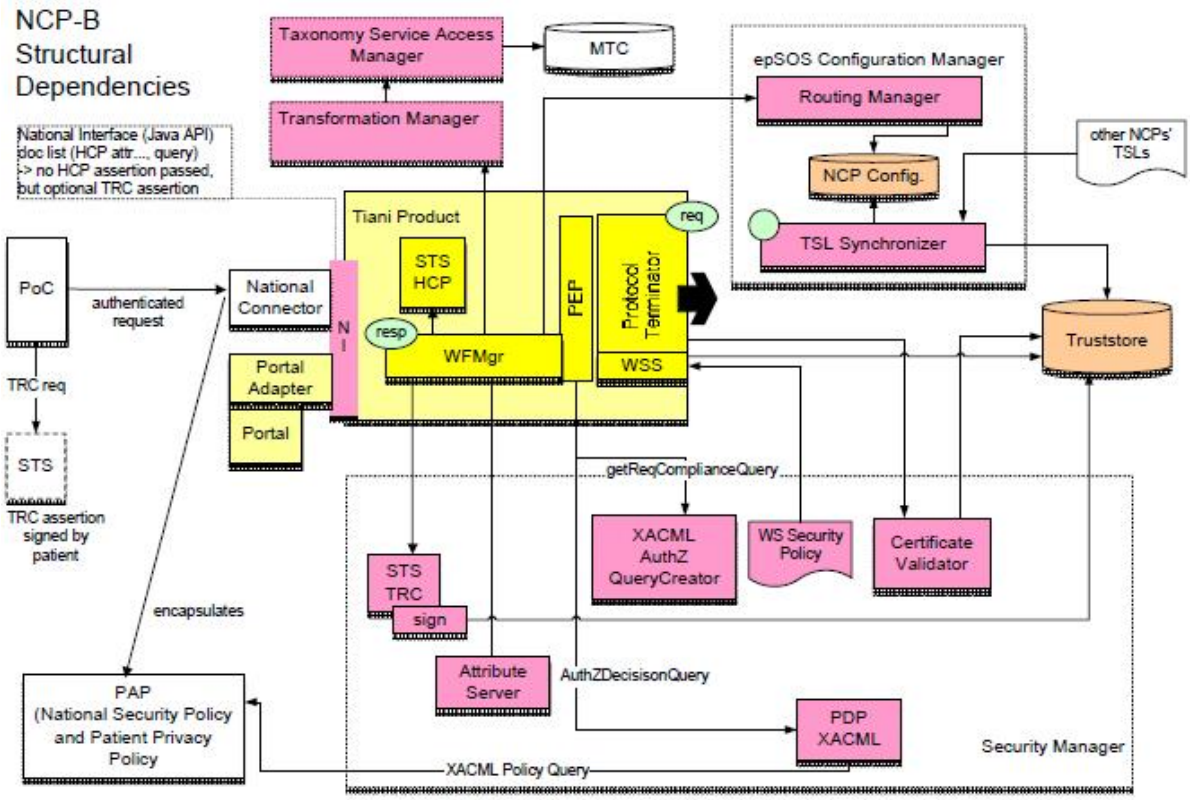


Figure 11: F.E.T. Design for NCP-B common components

4.3.2 NCP Customisation

See annex VII for NCP customization examples.

4.4 Technical Aspects of epSOS

This section contains various important aspects on the technical standard of epSOS. As previously mentioned each sections points to the primary source of information on the aspects, and if conflicts exist with other epSOS descriptions, these references are seen as the 'truth', more valid than others.

See section 4.1 for list of references epSOS documents/deliverables.

4.4.1 Interconnectivity

The epSOS services fundamentally require the initiation, implementation, maintenance of a common trust establishment between all participating nodes (gateways) that immediately interface epSOS. The organisational trust that is established and secured by a set of framework agreements (FWA), policies, and contracts between the epSOS partners must be transposed to the technological foundation of epSOS – epSOS NCP2NCP session.

- **à** See epSOS Concept Paper for the procedural (organisational and legal) definition
- **à** See D2.1.2 for the FWA onto establishing contract-backed organisational mutual trust
- **à** See D3.7.2 for the epSOS security policy

The technological establishment of mutual trust between the trusted nodes (gateways) – referred into within epSOS as trusted node infrastructure or NCP2NCP session – is normatively specified in D3.4.2 section 4.1 (pp. 84 to 85) and IHE ATNA as specified in IHE ITI TF-2a, section 3.19. The concrete security constraints and requirements are elaborated in D3.7.2 epSOS security policy.

Implementation and deployment options are briefly illustrated in the HLDD in section 3.6.2 (pp. 34 to 35).

à See D3.4.2 for the normative specification of the trusted node infrastructure
à See in IHE ITI TF-2a for the detailed specification of the mutual node authentication
à See D3.7.2 for the epSOS security policy
à See HLDD for a potential implementation and deployment illustration

4.4.2 Patient Identification

The procedures and processes regarding the patient identification within epSOS are divided into three principal layers:

- the technical processes and transport methods as specified in D3.4.2 section
- the legal & organisational requirements (including the security safe guards), primarily provided by D3.6.2 section 7 and D3.6.2 section 8 & 9.
- the concrete deployment options as illustrated in D3.6.2 section 9 and the HLDD, section 3.3.1.

à See D3.4.2 for the normative identification transactions and specific normative interfaces
à See D3.6.2 for the procedural (organisational and legal) definition and requirements
à See D3.6.2 for the concrete set of security safe guards that need to be met
à See D3.6.2 and the HLDD for potential deployment options

In addition to the technical specification, the legal foundation, and the security safe guards the epSOS specifications also provide a comprehensive set of identification process options and potential process implementation candidates for carrying out the patient identification within the respective MSs.

à See D3.6.2 for candidate process implementation candidates of patient identification
à See D3.6.2 for a proposed set of identity traits to be used in the identification process
à See D3.6.2 for advice on identification means, such as smart cards or other identity token
à See D3.6.2 for a compilation of the required actors and roles required to identify subjects

4.4.3 Patient Consent

Legal framework and requirements for patient consent is defined in D2.1.2 chapter 3.4 and HCP guidance in chapter 3.5.

As part of the patient identification and defined patient processes D3.6.2 defines the location of the patient confirmation consent in the epSOS processes, see D3.6.2.

The technical aspect of exchanging the patient consent is done by a WebService. The architecture for this service is defined in D3.3.2 chapter 6.5.1.5 (ConsentService) and the transactions/profile in D3.4.2 chapter 2.6 & 3.6. The exchanged documents giving the patient consent follow the IHE BPPC standard, and are transferred from country B to A.

4.4.4 HCP Authentication

HCP identity data is administered in autonomous systems within national infrastructure. For the epSOS LSP it is assumed that the HCP and HCPO that treat the patient can only be unequivocally authenticated by the competent authorities of country B.

The authentication of the health care professionals (HCP) is a prerequisite for any epSOS transaction (usually Identification Handshake). The authentication of the HCP is done by the identity provider which is part of the national infrastructure and must be separated from the NCP.

For more details on identity providers and authenticity levels, see D3.7.2 (mainly sections 4.3 and 5.3). The processes for identification and authentication of HCP are described in D3.6.2, section 7.3.1 (Identification and authentication of HCP).

epSOS country-B implementations may use dedicated Identity Providers for issuing HCP Identity assertions. The requirements for this case are described in D3.4.2, section 4.4.6 (Identity providers).

The identity ID and its attributes are then communicated among NCPs by means of HCP Identity Assertion described in D3.4.2, section 5.2 (HCP Identity Assertion).

The existence of a treatment relationship between a patient and a HCP can only be attested within the legal framework of the point of care (PoC). With epSOS HCP authentication and treatment relationship attestment are therefore performed within the country of care (e. g. by using an existing Identity Provider service of the national infrastructure). A brokerage of the HCP authentication and treatment relationship confirmation into the epSOS domain is performed in a way that the NCP at country B confirms the respective claims and maps them onto a unified syntax and semantics that can be processed by the NCP of country A. The treatment relationship confirmation is communicated by means of Treatment Relationship Confirmation Assertion described in D3.4.2, section 5.3 (Treatment Relationship Confirmation Assertion).

The NCP functionality needed to operate the NCP for the user HCP is implemented in the NCP-B Front-end. The functionality includes HCP authentication, HCP session life-cycle description and TRC session-life cycle and they are described in the HLDD in section 3.6.3, 3.6.7 and 3.6.8 respectively.

An overview of the relationship of identity provider to NCP components is described in HLDD, chapter 4 (Exemplary Deployment Composition).

4.4.5 Semantic Services

Semantic services are a cornerstone in the epSOS project providing translation, trans-coding, and mapping of clinical documents and information between MS formats. D3.5.2 defines the methods for semantic translation etc. between MS formats and the epSOS documents.

à See D3.5.2 Chap.4 and Appendix D; D3.9.1 Chap.5.3 and Appendix B2 for MVC / MTC

à See D3.3.2 for Semantic Services, D3.5.2 Appendix F and D3.9.1 Chapter 3, Chapter 5.3 and Appendix B2

à See D3.9.1 Chapter 3.5, 3.6 and Appendix B1 for epSOS semantic components & input format

4.4.6 Patient Summary Service

As part of the documentation of the Large Scale Pilot (epSOS LSP) functional requirements and Clinical Document content related to Patient Summary are included in D.3.2.2. Specifically requirements are depicted in chapter 5.3.1 (starting at page 26) and common information is at chapter 6 (patient summary)

Data elements are expressed using HL7 CDA Level 3 Rev. 2 (HL7 CDA here after) with the additional constraints of the HL7 Continuity of Care Document (CCD) and IHE Patient Care Coordination (IHE PCC). The Clinical Document Architecture (CDA) is described on chapter 3 in D3.5.2 from WP3.5.

Patient Summary lifecycle is described in D3.3.2, chapter 5.5.3 (pages 79 - 80), where different states of the process are defined. The details about Patient Summary services interfaces are described in chapter 6.5.1.2 (pages 127 - 128), including also implementation recommendations.

A very important point regarding the deployment of epSOS services is respecting patient privacy and identity rights. These topics are addressed at D3.6.2 which is part of the WP3.6. The patient should accept that his/her epSOS LSP health data is accessed.

In addition, attention should be given to deliverable D3.4.2 which describes epSOS architecture common components for the different services including epSOS implementation and communication infrastructure. In this document Common Message Format is defined, this format is required for exchanging information between different NCPs and therefore information generated within a NCP should be translated to this format before sending it.

Finally, the WP3.8 and WP3.9 JWG issued its NCP High Level Design Document describing the concept of NCP-in-a-Box, this document is a reference for NCP implementers. Sections 3.3.2 (pages 21 - 23) describes the epSOS Patient Service by means of sequence diagrams from both sides, NCP-A and NCP-B.

4.4.7 ePrescription/eDispensing Service

As part of the documentation of the Large Scale Pilot (epSOS LSP) functional requirements and Clinical Document content related with ePrescription and eDispensing are included in D.3.1.2. Specifically requirements are depicted in chapter 5.2.2 (starting at page 29) and common information is at 6.1 (prescription) and 6.2 (medicine datasheet).

Data elements are expressed using HL7 CDA Level 3 Rev. 2 (HL7 CDA here after) with the additional constraints of the HL7 Continuity of Care Document (CCD) and IHE Patient Care Coordination (IHE PCC). The Clinical Document Architecture (CDA) is described on chapter 3 in D3.5.2 from WP3.5.

ePrescription lifecycle is described in D3.3.2, chapter 5.5.4 (pages 80 - 82), where different states of the process are defined. The details about ePrescription and eDispensing services interfaces are described in chapter 6.5.1.3 (pages 129 - 131) and 6.5.1.4 (pages 131 - 134) respectively, including also implementation recommendations.

A very important point regarding the deployment of epSOS services is respecting patient privacy and identity rights. These topics are addressed at D3.6.2 which is part of the WP3.6. The patient should accept that his/her epSOS LSP health data is accessed.

In addition, attention should be given to deliverable D3.4.2 which describes epSOS architecture common components for the different services including epSOS implementation and communication infrastructure. In this document Common Message Format is defined, this format is required for exchanging information between different NCPs and therefore information generated within a NCP should be translated to this format before sending it.

Finally, the WP3.8 and WP3.9 Joint Working Group issued its National Contact Point High Level Design Document describing the concept of NCP-in-a-Box, this document is a reference for NCP implementers. Sections 3.3.3 (pages 24 - 25) describes the epSOS Order Service by means of sequence diagrams from both sides, NCP-A and NCP-B. Sections 3.3.4 (pages 26 - 27) describe the epSOS Dispensation Notification Service, depicting the sequence diagrams to initiate and discard a dispensation.

4.4.8 Consistent Time

The epSOS gateway infrastructure of interconnected NCPs is required to have a precise and common time reference. The common time is required for security validation on timestamps as well as audit traceability via audit logs with timestamps. Instead of building a new time source the global time source provided through Network Time Protocol (NTP) has been chosen and profile in D3.4.2 chapter 4.2 (pages 89 - 90).

4.4.9 Platforms

NCP gateway platforms are not specified in detail, and can be seen more as recommendation and intentions, see HLDD, chapter 4.3 on page 42, for design recommendations of platforms & frameworks.

4.5 Central Services

The Central Services are described in D3.9.1 Chapter 5.
In particular: Chapter 5.1 describes Central Service Goal and makes proposal on associated responsibilities.

- **à** Chapter 5.2 describes functions and structures of Configuration Repository Manager.
- **à** Chapter 5.3 defines epSOS Central Reference Terminology Service.

4.5.1 Example of possible solution (a virtual central service)

The solution addresses information structure & versioning, service addressing, network & transfer security issues and more importantly service responsibility.

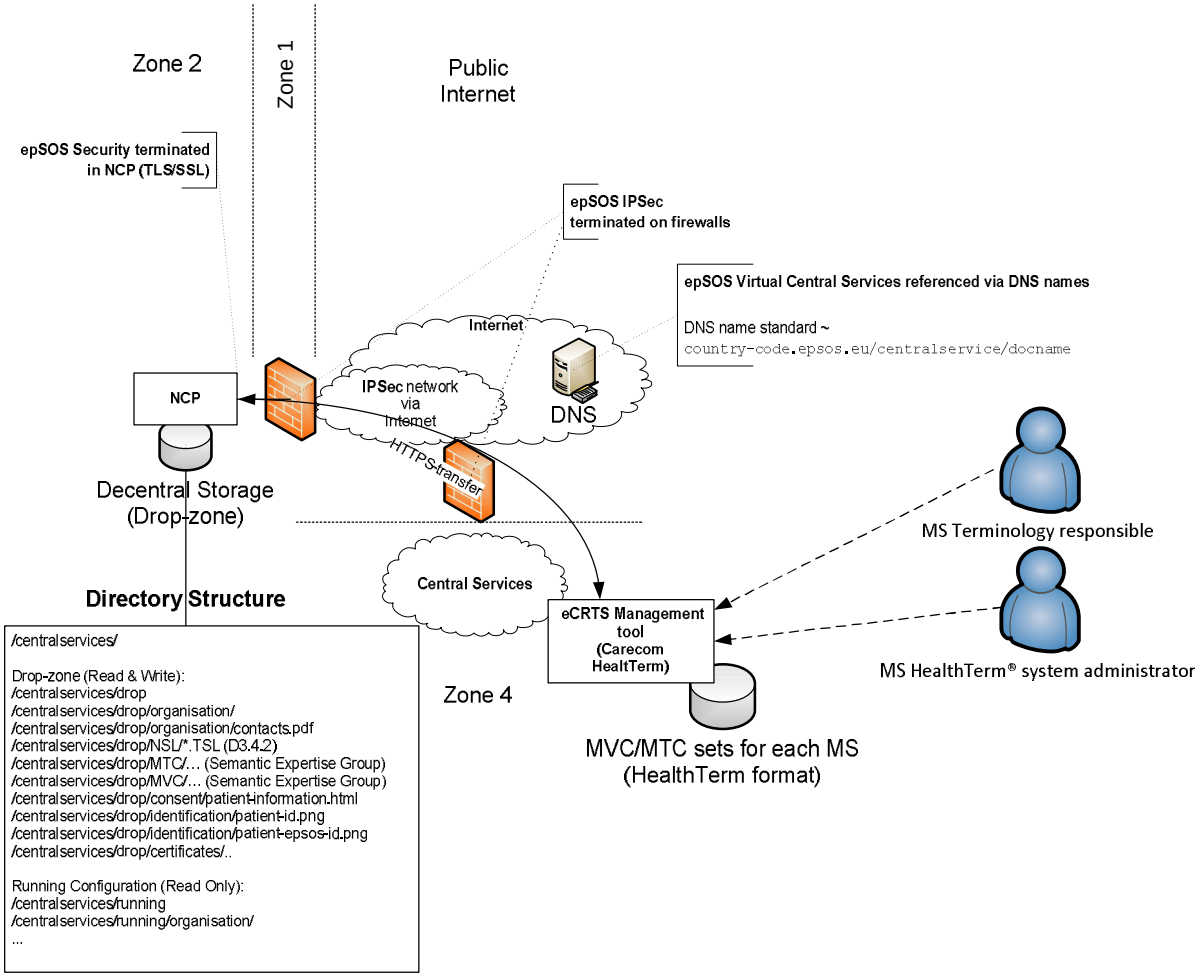


Figure 12: Virtual Central Service - proposed solution

Item	Responsibility	Description

Information Structure	NCP organisation	Versioning: two visual versions: Drop-zone (TO-BE) & Running (AS-IS), named: `drop` & `running`
		
		Underlying the information should be placed on a SubVersioned structure for full traceability (not shown in diagram).
		
		Structure for suggested central information for organization contact data, NCP TSLs & semantic MTC & MVC
		`<version>/`
		`<version>/organisation/`
		`<version>/organisation/contacts.pdf`
		`<version>/NSL/*.TSL (D3.4.2)`
		`<version>/MTC/… (Semantic Expertise Group)`
		`<version>/MVC/… (Semantic Expertise Group)`
		
		The information structure should be accessed in a REST way, as resources via HTTP protocol.
		
		Therefore the structure can be virtual in itself. Root of central services is `centralservices`

DNS name standard	NCP organization (epSOS & EU-hostmaster)	epSOS owns the 'epsos.eu' domain and is responsible for ordering the requested DNS name for the MS NCP. The name standard follow the pattern:

Item	Responsibility	Description
		<country-code>.epsos.eu/centralservices/<version>/<hierarchy>…/<document> **EX**: *Getting the current organization contacts for Denmark* https://dk.epsos.eu/centralservices/running/organization/contects.pdf
eCRTS Management tool	epSOS	The CareCom tool for editing and managing the epSOS and MS MVC & MTC. The tool guarantees that the information inputted by epSOS and MS is stored and transferred to the NCP – drop-zone, version drop safely and in intact form. To ensure safe transfer, file-trasfer over HTTPS is used with NCP certificates. File transfer signed by responsible party via OpenSSL -> CMs signature or likewise. Alternatively safe transfer could be on of the following: - SFTP - Webservice over HTTPS

4.6 Test Procedures

Will be produced by WP3.9/10. Until then, refer to chapter 6.6 of this document.

5 Legal Issues

5.1 *Contractual aspects*

This chapter concerns legal issues in the Framework Agreement. The chapter is directed to legal experts in MS and in epSOS.

5.1.1 Framework Agreement

This section is based on D2.1.2 Standard Contract Terms for engagement of pilot sites.

Within D2.1.2 you find the legal Framework Agreement (FWA) which forms the conceptual basis for all contracts within epSOS' trusted domain – i.e. the contracts between the NCP and the various HCPOs and PoC. More importantly, the FWA also provides a blueprint for the contracts which create the NCPs which will be signed in each participating MS. The objective is to create a network of localised contracts which are all cross-referenced and therefore in themselves create the framework of the trusted domain.

5.1.1.1 Forming local variations of the Framework Agreement

Each MS hosting one or more pilots is responsible for making a local version of the FWA in the national languages. The localisation should result in a contract which reflects the pilot situation in the given MS for which it has been adapted. The FWA must be localised to comply with national legal and professional requirements, however, the contract should be closely based on the FWA. This work should be done by local legal experts and the local epSOS team.

All localisations of the FWA must consider the following points:

(i) The epSOS security Policy (from D3.7.2). This document contains requirements.
(ii) The epSOS Pilot Strategy (from the TPM Task Force, December 2009) as an advisory document.
(iii) Processes, procedures and audit practices, which is required by WP4.2.[1]

5.1.1.2 Process for agreeing on local variations of the FWA

The localised contracts should be comparable across all pilot sites and they should satisfy the local and EU level legal requirements on issues such as patient consent, data security, patient confidentiality, liability etc.

Once each MS has drawn up its localised version of the FWA the MS must produce a document in English which states and explains where and why the localised version of the FWA differs from the original epSOS FWA. WP2.1 will evaluate it and will then recommend to the PSB to formally sign-off the content of each localised agreement thereby ensuring that the necessary commonality exists to create the legal framework of the trusted domain. Once the PSB has accepted the content of the document each MS will ensure that it is formally signed by the relevant party who at MS level can authorise the creation of the NCP.

5.1.1.3 Signing of FWA

All MS participating in epSOS have agreed on the FWA delivered by WP2.1. The FWA should be signed between:

a) Each National Authority Beneficiary (NAB) and/or organisation(s) legally entitled to establish the NCP and
b) Each legal entity which assumes the role of NCP.

[1] As described in D2.1.2, page 16-17.

Once the NCP has been created in this way and the same core rules of NCP operation have been implemented in each participating MS, then the NCPs will continue to create further contracts between the NCP and HCOs or PoCs in order to ensure the delivery of epSOS services.

The localisation process has the following timeline:
January to July 2010 (M19-M25) – Localisation of FWA.
September 2010 (M27) – National NCP Agreements signed.[2] These national NCP agreements will be held locally in each MS, although PSB may require a formal lodging of copies of the national agreements in the project archives in order to allow easy consultation by all project partners.

5.1.2 Legal Establishment of NCP

As outlined above, the FWA will be used as the blueprint for a contract which establishes the legal relationship between the NABs and the NCP. In some cases, however, the NAB is responsible or acts as the NCP and, consequently, there is no need for an additional contract. Where this is the case, it is recommended that a formal note is signed internally by which the NAB agrees to the terms of the FWA. In this case, the MoU and FWA together will form the legal reference point for the duties the NAB has agreed to assume in acting as NCP. The NCP works as a legal entity which ensures that all epSOS legal requirements are upheld. The NAB guarantees that the NCP is capable and fit for performing this role.[3]

In the pilot phase, the legal relationships between NCPs at EU level are established indirectly through their NAB as stated in the epSOS Grant Agreement. The PSB approves an audit system which should be transparent and independent and, as signers of the Consortium Agreements, they ensure that NCP responsibilities are fulfilled[4].

This means that:

1) The NABs have entered into a contractual relationship with the EU through the Grant Agreement and Consortium Agreement.
2) National/local legal experts working with the local epSOS teams have localised the FWA to fit national/local legislation. This may be done by the NAB designating responsibility to a local legal expert to draw up a first draft of the local contract based on the FWA or may be done internally by the NAB's epSOS team.
3) Within the context of the project, the NAB assumes legal responsibility for ensuring that the NCP and its partners (HCOs and PoCs) deliver the epSOS services. In the event of a breach of contract by the NCP local contract law will apply.
4) If the NAB is providing the NCP directly, then it is directly accountable to the project through the Grant Agreement.
   → The organisation(s) in question must sign the FWA.

Each HCP(O) or PoC participating in the pilot has signed a contract with the NCP taking into consideration the FWA and tailored to local law and its specific duties. Potential epSOS patients have been duly informed about their rights and locally applicable consent mechanism have been established.

5.1.3 Legal relationship between NCPs

The localised FWA signed in all piloting MS will ensure that the NCPs can interact in a trusted domain without the need of contracts between the ten national NCPs. However, if national legislation requires contracts, the FWA will not sufficient remedy. It is important to note that contractual obligations do not change national law.

[2] D2.1.2 page 25.
[3] D2.1.2 page 15-16.
[4] D2.1.2 page 15.

The picture[5] below shows how the different entities are connected by the legal framework for epSOS. There are two levels: EU level and national level.

At EU level, the NABs have entered into a contractual agreement with each other via the Grant Agreement and Consortium Agreement.

At national level, the connection between the NCPs is illustrated. Here you have the FWA and the local versions of the FWA which establishes the contractual relationship between the NCPs. The yellow circle which shows the localised FWA sphere can be extended to also including NAB1 in cases where the NAB acts as the NCP.

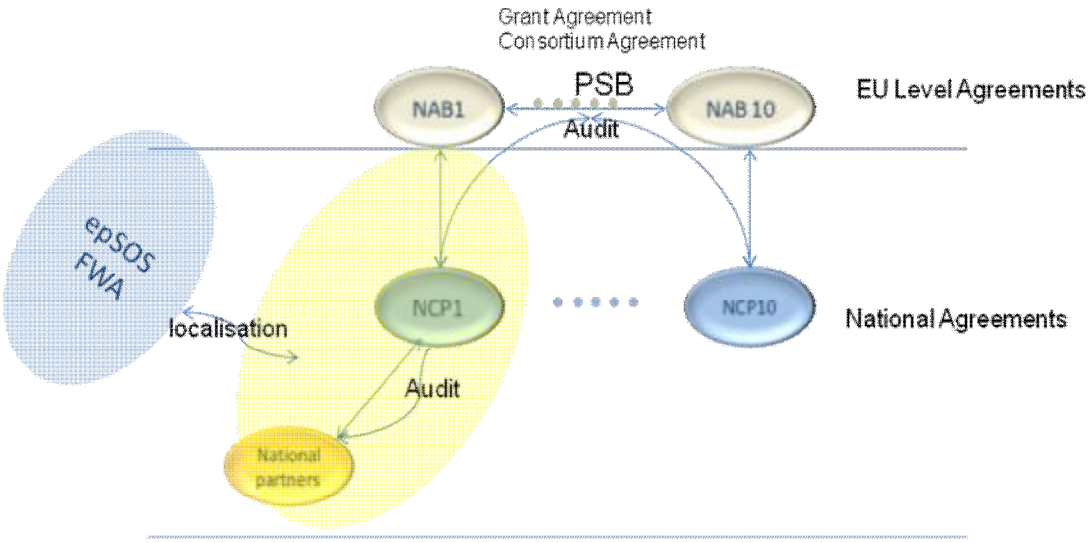


Figure 13: Levels of Agreements

5.1.4 Legal recognition of Point of Care and Healthcare Organisation

The legal relationship between the epSOS partners in the MSs – i.e. the NCP and the various HCOs and PoCs will be regulated by contracts between the NCP and the partners. Those contracts will be based on the FWA in order to reflect the duties set out in the FWA.

The local contracts between the NCPs and the PoC will ensure that appropriate processes and procedures, such as security measures and safeguards, are in place. The NCP should maintain records and reports demonstrating compliance to the abovementioned measures. This should be used for traceability and external audit purposes[6]. The NCP will also be responsible towards the project for ensuring that these duties are fully met.

5.2 *Clinical Aspects*

This chapter concerns clinical legal aspects related to epSOS. The chapter is directed at legal experts in MS and in epSOS.

The clinical aspects focuses on the responsibilities of the NCPs and how to ensure that confidence in the epSOS system can be built regardless of differences in national legislation.

[5] From D2.1.2 page15.
[6] D2.1.2 page 15.

5.2.1 General Information

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 unauthorised parties, and that patient rights according to national legislations is e.g. the right of informed consent to data access are duly respected by all parties.

The PSB have approved a Security Policy (D3.7.2) contained by four separate documents, as follows:

- Master document
- NCP Security Policies
- Security Services Description
- Congruity and Suitability analysis

Each NCP and each national organisation at every participating level must form security information policies and ensure implementation on contractual basis. A documented "Information Security Policy" at every level ensures that information regarding patients care is accessible and useful for authorised HCPs. The application of the Security Policy[7] for every NCP will (in accordance with the FWA that constitutes a contractual agreement between PSB-NCP) be approved, implemented and periodically audited by epSOS partners represented by the PSB, through an independent party, e.g., through a contracted auditor under the supervision of the PSB[8].

Each epSOS country is responsible for the implementation, organisation, service quality and conformance to epSOS standards towards the rest of the epSOS community.

Each NCP must ensure that the epSOS policies, including the NCP Security Policy is appropriately implemented and must put in place appropriate measures (processes and procedures) including security measures. Based on contractual agreements between NCP-PoC, the NCP shall be legally competent to enforce audit and corrective action emerging from audits[9]. The NCP must ensure proper application of epSOS standards of practices and that PoC conformance is demonstrated to the epSOS requirement and national legislation. The NCP in each country will also assume the responsibility of ensuring that patient consent is appropriately handled and that all epSOS HCPs are trained with respect to their epSOS duties.

A data protection audit aims to identify non-compliance issues; detecting weaknesses in the data protection management process applied by HCPs and PoC; and maintaining and ensuring compliance with relevant data protection principles required by the Data Protection Directive.

Any discrepancies between epSOS requirements and national legislation must be thoroughly discussed with national Data Protection Authority (DPA) and NAB. The transfer of medical data across national borders and the NCP role as Data Controller or Data Processors (as appropriate for each MS) according to national legislation are key issues in these discussions; the NCP must be able to comply with national rules on data protection and on data security since NCPs in each MS are created under local law on basis of a framework agreement. The criteria for nominations of Data controller and Data processor is designated by national law or Community law (Dir 94/46/EC).

In order to overcome or prevent current legal barriers and take advantage of technologies to improve the services to cross-border patients there is also a need for action at European level. This

[7] WP 3.7 , D 3.7.2 Final security specification Definition – epSOS Security Policies
[8] Project steering Board Meeting Tuesday 19 January 2010 "Note on the role of the PSB in the epSOS pilot legal framework
[9] D2.1.2, page 29, section 2.3.4

is also necessary for the creation of a common medicine nomenclature or language, as well as common criteria for the maintenance and updating of semantic descriptions of the different medicine elements.

When establishing an epSOS system within each MS, key definitions of concepts and key terms such as Data controller, Data Processor, Personal Data, Processing of personal data, Medical Record or Health Record and so forth, according to the work done in D2.1.2 Standard Contract Terms for engagement of pilot sites – must be identified and clarified according to national legislation. This means a clear statement, in accordance with the FWA and national legislation as to;

- What information is to be processed?
- What are the requirements for the user?
- Who grants accessibility, description of process for access?
- What legal entity is responsible for the integrity, accessibility and confidentiality of the data?
- Who is in control of access and logging?
- How will the patients' rights be enforced?

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 that is not necessary for health care purposes. Data will only be stored at MS level and not on central level.

The establishment of an NCP also requires identification of System Owner and responsibilities for the national epSOS system. The system owner should describe requirements on users who grant access to information system and are thereby given access to information. The requirements should:

- be documented and communicated.
- cover security as well as competence needed.

According to Commission decision of 16 August 2006 C (2006) 3602 concerning the security of information systems used by the European Commission, the "System Owner shall bear responsibility for the security of their information system. They shall define the security needs of the information system and the information processed therein. To this end, they shall take note of the needs expressed by data owners and users". http://ec.europa.eu/dgs/informatics/procurement/useful_documents/doc/decision_3602_2006_en.pdf#xml=http://158.167.146.104:7001/www/xmlread.jsp?ServerSpec=158.167.146.104:9000&K2DocKey=http%3A%2F%2Fec.europa.eu%2Fdgs%2Finformatics%2Fprocurement%2Fuseful_documents%2Fdoc%2Fdecision_3602_2006_en.pdf%40EUROPACORE_eceu_x&QuetyText

A System Owner is responsible for:

- Purchase
- Maintenance
- Operation of the system
- Security
- Define functional requirements of the system
- Appoint system administrator with adequate competence for the task.
- Approve the system before operations is started.
- Sign contracts necessary for the operation of the system.
- Making sure that the system is run in accordance with laws and regulations etc.

Through identifying roles and responsibilities on a national level described in an information security policy for the NCP built on the FWA and national legislation, each NAB will demonstrate conformity and transparency and thus secure a system of trust.

Information security policies established at every participating level are clarified in security instructions for the end-users, operators, and administration and management personnel. In some cases, specific system instructions could be needed.

Please refer to ISO27002. Official link: http://www.iso.org/iso/catalogue_detail?csnumber=50297

Example of national implementation:
One National model for the how to implement the European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as the European Directive 2002/58/EC on privacy and electronic communications, is the Swedish "Basic Level of Information Security(BITS)
http://www2.msb.se/upload/Publikationsservice/KBM/rekommenderar/bits_rek_2006_1_eng.pdf

5.2.2 Data availability/integrity/confidentiality

Data Availability[10] is defined as the property of being accessible and usable upon demand by an authorised entity.

Data Integrity[10] is measures to be taken in order to ensure that sensitive data has not been modified or deleted in an unauthorised and undetected manner. The technical aspects of this subject are dealt with by WP3.7.

Data Confidentiality[10] is measures to be taken in order to ensure that sensitive information is not disclosed to unauthorised individuals, entities or processes.

The legal responsibility for the quality and confidentiality of data in the eP and PS delivered by the NCP in each MS are defined by the definition of Data Controller at national level – the entity that is defined as Data controller of the medical data in eP and PS that is processed according to national legislation is also responsible for the quality and confidentiality of the Data delivered.

The HCO/NCP contract shall detail the duties of both parties with respect to maintaining the security, availability, confidentiality and integrity of all data flows.

The information security policy is clarified in security instructions (for more information see annex 1 of this document).

5.2.3 Patient Consent – Information to be Provided, Processes for Confirming and Documenting 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[11].

Access to patient data in the epSOS system is limited to situations where HCP request information 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.

We must distinguish between two processes for which patient consent is needed– one for providing medical service per se, the other for realising the epSOS "business case" as a specific processing of already existing personal data[12].

[10] http://www2.msb.se/upload/Publikationsservice/KBM/rekommenderar/bits_rek_2006_1_eng.pdf
[11] D2.1.2 Standard Contract Terms for engagement of pilot sites, page 22

For “Duties and responsibilities concerning Patient Consent (terms to be embodied in the national contracts creating the NCP´s and contracts between NCP´s and their partners as appropriate)”[13]. Participating MSs are required to embody terms for duties and responsibilities concerning Patient consent - these terms can be found in p.30 D2.2 Legal and Regulatory Constraints on epSOS Design. Access to data is allowed if patient consent has been granted in accordance with national law in the patient’s country of affiliation, and the purpose of access is to provide care for the patient. This means that NCP A must inform if prior general consent is given by the patient if so is required by national law.

> *Irrespective of the national approach for consent for creation of a personal data record and access to this information by HCPs within the MS, access to this data from abroad will be executed in accordance to Article WP29[14] recommendations in an opt-in.*

Regardless if prior consent is registered, consent must always be provided at the point of care, (consent must be specific*)* 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 emergencies 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.

For consent verification procedures and processes refer to D2.1.2 Standard Contract Terms for engagement of pilot sites, page 30 and 36.

For more details on the consent process, please refer to chapter 9 “Step-by-Step Description”.

5.2.3.1 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.

Patient consent must be informed. Patient information about epSOS must be provided in Country B in the patient’s language.
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 know 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.

epSOS healthcare professionals will 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.

Steps in the epSOS process are explained in D2.1.2 Standard Contract Terms for engagement of pilot sites, page 31 or section 7.1.2 of this document.

5.3 *National and European Rules, Laws and Directives*

This chapter is about legal relationships, rules and directives for MSs. The chapter is directed at legal experts in MS and in epSOS.

[12] D2.1.2 Standard Contract Terms for engagement of pilot sites, page 33
[13] See D2.1.2 Standard Contract Terms for engagement of pilot sites
[14] WP29: Article 29 Data Protection Working Party

Deliverable 2.1.1 sets out in detail what legal issues the epSOS use cases raise and how those legal issues are provided for with in EU level and national level law. In this document we only offer a light touch recap of those issues.

5.3.1 The effect of different laws

It is important to note that generally all EU level legislation pertaining to the epSOS use cases is contained in legislation while drafted at EU level must be transposed into national level legislation eventually.

This is because the Treaty of the European Union specifies in article 278 TEU that the provision of health services is a national or regional matter which is governed by the principle of subsidiary. Accordingly, the European Union enacts Directives which set the framework which must be followed within national legislation rather than Regulations which must be directly applied.

This also means that generally citizens do not have direct recourse to the European Court of Justice on any matters provided for in the Directives, but must proceed through their national legal systems. In some cases the ECJ will be called upon to adjudicate where a citizen argues that a right or duty provided for the Directive is not adequately reflected in the relevant national legislation.

In epSOS, the guidelines and the FWA are based on the general duties as set out in the relevant Directives, the localisation of the FWA into local NCP contracts will take account of any variations in local transposition of the Directives which may exist.

5.3.2 EU Directives

Deliverable 2.1.1 sets out and examines the applicable EU level legislation. The most important of these are the legislation concerning Data Protection:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[15],
- Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981),
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications)[16],
- the Article 29 Data Protection Working Party Working document on the processing of personal data relating to health in electronic health records (EHR) (WP 131)[17],
- the Council of Europe Recommendation no (97)5 on the protection of medical data.

The role of the present guidelines is to provide common solutions where variations in local legislation make it difficult to have one single rule. A particular case arises in patient consent procedures and HCP(O) accesses rights. As a result of different interpretations of the law in these two areas the epSOS guidelines provide for collection and confirmation of consent at both NCP-A and NCP-B.

[15] OJ L 281, 23.11.1995, p. 31.
[16] 7 OJ L 201, 31.7.2002, p. 37.
[17] Article 29 Working Party Working Document 131 on the processing of personal data relating to health in electronic health records (EHR), adopted on 15 February 2007. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

It is important to note however that the guiding principle of epSOS is that when a patient travels s/he will receive treatment in country B according to the rules of country B. Country A may however restrict the categories of information available in country B in order to comply with local rules on data protection.

5.4 Liability

In general terms liability concerns some form of obligation or responsibility arising by way of contract, tort, or statute. In legal terms, the word liability refers to the responsibility that a natural or legal person must assume for the harm or loss of another arising from a service or product made or provided.

It is important to note that at present no specific legislation exists at EU level that targets eHealth services and products specifically. Legally, these products will be covered by a range of legislation. At a most simple level any product – be it eHealth or any other – will be covered by the national legislation based on the EC product liability directives (Directive 2001/95/EC and Council Directive 85/375/EEC as amended by Directive 1999/34/EC). This will ensure that the purchaser has redress if the goods are not fit for the purpose sold, while other EC legislation such as Directive 2002/95/EC on the Use of Hazardous Substances will provide the purchaser with certainty about certain aspects of a product's quality.

Liability in epSOS is both medical and non medical. That means actors, whether natural or legal person, involved in providing epSOS services will assume responsibility towards each other and towards the end users and patients for the safety of the services delivered. It means also that any individual or organisations that suffers a harm or loss as the result of using epSOS services or receiving healthcare in which the HCPs and HCPOs have made use of epSOS services may be able to claim for compensation if the harm or losses can be attributed to a failure to execute epSOS services as provided for in the epSOS documentation. Liability in epSOS may therefore arise from a multitude of risks which often co-exist in the various processes. In addition liability lies in the design and implementation of the epSOS common components, which is highly dependent on the chosen "implementation scenario".

An analysis of liability issues has been made by the pilot partners, with particular emphasis on the risks related to the processing of medical data[18]. Any processing of data, including for example coding, transcoding, storage or semantic service, must be carried out in accordance with the law of the Members State within which the data are being processed. The data protection responsibilities will lie with data control and data processor as provided for in the national data protection legislation which has been enacted in accordance with Dir 95/46/EC on Data Privacy[19]. It is therefore vital that the roles of data controller and data processor are identified in each MS[20].

[18] Internal supporting document to the FWA
[19] Directive 94/95/EC art. 4
[20] Internal supporting document to the FWA

6 Organisational Issues

6.1 Establishment of NCP organisation

Chapter 6.1 is the chapter to use when MSs are setting up the NCP organisation.
The reader will get general information of what should be organised and how to publish. It will be necessary to read about Legal Issues for contracts etc. In the Checklist you can find relevant information for establishment of the NCP organisation.

6.1.1 General NCP Organisation

Implementing and maintaining the organisation around the NCP requires the MS to understand which requirements NCP puts onto it.

This section will identify these requirements and the roles that need to be implemented in the MS organisations.

The organisational entities the NCP will influence are

- operations from service desk to security
- information management department
- audit organisation

Operating the NCP pilot will require the pilot sites to implement the standard package of operating procedures and policies as with any other system. The service desk has to be informed and educated about NCP, incident and problem management will be required to provide support and services, the NCP needs to be implemented in national change management, SLA has to be managed and implemented and all security related requirements need to be handled on the national level.

Information about NCP has to be incorporated into the information flow in/out of the above organisations.

More details on these issues are provided in this chapter.

Additionally the technical, legal and practical organisations within the MS will have requirements to implement. These are covered in chapter 4, 5 and 7 and not discussed further here.

6.1.2 Description of Organisational NCP Roles

Organisational guidelines are needed to support those responsible for implementing and maintaining the NCP and the pilot. Examples of such organisational measures can be: procedures (e.g. changes in the organisation) or policies (e.g. fixing responsibilities in agreements and contracts with other parties). The latter case typically applies to the party responsible for implementing and maintaining the national infrastructure.

6.1.2.1 Organisational issues stemming from the NCP's functional behaviour

Functional requirements on the NCP lead to organisational measures. The primary function of a NCP is to support both of the LSP use cases (Patient Summary, ePrescription), both as a provider (role NCP-A) and as consumer (role NCP-B); except when NCP-B provides the eDispensation to NCP-A (as a notification). To this end the NCP is to be connected to two infrastructures: First, it is

to be legally connected to its MS's national eHealth infrastructure. Second, it is to be connected to the epSOS circle of trust.

NCP must have a mandate from the national organisation to access the medical information (also identification & authorisation) of patients (role NCP-A). In the other role, role B, the NCP must have a mandate from the national organisation to use the national infrastructure for authentication and authorisation of HCPs identification of patient process.

Necessary adaptation, now and in the future, in the national infrastructure as a result of supporting epSOS must be specified in agreements between epSOS and the MS. Conversely, future adaptations in the national infrastructure are bound to occur as well. This must be taken into account in the NCP: its connection to the national infrastructure should be checked to see what the effect of local adaptations to the national infrastructure is.

The NCP must be connected to the epSOS infrastructure: The NCP is part of a "federation" (called the epSOS circle of trust). PKI credentials (keys and certificates), used to technically implement the circle of trust, must be protected by technical and organisational measures. Procedures for requesting new credentials in case the current credentials are compromised or in case of failure should be setup with the certificate authority (CA).

Enrolment of a (new) NCP means connecting the new NCP to the epSOS circle of trust (possibly means updating the other NCPs). Organisationally, this means approving the security policy of the new NCP (cf. D3.6.2; page 47). The organisation responsible for maintaining the NCP (and therefore partially responsible for the circle of trust) should have the resources to carry out such approvals (though this may not be relevant during the pilot phase).

6.2 NCP Operating Organisation (Selected Processes)

This chapter describes the organisational setup and procedures within these for operating the NCP. ITIL[21] has been used as framework for the following sections. The selected service and support processes have been deemed minimal requirement for operating the NCPs in a coherent way.

It is for to the MS to decide the actual implemented operating management framework, as long as the described functions are established and implemented for cooperation between MSs.

Special notice should be given to the chapter, *6.3 Security Organisation*.

The chapter is targeted towards service, support and security management and staff.

6.2.1 Support Organisation.

6.2.1.1 Incident Management

Purpose

All MS must have Incident Management in place for the epSOS pilot phase as well as future operation of epSOS. Incident Management is part of the organisation around the NCP or the country. As part of the Incident Management system, the MS must have a service desk function. This service desk function will differ from country to country.

[21]" ITIL® is the only consistent and comprehensive documentation of best practice for IT Service Management. [...] ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT. ITIL has been developed in recognition of organisations' growing dependency on IT and embodies best practices for IT Service Management." (http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp)

Incidents can be technical, organisational or practical.

Incident Management is important for the individual MS operations organisation of epSOS in the country itself (country A), as well as other epSOS countries (country Bs) should be able to contact the MS in case of technical or organisational problems in running epSOS.

Incident Management aims to restore normal service operation as quickly as possible and minimise the adverse effect on business operations, thus ensuring that the best possible levels of service-quality and -availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits (see chapter 6.2.1.4). An 'Incident' is any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

Primary functions of the Service Desk include:

- Incident control: life-cycle management of all service requests
- Communication: keeping the customer informed of progress and advising on workarounds

Approach
For operating the epSOS pilots, each MS must have the following functions in place organised as a part of the NCP in the country:

- Single point of contact (SPOC)(on national level)(see chapter 7.4.2)
- Single point of entry
- Single point of exit

MS can organise their Incident Management and Service Desk as it is best fitted into the IT-operation organisation of the MS. It could be as part of operating the infrastructure of the country or as a self-contained unit.

Contact information (telephone no. and email addresses) of the NCP Service Desk for each MS should be provided and should be updated by each of the MS, when needed.

6.2.1.2 Problem Management

Purpose
Problem Management aims to resolve the root causes of incidents and thus to minimise the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A `problem' is an unknown underlying cause of one or more incidents, and a `known error' is a problem that is successfully diagnosed and for which either a work around or a permanent resolution has been identified.

Problems and known errors are defined as follows

Problem management differs from *incident management*. The principal purpose of *problem management* is to find and resolve the root cause of a problem and prevention of incidents; the purpose of *incident management* is to return the service to normal level as soon as possible, with smallest possible business impact.

Approach
epSOS MS must have organised ways to solve problems in operating the Piloting phase of epSOS. It is here called *Problem Management* but MS might have other names for such functions.
For epSOS purposes the Problem Management should be part of running the NCP as a technical, organisational and practical entity, but epSOS problems to be solved in a country can of course also involve the infrastructure of the country and the PoC.

6.2.1.3 Change Management

Purpose

Change Management aims to ensure that standardised methods and procedures are used for efficient handling of all changes in the technical setup, in the organisational setup or in practical matters in a MS.

A change is “an event that results in a new status of one or more configuration items” which is approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure.

The main aims of Change Management include:

- Minimal disruption of services
- Reduction in back-out activities
- Economic utilisation of resources involved in the change

Approach

Each MS must have a documented process of implementing changes of technical, organisational and practical kinds. The change process must include proper planning and ensure that sufficient information has been disseminated in the MS and to other epSOS MS piloting the epSOS services.

MS making changes in their processes or in their systems must inform other countries about such changes either by mail-communications or by a central information board which might be implemented at a later phase.

If changes involve systems or processes in other countries it must be decided in a *CAB (Change Advisory Board) which for epSOS is PSB.* Such changes should be avoided, but they can be necessary to get the technical solutions to run without serious errors. Legal changes in a country can also impose changes in the epSOS - processes which also involve other countries and have to be handled in a CAB.

6.2.1.4 Service Level Management

The objectives of the epSOS Service Level Management Process are:

- To **list the epSOS Service Levels defined by the Consortium**. The Members States are responsible for delivering a particular service within the agreed service levels.
- To **report on MSs Service Levels**. The Members States are responsible for providing a periodic report on their achieved service levels, their ongoing measures for service improvement and any exceptional events.

epSOS Service Level Agreements (SLA)

The SLA describes the service level targets. Service Levels are defined by the Consortium so that it provides a unified Service Level to the users.

SLA is defined for the following services delivered by the MSs:

- epSOS Systems (eDispensing, ePrescription and Patient Summary)
- Service Desk

- epSOS Systems SLA

  Availability:

  Availability is the property of being accessible and usable upon demand by an authorised entity (ISO 7498-2:1998). Availability is usually expressed as a percentage of uptime in a given period, presuming that the system is required to operate continuously. If a user cannot access

the system, it is said to be unavailable. Generally, the term downtime is used to refer to periods when a system is unavailable.

The epSOS System availability level must be at least 95% per month, 7 days a week from 7.00 am to 8.00 pm, corresponding to downtime between 19,5 and 39 hours per month (30 days).

The availability level is determined on a service level on the NCP of the given MS from the point of view of another NCP. In other words, the NCP service of a MS has to be available for service requests from other NCPs minimum 95% of the time in the given time period. In clustered setups availability is measured on the entire cluster rather than individual cluster nodes.

Network components outside of the NCP infrastructure are not included in availability measurements.

Since epSOS is a pilot a higher availability level is not required. The financial investment level between 95% availability (from 7.00 am to 8.00 pm) and 99% availability (24 hours /day) is very high. On the other hand, a lower availability than 95% is not recommendable as the available uptime for the whole epSOS system in worst case then will be less than 60%. This figure will be even lower when the differences in time zones in Europe are taken into consideration.

Monthly calculation:
- 100% of unplanned downtime (application, middleware, operating system failures, etc) are included in unavailability calculations.
- 50% of planned downtime (maintenance, systems configuration changes, etc) are included in unavailability calculations.
- Calculation is done on the 7.00 am to 8.00 pm period.

Integrity:
Full integrity of data and applications must be guaranteed by all the systems participating in the epSOS service delivery. Data and systems must be protected against technical or applicative modifications, whether they are incidental or malicious. It must be proved that the transmitted data has not been damaged, reduced or altered. Each serious event will be detected as soon as possible and MSs will guarantee their ability to come back to a previous normal situation without any loss and/or distortion of information.

The epSOS System integrity level must be appropriate .

Confidentiality:
Whenever identifiable medical data is communicated, stored or processed, the confidentiality of the data must be guaranteed by all the systems participating in the epSOS service delivery. All communication of identifiable data between the epSOS LSP partners must be performed in a way that prohibits any unwanted disclosure of medical data to any third party. Furthermore, all the systems participating in the epSOS service delivery must assure that any data access is possible only via safeguarded, well-defined interfaces.

An unwanted or unlawful disclosure to an unauthorised party must be prohibited at all times.

The epSOS System confidentiality level must be 100%.

Traceability:

Any data access or attempt to access medical data through the epSOS LSP services must be accountable and traceable (throughout the pilot period) e.g. by logging of “who” accessed, “which” medical data from “where” at “what” time under “whose” authority.

Once all audit data is available, a supervising authority must be able to fully recover and reconstruct an access attempt and access path in order to verify its regulatory compliance. The collected data must be available and suitable for scheduled and unscheduled security audits.

All data gathered by the audit services may contain identifiable personal data, and hence must be protected accordingly. Furthermore, since the audit trail may be considered as evidence/proof in potential investigations, all protocols must be fully safeguarded in terms of integrity and confidentiality. Access to the audit trail must be restricted and only be granted to authorised persons with concrete access necessities within epSOS.

The audit services of the epSOS LSP services should collect a pre-defined set of operational data in order to provide an adequate quality- and capacity- assessment. These protocols must only be used for continuous service delivery and/or service improvement, and must not leave the epSOS LSP context.

The epSOS System traceability level must be 100%.

Response Time

The response time considered here is the response time perceived by the user between the instant at which he makes a request and the time it takes to receive a response.

The epSOS functional specifications do not ask for response time SLA. It is very difficult to agree on an end-to-end response time SLA, as multiple systems are used in the Patient Summary and ePrescription Services.

It must be noted, however that the epSOS functional specifications make the following recommendation: “Shall be deemed an acceptable response time to load information of less than 10 seconds”. If we want to achieve this objective, we recommend that each system does not exceed 5 seconds of response time for 95% of the requests.

- Service Desk SLA

The epSOS Consortium has defined only 3 SLA parameters for MSs’ Service Desks. These SLA are related to performance but not to efficiency. It is up to each MS to define its own level of efficiency.

Abandonment Rate: Percentage of calls abandoned while waiting to be answered.
ð The Abandonment Rate must be < 10%

Time Service Factor: Percentage of calls answered within a definite timeframe.
ð The Time Service Factor must be > 80% of calls answered in 30 seconds or less (also automatic telephone queues).

First Call Resolution: Percentage of incoming calls that can be resolved without the use of a call-back or without having the caller call back the service desk to finish resolving the case.
ð The First Call Resolution must be > 80%.

Report on MS Service Levels

It is the responsibility of each MS to provide (publish) a periodic report on their achieved service levels, their ongoing measures for service improvement and any exceptional event.

(For further information about SLA for Central Services, please refer to D3.9.2)

6.2.1.5 Configuration Management

Configuration management holds, controls and issues information on all configuration items (CIs) and their components necessary for installing and operating an IT system. It covers the identification, recording and reporting of its components with their versions, constituent components and relationships. CIs under the control of Configuration Management include hardware, software and all associated documentation.

This chapter is important for the MS and is therefore included in the guidelines. However, final decisions for the central services, which influence this chapter, have not been taken.

Scope in epSOS

The PSB meeting on 21st June 2010 concluded that some central services including the management and provision of specific data will be implemented in epSOS as a service to the MSs, to be hosted by a volunteering beneficiary. epSOS is in the process of specifying the requirements towards these services and publishing them for reference.

Semantic operability in epSOS is based on a specific terminology developed for the purposes of the project and provided for usage to all participating MS. A central service eCRTS will manage this terminology with the support of the MSs and make it available to each NCP. The functionalities offered by the service will be described in the epSOS Pilot System Components Specification D3.9.1 chapter 5.3.1 along with the technical details on architecture and interfaces to be used. The process of terminology generation and management can be found for reference in chapter 5.3.3.

A central service Configuration Repository Manager will control and provide specific data to the NCPs located in the MSs thus facilitating the interoperability of all NCPs during their operation. The functionalities offered by the service will be described in the epSOS Pilot System Components Specification D3.9.1 chapter 5.2.1 along with the technical details on architecture and interfaces to be used. The list of data which can be retrieved by each NCP will be provided in chapter 5.2.3.

While the above services will support the NCP operation with some centrally managed data, it lies in the responsibility of each MS to ensure that their NCP is interoperable with all other NCPs, thus assuming alignment with their configuration.

Technical Realisation

Configuration data required for the NCPs' successful interoperability with partners during the pilot operation include static location tables as described in D3.3.2, epSOS HLDD which will be employed for service discovery and location. Therefore, according to D3.4.2 chapter 2.1.4, each NCP MUST provide its service addresses and certificates in a centrally managed location table, at the same time each NCP MUST hold a copy of the other NCPs' location tables as part of its internal configuration. This way the NCP assumes responsibility for holding the updated location table locally. The epSOS Configuration Repository Manager assumes responsibility for providing the compiled location table to the NCP via a defined interface as referenced above.

Chapter 4.5 of this documents deals with a detailed technical solution for the storage and transfer of configuration data in epSOS introducing the concept of a virtual central service (see example hereof in 4.5.1), however decision on final design of central services is missing.

Will be finally described in D3.4.2 and D3.9.2.

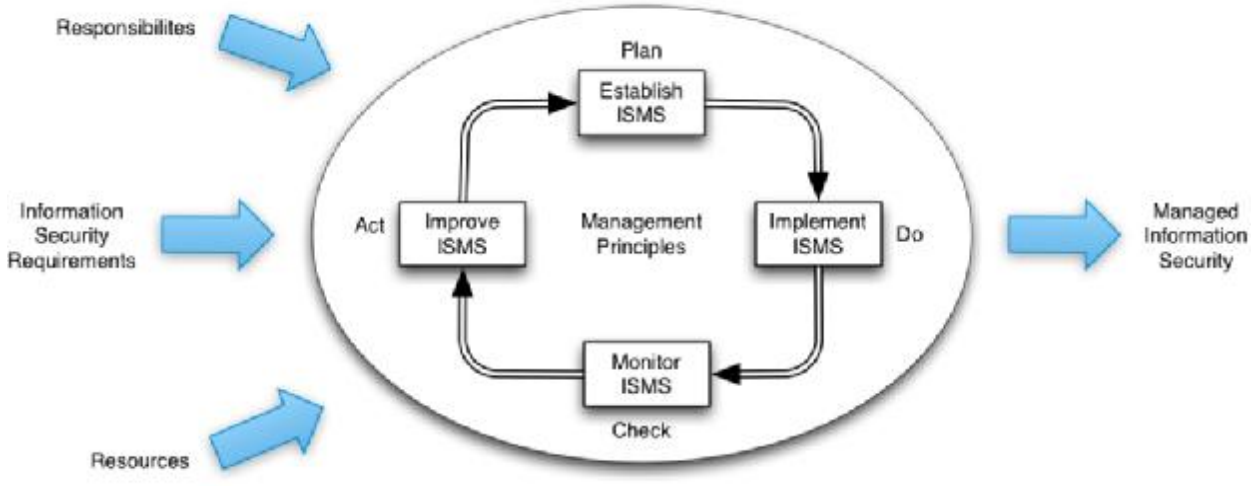
6.2.1.6 Security Management

Please refer to chapter 6.3.

6.3 Security Organisation

The purpose of security management is to fulfil security requirements in a consistent way open to scrutiny. We are using the terminology and structure of ISO 27001 as the current best practice to describe how information security is to be managed in epSOS. However, NCPs are free to adopt different schemes and standards.

General requirements
"*The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS*[22] *within the context of the organization's overall business activities and the risks it faces. The process used is based on the PDCA model shown below.*" [ISO27001/4.1]



Establishing an ISMS
A large portion of the work needed to establish an ISMS is provided by epSOS. The following table shows the security-related tasks, deliverables and responsible units:

Unit	Task	ISO 27001	Deliverable
Commission	Define scope, objectives, boundaries	4.2.1 a)	Annex I (B1.1.2, B3.6)
epSOS WP 3.1	Define business-level security requirements	4.2.1 a)	D3.1.2 (FR01-04, NFR02, NFR04-12)
epSOS WP 3.7	Define business-level security requirements	4.2.1 a)	D3.7.2/Section I - Security Policy chapters 1 - 2.3
epSOS WP 3.7	Set security goals	4.2.1 b)	D3.7.2/Master Doc Chapter 3
epSOS WP 3.7	Select risk management approach	4.2.1 c)	D3.7.2/Master Doc Chapter 3 (combined approach)
epSOS WP 3.7	Identify risks	4.2.1 d)	D3.7.2/Master Doc Chapter 5.1 (data classification)
epSOS WP 3.7	Analyze risk per security service (informal)	4.2.1 e-f)	D3.7.2/Section II
epSOS WP 3.8	Analyze risk (baseline approach)	4.2.1 e-f)	D3.8.1/Annex
epSOS WP 2.1	Define legal basis for trust domain	4.2.1 g)	Pilot contract FWA
epSOS WP 3.7	Define high-level security controls	4.2.1 g)	D3.7.2/Section I – epSOS Security Policy 2.4-2.5
NCP	Commit management to information security	4.2.1 b)	Approved NCP security policy
NCP	Define management responsibility	5.1	Provision of resources; Training, internal audits
NCP	Add NCP-specific risks and requirements	4.2.1 d)	NCP inventory of assets
NCP	Approve proposed residual risks.	4.2.1 h)	ISMS documentation
NCP	Obtain authorization for ISMS operation	4.2.1 i)	ISMS documentation
NCP	Prepare statement of applicability	4.2.1 j)	NCP statement of applicability
NCP	prepare ISMS operating procedures	4.2.3 c)	ISMS operating procedures manual
NCP	keep ISMS records	4.3.3	ISMS document management

22 ISMS: Information Security Managed System

Annex I of this document contains documents to simplify the establishment of an ISMS for the NCP:

- NCP security policy
- NCP baseline security profile (requirements and recommendations)
- NCP baseline security checklist (can be used for an ISO 27001 SOA)

The creation of the SOA (statement of applicability), which handles each single security control, is the main document that defines the safeguards to be implemented. It is:

- An explanation of how the organization complies with them
- An explanation and justification of any deviations from them

6.4 Auditing Organisation

This chapter is an informative chapter as final decisions on auditing has not yet been taken. However, it is an important chapter for the MS as they need to prepare for auditing.

The chapter is in general referring to the security chapter 6.3 and the documents in the Annex I of this document. All security auditing must be related to the security policy and the security baseline documents. It should be noticed that auditing is concerning technical, clinical, physical and organisational processes in the MS.

As known for now, the auditing will be organised as self-assessment by the MS. This means that the MS must follow certain rules for their auditing processes:

1. MS should appoint one or more skilled auditors and form an auditor structure.
2. MS will write a report stating which audits have been carried out in the country and if all required security measures in the baseline document have been met (the formal structure of the report will be an epSOS checklist).
3. First auditing must be finished and treated in PSB before pilot operation phase 1 with real patients.
4. Afterwards, one audit per year is needed according to epSOS 1 discussions, but might be adjusted after start of epSOS 2.

6.5 Central Services

The Central Services are described in D3.9.1 Chapter 5 and in D3.9.2 in which the Service Level Agreement has also been agreed upon.
In particular: Chapter 5.1 describes Central Service Goal and makes proposal on associated responsibilities.

- Chapter 5.2 describes functions and structures of Configuration Repository Manager.
- Chapter 5.3 defines epSOS Central Reference TerminologyService.

6.6 Organising the Test Procedures

Before a MS can participate in epSOS LSP Operation some test steps, which are described in this chapter, have to be fulfilled (further information can be found in D3.9.2).

epSOS will provide test cases and simulators based on IHE-Europe test tool (Gazelle). With Gazelle all functional requirement and use cases of epSOS can be tested.

6.6.1 Gazelle

Gazelle was developed by IHE Europe and includes following:

- Test Cases, described as a Storyboard, to run tests step by step

- Simulators for test step by step
- Simulator for NCP A
- Simulator for NCP
- Simulator for end-2-end tests
    - For Patient Summary
    - For ePrescription
    - For eDispensation

6.6.1.1 Simulators

The Simulators will support the tests to make it easier and to check the outcome. Test Cases are prepared for step by step tests or complete workflows. (e.g.: Test of Patient Summary)

6.6.1.2 Test Data

Dummy Test Data will be provided by IHE-Europe and from different MS. Those test data should be used by the MS too.

6.6.2 Lab Tests

These tests are the first steps in order of the tests and have to be run within the MS. Target is to run successfully the pre-tests for epSOS Projectathon.
For these tests epSOS will not deliver a simulator – the messages to/from the National Connector to the National Infrastructure have to be monitored

6.6.2.1 Test of Common Components of FET

Before the Common Components will be handed over to MS, FET will test their application with dummy data based under test cases of Gazelle.

6.6.2.2 Test of National Connector within MS

6.6.2.2.1 Test as Country A

The National Infrastructure has to handle with the National Connector following Use Cases

- HCP Authentication
- Patient Identification
- Validation of Patient Consent
- Patient Summary: CDA Document of Patient Summary
- ePrescription: List of ePrescriptions

6.6.2.2.2 Test as Country B

Country B can work either via Portal (will be developed by epSOS) or National Infrastructure has to handle with the National Connector following Use Cases

- HCP Authentication
- Patient Identification: Identifier of Patients
- Patient Consent
- Confirmation
- Display of Patient Summary
- Display and Select of ePrescriptions
- Sending eDispensation

6.6.2.3 Tests from/to National Connector from/to NCP

These tests will be supported with several simulators developed by IHE Europe which can and should be used from the MS. Test for Country B can be done either via Portal (will be developed by epSOS) or National Infrastructure.

6.6.3 Projectathon (PAT) Pre-Tests

For participating on PAT the MS have to report that all Gazelle Test Cases were fulfilled depending on the scenarios (defined from WP 4.1).
Only MS which positive results can participate at PAT

6.6.4 Projectathon

Projectathon (PAT) tests interoperability between different MS. The plan is to have end-2-end tests (National Infrastructure A -> NCP-A -> NCP-B -> National Infrastructure B and vice versa)

At the moment, two PAT's are planned:
- First PAT: November 2010 in Bratislava
- Second PAT: mid of April 2011 in Pisa (together with IHE Connect-a-thon)

6.6.5 Pre-Pilot

In this phase several MS will test different scenarios with test data and virtual patients on a test environment. This test environment should be available during 2011 for testing of additional scenarios and for extending epSOS in the future. Each MS should participate in the minimum with one pilot.

6.7 NCP Roles

Below is a list of important roles related to epSOS piloting. These roles are legal, organisational and practical. The list might not be exhaustive and may vary from MS to MS.

Role	Description
Change manager	A person-role, but the role can be shared. See chapter 6.2.1.3 and Chapter 10 Glossary for tasks for Change Manager
CIO (Chief Information Officer)/IT manager	Equal to ICT system manager.
Citizens	Citizens are individuals in MSs who can be patients, relatives of patients, carers or persons who may need to have access to healthcare in the future. At its simplest, citizens are represented as the total population of a MS.
Configuration manager	A person-role, but the role can be shared. See chapter 6.2.1.5 and Chapter 10 Glossary for tasks for Configuration Manager
Data controller	Is here understood as a term from European Directive 95/46/EC. See chapter 5.2.1 and chapter 10 Glossary. Not a person-role, but a legal person (entity) controlling personal data.
Data processor	Is here understood as a term from European Directive 95/46/EC. See chapter 5.2.1 and chapter 10 Glossary. Not a person-role, but a legal person (entity) processing data on behalf of the Data Controller.
”epSOS officer” – Information	Person responsible for contacting GPs, pharmacists, hospitals, system administrators etc. informing them about epSOS and involving them in the project.
“epSOS officer” – Marketing	Person responsible for marketing towards citizens and other stakeholders.
“epSOS officer” - Training	Person responsible for training GPs, pharmacists, hospitals, system administrators etc. in use of epSOS system.
European	The Commission's job is to represent the common European interest to all

Commission	the EU countries. To allow it to play its role as 'guardian of the treaties' and defender of the general interest. The Commission has the right of initiative in the lawmaking process. The Commission is also responsible for putting the EU's common policies into practice and manage the EU's budget and programmes. epSOS has been institutionalised by the Commission. epSOS is referring to the Commission as well as the MSs. The Commission is reviewing epSOS as the Commission is a financial contributor to epSOS.
Evaluation responsible	Person responsible for evaluation of epSOS services. Evaluation instructions delivered by WP1.2.
Health Care Professional (HCP)	A doctor of medicine or a nurse responsible for general care or a dental practitioner or a midwife or a pharmacist within the meaning of Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC . This means that a Health Care Professional is a person who delivers health care or care products professionally to any individual in need of health care services, in order to prevent, relieve or treat a medical problem.
HCPO	Health Care Provider Organisation is an institution, authorised to provide health care services, univocally identified in the set of the Health Care Institutions. Examples: Health Centre / Hospital / Medical Emergency Vehicle / Medical Practice / Pharmacy.
HCPO Contact Person	Is the coordinator between SPOC and PoC.
Health Term Administrator	Person responsible for technical support to the MS terminology team (the MS end users) in their creation of the MS's terminology content (for more information please refer to *epSOS Central Reference Terminology Service: A description of roles regarding using the CareCom tool: HealthTerm,* page 6, produced by WP3.9).
Hospital manager	Manager who is responsible for the epSOS services at a pilot hospital.
Hospital president/director (CEO)	Person responsible for all functions and staff at a hospital.
Hospital staff	People working at a hospital which is participating as an epSOS pilot point of contact. Can be administrative, clinical or technical.
ICT System manager	An information systems manager is responsible for the computer systems within a company, overseeing installation, ensuring back up systems operate effectively, purchasing hardware and software, providing the ICT technology infrastructures for an organisation, and contributing to organisational policy regarding quality standards and strategic planning.
Incident manager	A person-role, but the role can be shared. See chapter 6.2.1.1 and Chapter 10 Glossary for tasks for Incident Manager
IT architect	Designing IT-systems. The architect uses different tools to design systems. Usually the architect starts form the Use Case -description and can use Entity Relationship diagrams or UML (Unified Modelling Language) as modelling tools. The IT-architect are using SW – standards in his design. In epSOS an important standards are HL7 and IHE.
Legal responsible person	Legal expert representing MS and responsible for legal activities in MS concerning Pilot preparations. Assure progress in legal pilot preparations and provide reporting on it to WP4.2.
National Authority Beneficiary (NAB)	National health authorities which is represented in epSOS for each MS.

National Contact Point (NCP)	Organisation 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.
NCP manager(s) (person(s) or organisation)	The NCP needs managers who are responsible for setting up and running the NCP. This can be person(s) or an organisation which has signed a contract with the NAB and is therefore included in the epSOS circle of trust.
Patient	Any natural person who receives or wishes to receive health care in a MS
Pharmacist	Pharmacist working at a pharmacy involved in epSOS.
Pilot site manager	Person responsible for epSOS services at pilot site level.
Point of Care (PoC)	Any pilot location where health care is provided.
Problem manager	A person-role, but the role can be shared. See chapter 6.2.1.2 and Chapter 10 Glossary for tasks for Problem Manager
Security Auditor (person or organisation)	Person or organisation in a MS taking care of auditing the security for epSOS and epSOS connected ITC systems.
Security manager	A person-role, but the role can be shared. See chapter 6.2.1.6, pointing at chapter 6.3, again pointing at annex.
Single Point of Contact (SPOC)	MS's single point of contact for epSOS (MS SPOC): • Acts as the single responsible point for communication epSOS-to-MS and MS-to-epSOS for all matters concerning the piloting activities of the MS. • Can be an organisation or a person. • Different aspects (organisational, legal, technical and clinical) can be covered by different persons/orgs.
System administrator	epSOS System administrator is a person (person-role) which has access to alter and correct the system, set up new user accounts. The System administrator must typically have access to all part of the system and by that data in the system. This means root access. Usually responsible for system and network.
System developer	System Developer, one who programs computers or designs the system to match the requirements of a system analyst or IT-architect.
Terminology responsible	Person who is responsible for the MS's creation of the MS's terminology content (for more information please refer to *epSOS Central Reference Terminology Service: A description of roles regarding using the CareCom tool: HealthTerm,* page 5, produced by WP3.9).
Test manager	If appointed, the test manager should follow the epSOS test strategy to Quality assure the epSOS system with interface to National Infrastructure (Projectathon, Field test etc.)

7 Practicalities

7.1 Manual processes

This chapter cannot be more than advisory, as it is up to the MS to decide how to run their business processes. Nevertheless, the MS must be able to describe their business processes, so the needed auditing can take place in a transparent way.
This chapter can be addressed to all who have interest in epSOS and the epSOS pilots, but most importantly it is addressed to the people responsible for setting up and running the NCP.

7.1.1 How to run the NCP in daily use

There are several practical aspects of operating the NCP in daily use:

1. The Framework Agreement
   Be aware of the FWA to be sure that all national contracts are maintained.

2. The National Contact Point (Single point of contact)
   The daily communication between the GPs, Pharmacies, Hospitals and other epSOS entities must be taken care of by the NCP organisation/SPOC. Communication will be electronically as well as orally communicated. It is important to establish the communication channels with necessary telephone numbers, addresses etc for a service desk/service staff, system administrators etc.

3. Managing staff
   A managing structure for all staff involved in the epSOS pilots must be described. Especially, it is important that epSOS system administrators are aware of the security responsibilities in the trusted circles of epSOS, and a sufficient Non Disclosure Agreement is kept with the epSOS system administrators.

   It is important that management care for initial training. In order to maintain the level of service, further training is necessary along the way. See A.8.1.1 - NCP BSP of Annex 1 of this document.

4. Security matters
   The management of the NCP must be particular aware of the rules described in chapter 6.2.1.6 Security Management and chapter 6.3 Security organisation.

5. Security Auditing
   Described in Chapter 6.4.

6. Statistics and Reporting (SLA-reporting)
   There will be statistics and reporting within the MS concerning the NCP as well as epSOS reporting. The responsibility for such reporting must be decided, so epSOS can use the NCP for communicating.

7. Evaluations
   The required evaluation of epSOS pilots according to the regulations in chapter 8 Guidelines for epSOS pilot evaluation is the responsibility of the management of the NCP in the MS.

8. NCP economy
   Can be separate or part of MS infrastructure economy, but there will be separate epSOS economy which is the responsibility of the MS NCP management.

9. Maintaining the technical set up (Service contracts)
   Needed daily adjustment of server parameters should be done by NCP staff to optimise the operation of the NCP.

10. Updating the Technical set up. (According to epSOS development and according to technical development)
    Updating the HW, System SW and the epSOS applications must be done surely and according to need and central decisions. The MS NCP management will be responsible.

7.1.2 How to handle epSOS at the PoC

In order to handle epSOS at the PoC the following aspects must be dealt with:

1. Training
The potential users of the epSOS pilot service must have been trained and must be familiar with the pilot services. In the training they will need to be informed of the aspects mentioned in this chapter.

2. Legal aspects
The potential users of the pilot service must be aware of their responsibilities, rights and duties, including processing of patient consent, HCP authentication access to the patient information, data protection, liabilities when providing the service to the patient:

- The pharmacist might consider he has not proper or right information to dispense a medicine, so he decides not to dispense it, liabilities regarding the medicines they have dispensed (the information about the medicines dispensed must be recorded).
- A HCP can decide not to use the information provided in the PS if he/she considers that the information is not right or proper. (all accesses must be recorded).

3. Security
The HCP must be authenticated in the epSOS service pilot applications.

Patient information disclosure must be prevented. If during the process, an error occurs, the pharmacist/doctor should follow the errors guidelines provided by his support services[23].

4. Safety
At the PoC the HCP should be aware that the original information from country A could be consulted. In the case of the eP service, the information about the medicines dispensed has to be recorded during the process of dispensing in the epSOS eP service pilot application to be sent to country A. The information provided by country A is for that specific encounter. If a new encounter takes place (i.e. patient leaves the PoC and thus, the patient's session has been closed; some time later he comes back again), all the process has to be performed again as the patient summary or the patient treatment administration routine might have changed.
The HCP might decide that the information he has is not enough either to give the service to the patient so he will need to inform the patient and advice him about possible solutions

If during the process, an error occurs, the HCP should follow the errors guidelines provided by his support services.

5. Support
A service desk is available where the HCP can find information and report problems. For more information, please refer to chapter 6.2.1.1.

[23] Errors guidelines will be produced by WP4.3 to be completed by each beneficiary piloting and distributed to all HCPs

6. Information to patients
Potential patients will need to be informed of the epSOS services at the PoC. The information will need to include the description and goal of the service, the pharmacist/doctor and the patient responsibilities, rights and duties, the objective and content of the patient's consent (why, about what, duration, type of consent), which patient's information is accessed, how this information is handled (what information is going to be kept by the HCP, if any, why and security measures).
As a summary, the process could be:
Some pre-requisites are needed to be in place in order to handle an epSOS patient:

- The PoC is legally authorised and registered to use the pilot epSOS service
- The dispenser/doctor has been previously trained and is familiar with the pilot service
- The pilot service is available at the PoC
- The PoC has information about the pilot service (description of the pilot service, possible outcomes legal aspects, rights and duties) in the different languages to inform the potential epSOS patients
- A service desk is available (for information purposes and to report problems)

When a potential epSOS patient arrives at the PoC he should be informed of the pilot service. Once the patient has been informed and if he wishes to use the service, the HCP must be able to authenticate himself, if not done previously, in the service. The HCP then should ask for an identification of the patient and for his consent to access to his information.

- After successful identification of the patient and registration of the consent, a list of available prescriptions are shown to the pharmacist and he should be able to check with the patient which prescriptions he wants to withdraw. When dispensing the medicines, the information about these medicines have to be recorded in the pharmacist's system to be further treated in epSOS by NCP-B and NCP-A, and when the patient is about to leave, the pharmacist has to log out of the patient session. If the pharmacist considers that he has not proper or right information to dispense a medicine, he should inform the patient and advice him about possible solutions.
- After registration of the consent and successful identification of the patient, the PS is shown to the medical doctor and he should decide if this information is helpful for him.

Each access has to be recorded and stored in the Audit trail repository. For more information on audit trail, please refer to 6.2.1.4 of this document.

In case of an error, the HCP should follow the errors guidelines provided by his support services.

7.2 Manual regulations to run the NCP

This chapter is partly an advisory chapter and partly there are requirements to be fulfilled. It is requirement that servers and server rooms are secure and safe, but it is of course up to the MS to decide the arrangement for such security. It is important to make sure that needed arrangement has been done, so the auditing before the epSOS start can be accepted. Transnational epSOS training appliances will currently be developed and referred to, - not form the beginning of the epSOS pilot period, but after time.

7.2.1 Servers to be used for the NCP – virtual/dedicated

The servers to be used for NCP can be either dedicated servers or virtual servers, according to decision in the MS. The servers can be part of the existing server-environment of the infrastructure in the MS or they can be placed in a special set up for the epSOS. There can be one or more physical servers with one or more logical servers.

The server set up must be able to fulfil the agreed epSOS Service Level Agreement by having the needed redundancy for server capacity, storage capacity, switch capacity, emergency Power Supply etc.

In all cases the servers must fulfil the demand of security and auditing (see chapter 6.3 and 6.4) and the servers must be according to chapter 4.4.9 Platforms in Technical Issues.

7.2.2 Securing the server room and servers

The epSOS Security Group stresses the importance of securing the server rooms and epSOS servers within it. This is caused by the fact that the technical security and accessibility can easily be broken if servers and server rooms are not secure.

For more information about this topic, please refer to chapter 6.3 and Annex I of the guidelines.

7.2.3 Training System administrators and other support staff

Education of and information to system administrators and other staff is a very important and critical factor and will be achieved through a specific introduction session. A training process for support staff will be a series of activities which aim at enabling them to assimilate and develop knowledge, skills, values and understanding a broad range of problems in a way that can analysed and solved.

7.2.3.1 Objectives

The objective of the training process is to provide support staff with sufficient skills in order to support the operation and maintenance of epSOS software, system software and hardware.
Administrator training in general will focus on areas including, but not limited to, system set-up, configuration, system maintenance, administration utilities, security administration and backup/restore of the system.

More specific:

- Knowledge of epSOS architecture
- Knowledge of used standards for communication and interoperability among systems
- Knowledge of support and troubleshooting of systems interfacing
- Installation, set-up and configuration of epSOS software and hardware
- System maintenance of epSOS software and hardware
- Security administration of epSOS software and hardware
- Backup/restore of the system and supporting of availability options

7.2.3.2 Training Process

The design and delivery of training programmes will be based on deploying general terms, references, and standards of the European and international policies towards Training. These standards involve:

- The Background and experience of the training Consultants
- The quality of the training material
- The quality of the means used to deliver the Training sessions

A basic model for a systematic approach and base activities to training would be:

- Investigate training needs
- Design training
- Conduct training
- Assess effectiveness of training

The model of a systematic approach to training has been presented here, as a number of stages which have been arranged in a sequential order:

- **Analyses for Training**

During the analysis stage, information will be gathered which identifies the main objectives, the conditions under which it is performed, responsibilities, main and subsidiary tasks, difficulties and distastes, etc. Consideration would need to be given to such factors as the importance or the difficulty of the tasks and how frequently they are performed.
This would help to decide the nature of the training which needs to be undertaken for the specific MS or by what other means the performance gap could be filled.

- **Prepare training objectives**

Training objectives must be specified in details to provide unambiguous statements which describe precisely what trainees are expected to be able to do as a result of their learning experience.

- **Consider principles of learning, motivation and training methods**

Having identified earlier the knowledge, skills and attitudes which trainees need to acquire, the trainer should then be concerned with creating a suitable environment to ensure that the training objectives can be achieved. A part of that training environment is the methodology which the trainer can use. Another part includes such factors as physical arrangements, time of day, resources, etc. However, consideration must be given, at this stage, to the principles of learning and motivation such as knowledge of results, reinforcement, rehearsal, practice, etc that may need to be embedded in the training environment.

- **Design and pilot training**

The design of training involves the translation of objectives and strategies into a balanced programme of instruction and learning. This does not necessarily mean a course; it could be a learning package, a video, computer-based training, etc, or it may include a number of different methods and strategies.
Piloting of every aspect of the training programme including administration should be planned in detail and executed.

- **Deliver the training**

Within this stage, the Training material designed and developed will be delivered to the relevant personnel. The courses will cover all the objectives that were indentified at previous stages.

- **Internal validation**

Internal validation is the process of measuring trainees' performance to see if they have achieved the objectives of the training. Information to make this assessment needs to be obtained in two ways. Firstly, a series of tests, exercises and assessment instruments should be designed and used to examine objectively or to check on the progress of trainees. Secondly, trainers need to seek the views of trainees on their training programme including such factors as the performance of their tutors or instructors, the learning materials and the environment.

7.2.4 Nondisclosure agreement for system administrators

Generally NCP system administrators will have no need to see the contents of any data packages passing in the NCP. The administrator will only need to ensure that all authentications are correctly certified and assure the non-repudiation of the data transfer. In some circumstances it may however be necessary that, in the course of audit, maintenance or error management the system administrator accesses the content of data packages.

As already described some MS will not be allow such access to patient identifiable data, accordingly they must provide some mechanism whereby data can be duly anonymised or where some duly authorised person can access the system in order to undertake the necessary work.

In many MS the local legislation will however allow for access to patient identifiable data by people other than accredited medical personnel on this basis of contracts conferring a duty of responsibility. Where this is provided for in national legislation such contractual non-disclosure agreements should be foreseen. In accordance with DPA, such NDAs should include a term which allow for necessary legal action of any person who breaches the NDA.

7.3 Marketing Activities

An important part of the epSOS piloting activities is marketing. Some marketing activities can be applied to all target groups and some are specific for each group. In this first part, general activities for pharmacies, hospitals and GP clinics are mentioned. Afterwards, more specific information about the different groups is elaborated.

These guidelines are only meant as inspiration/recommendation as each country is advised to use its usual communication channels/structures to reach the pharmacies, hospitals, GPs and citizens/patients. The marketing /information activities about the epSOS pilots must be integrated into the existing National and or Regional eHealth channels. These different and possible communication layers are country specific. The communication must be started by the local authority responsible for the pilot site, which is liable for the pilot duties under the FWA signed by the NCP.

It is advisable to use three-tiered communication and top-down integration.
To approach the professionals at the pharmacies, hospitals and GPs the authorities at the different and specific levels of power may instantiate the following activities step by step:

1. The entity responsible for the epSOS piloting in the pilot site must call for an informative session through a formal letter to relevant persons (for example general hospital manager, individual doctors, pharmacies, data controller and data processors). This could be one meeting for all or individual meetings for pharmacists, hospital staff and GPs etc. Invited persons to the “presentation” are, in addition to the general manager, the Information Systems responsible, the hospital responsible for the services, main insurance organisations for which the professionals may work and the persons responsible for accounting regarding health care charging. In some cases, some roles may be embodied in one person, may not exist or be irrelevant. This depends on the national setup.
   Necessary announcement/invitation to stake holders, for example the Medical professionals’ territorial associations, to the informative session must be considered.

2. Second step, the hospital management will select a small group of doctors and the epSOS project management will select a group of GPs and pharmacists to be trained in epSOS usage. Mainly in the following issues:
   - Objectives of epSOS regarding eP
   - Benefits for the pharmacy/hospital/GP (epSOS pilot and in the future)
   - Benefits for the patient (epSOS pilot and in the future)
   - Duties and rights of the pharmacists/hospital/GP (including own ID or professional certification, patient consent, data protection, safety, security issues etc)
   - Legal framework and implications (including semantics) (please refer to 5.2)
   - Payment and reimbursement
   - Use case description: scope, how to proceed, exceptions, errors

This second step will be replicated in cascaded order until all the staff that will be involved in piloting epSOS ePrescriptions/Patient Summary services is trained.

7.3.1 Hospitals and GPs

Hospitals involved in epSOS piloting may belong to two different typical organisational models. Depending on the organisational model the approach to install and deploy the epSOS platform may vary slightly. Model A: All hospitals involved in the pilot undergo to the same organisational and administrative model and may/may not have strong links to the territorial Medical professional associations. Model B: hospital/s involved present an autonomous management and organisational system/model each one independent from others.

Two layers within the hospital (country specific) may be:

- General Hospital Manager
- Other staff
    - Informatics service centre of the Hospital
    - Entrance and discharge administration department
    - Emergency department
    - Nursery, and those departments involved/committed to epSOS piloting

These units must define three types of activities with the personnel involved in the pilot who will be different from the content point of view and from the time to take place and according to the periodicity.

- Information activities global for all and specific according to personnel duties regarding patient treatment, system access, and ID specificities. (At the beginning)
- Training with a simulation case with a number of professionals (second phase)
- Evaluation information activities about the reporting and success validation (at given times).

The guidelines to instruct and motivate individual GPs participating in epSOS generally follow the same guidelines as those outlined for the hospitals, having two remarkable differences, that are strongly different depending on the fact if the GP belongs to a specific organisational circumscription in terms of centre concentrating several professionals (similar to a policlinic) or if, on the contrary, each professional must be considered as an “isolated” user of epSOS.

Regarding the set of isolated GPs, a second factor affects the whole procedure, and this is related to the insurer organisations to which the professional may have associated his/her services.

7.3.2 Citizens/Patients

This section describes marketing activities which can be used by epSOS countries to inform its citizens and patients, nationals as well as epSOS patients, of the availability, functionality and framework of epSOS services.

Marketing/information to the citizen/patient:

- Availability of the service
- Benefits of the service
- Security issues (including patient consent, data protection)
- Data
- Legal implications
- Payment and reimbursement

Considering the range of different national systems and infrastructure the guidelines are general and are to be applied on customised national communication plans. The guidelines are based on

the notion of a three-tiered communication and top-down integration between them (i.e. one level forwards information from the above levels). The three levels are:

1. EU level through epSOS WP1.3, Dissemination
2. National/regional
3. Local (HCO, pharmacies)

Further, the guidelines presuppose that epSOS specific information on the national/regional level is integrated into existing eHealth channels and information and that an appointed liaison, single point of contact is responsible for linking the three different levels, epSOS (EU), national/regional and local.

The guidelines focus on marketing activities, meaning that they describe what organisational level is responsible for what information as well as what channels can be used for these purposes. The activities do not describe the actual information to be conveyed in connection to an event or scenario (e.g. dispensation, dosage, consent etc.).

In order to specify information to be directed at patients and citizens, one must first differentiate between country A (home country) and country B (host country). In addition, the activities may differ depending on the location of the patient or citizen, why another distinction has been made between the target groups. To illustrate these basic conditions, the guidelines are divided into three different target groups, describing communication and information by and from each applicable level towards the target group in question, with examples of potential channels. Which channels are used in the end is highly dependent on the existing national infrastructure why the ones mentioned here are only to be considered examples.

Country A informs target groups: citizens, residents and national patients
When acting as country A, the home country, informs target groups 1 and 2: citizens and residents (1) and national patients (2), the latter while in country A or B.

7.3.2.1 Country A, target group 1: Citizens and residents

Country A will make general information about epSOS available to its citizens and residents. This communication is disseminated through three different levels:

Level	Information	Channel
1. EU	The EU level supplies citizens and residents with general information, pilot participants in the epSOS project, further information and contact.	The epsos.eu website acts as a hub with direct information to citizens but also working down-stream towards the lower levels.
2. National/Regional	The national/regional level supplies citizens and residents with information on national/regional pilot participation, pilot functionality, scenarios, patient utility and safety. The national/regional level also forwards information from the EU level.	Examples: 1. Information website (unique or other [e.g. NCP] depending on national existing infrastructure) 2. epsos.eu national sub-site (e.g. epsos.eu/Austria) 3. Media, NCP, government offices, insurance offices, travel agencies, national organisations abroad
3. Local	Information about epSOS to be placed in pharmacies in country A to inform citizens going to Country B. In national language and partner language.	Flyers and posters.

7.3.2.2 Country A, target group 2: National Patients

There are two possible scenarios when national patients should be informed about epSOS, and the level responsible depends on the scenario. The local level informs about epSOS participation during a health care encounter in country A (example 2A). The national/regional level refers travelling patients to the appropriate NCP in country B (example 2B).

Target group 2A: national patient during health care encounter in country A before travel

Level	Information	Channel
1. EU	N/A	N/A
2. National/Regional	N/A	N/A
3. Local	The local level informs their patients of epSOS participation, i.e. of inclusion of the patients' Patient Summary and ePrescription in the epSOS pilot and of their rights (Framework agreement – Annex II) during a health care encounter in country A and before travel. A prerequisite is that information from EU and national information is integrated in the customised patient information, the local level is responsible for the direct information.	Marketing activities at the local level in particular are highly dependent on the national organisation of health care and existing infrastructure. Channels may include: 1. Local HCO websites 2. Customer magazines, newsletters 3. Referrals

Country A, target group 2B: national patient during travel in country B

Level	Information	Channel
1. EU	N/A	N/A
2. National/Regional	The national/regional level shall refer their travelling national patients to the organisation responsible for the NCP in country B for further assistance. To ensure consistency, information on availability of epSOS services is owned and maintained by each MS. To illustrate, country A will not be able to refer a country A citizen to a specific pharmacy in country B, but only to the relevant NCP for further information.	The existing national/regional level channels, which may include health care advisory organisation (phone and website).
3. Local	N/A	N/A

7.3.2.3 Country B, target group 3: epSOS patients

When acting as country B and informing target group 3, epSOS patients (e.g. a patient whose home country is France while travelling in Austria), the following information needs to be made available at the different levels:

Level	Information	Channel
1. EU	The EU level supplies the below levels with epSOS logotype and marketing props.	N/A

2. National/Regional	The national/regional organisations when acting as country B informs epSOS patients of epSOS availability, i.e. complete information on epSOS connected HCOs and pharmacies in the specific country. In addition to the NCP, organisations may include health care advisory organisations (phone and website services) and insurance offices.	To target potential patients, hotels, tourist agencies and foreign missions are considered appropriate channels.
3. Local	When actors as country B, the local level (HCOs, pharmacies) inform epSOS patients about availability and forwards information from prior levels to patients. Direct information regarding patients' rights to an epSOS patient during an event is considered country specific and should be included in the information to HCO/pharmacies through the user interface.	The local levels uses the marketing props supplied by the EU level, e.g. signs and information brochures, and if applicable also communicate using local websites in English

7.3.3 Public Information Policy

In an ideal architecture the workflow has to be organised in a way that healthcare providers and patients using epSOS services do not have to be aware that something like a NCP exists. Therefore, the NCP might only occur in informational material for special target groups. Special target groups are NCP staff, National Authority Beneficiaries and Health Care Providers (in Pharmacies, Hospitals Doctors Office etc.)

The existence and the role of the NCPs in epSOS will be covered in the overall information which should be prepared for an expert audience. Information especially targeted at those groups who are relevant for the setup and continuous service of the NCP might be useful (government, hospital owners, HCP management). This kind of information will differ from country to country, as the mentioned organisations are very much different.

Following the different epSOS target groups in deliverable D 1.3.1 dissemination has to aim at governments and healthcare providers. Special interest information has to accompany the setup and implementation measures. This might be – where necessary – supportive information for the legal process as well as for technical implementation of epSOS tools.
A controversial subject might be the role of the NCP regarding data protection and data security. The preparation of factsheets on these items should be mandatory (please refer to chapter 6.3 and 6.4).

A structured information plan for the target-groups could be:

- communicate information in a structured and consistent way, i.e. about security, identification, semantics and components in epSOS.
- define quality requirements of the information that is communicated
- enable establishment of communication plans containing information on who gets what information when and how

Unspecific information should be provided on the epSOS website, where also individual country information (in native language) might be provided by the beneficiaries.

7.4 Communication Structures

It is important that this chapter is read by managers and staff, organising the communication structure in MS. In the country the communication is up to the MS, but the communication structure should be described for auditing.

7.4.1 NCP as Communication Centre

The NCP works as a national communication node for several directions.

1. towards epSOS – the communication partner towards epSOS is MS Single Point of Contact (SPOC). SPOC works on one hand as liaison body for transmitting the epSOS requirements and coordination directions, on the other hand as the recipient, processor and distributor of the request of NCP towards epSOS. This communication partnership will last from the first day of existence of NCP.
2. towards other pilot sites – after localisation of FWA and extending of trust domain all the way to the pilot sites (by means of the contracts between NCP – pilot site) each pilot site will have the responsible liaison person communicating with epSOS via SPOC (concerning the issues related to coordination of pilot preparation and pilot operation) and with NCP via responsible person mainly for purpose of solving the operational issues (requests receipt and distribution; data quality, integrity and completeness; translations/transcoding).
3. towards the institutions providing the process services (identification; authorisation; audit) if not being integrated in NCP

Pilot sites (in most cases HCPOs) work as a local communication node for several directions:

1. towards NCP – most issues will probably concern coordination between pilot sites and NCP
2. towards epSOS - the communication partner towards epSOS is MS Single Point of Contact (SPOC). List of all SPOCs can be found below. SPOC works on one hand as liaison body for transmitting the epSOS requirements and coordination directions, on the other hand as the recipient, processor and distributor of the request of pilot sites towards epSOS. This communication partnership will last from the first day of existence of (contractual) relation to epSOS.

Each NCP is recommended to point to a role able to deal with technical, legal, semantic and security issues. List should be made available within all epSOS trusted domains.

Each Pilot site should point to a relevant contact person (one or more persons). These persons should have different profiles dependant on the pilot site in question.

Means of communication: standard means of communications should be in use (mail, email, and phone). Use of particular mean of communication depends on seriousness, urgency and security demand. Entire communication that concerns pilot should be recorded in a log book or any other equal way maintained in the MS.

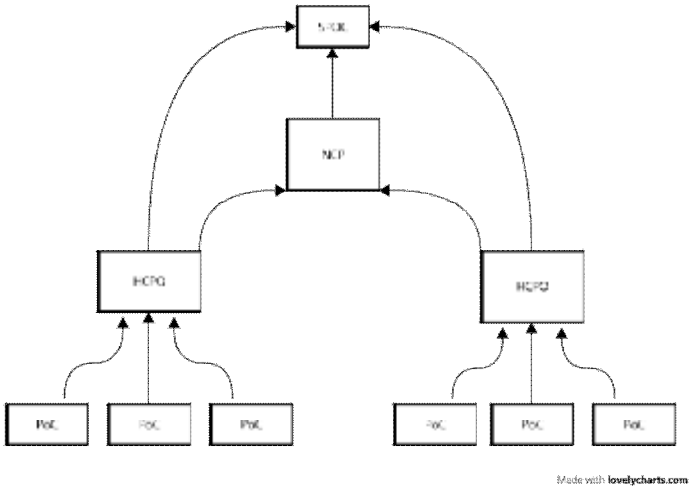


Figure 14: Communication structures

The communication structure can be seen in figure 14. The general idea is that Points of Care (PoC) should not address their communication towards epSOS pilot coordination directly to SPOC but through their HCPO epSOS contact person.

7.4.2 Single Point of Contact

The Single Point of Contact (SPOC) is the institution (either legal entity or the person with close relation to the project) established by epSOS project to ensure the liaison towards related entities external to original project consortium. SPOC has been nominated by each of 10 countries participating in epSOS pilot phase.

From position of pilot partners (HCPO, NCP) SPOC can be addressed with any matter related to pilot preparation and operation.

The SPOCs for each country (per 12.07.2010) are:

State	Beneficiary	Name	email
AT	ELGA	Martin Hurch	martin.hurch@elga.gv.at
CZ	IZIP	Milan Ruzicka	milan.ruzicka@izip.cz
DK	Digital Health	Anni Buhr	abu@sdsd.dk
F	ASIP	Alain Périé	alain.perie@sante.gouv.fr
G	Gematik	Roland Halfpaap	Roland.Halfpaap@gematik.de
GR	THESS	Athanasios Siachoudis	asiach@itc.auth.gr
IT	REGLOM	Marcello Melgara	Marcello.Melgara@cnt.lispa.it
SK	NHIC	Ing. Pavol Rieger	pavol.rieger@nczisk.sk
ES	ESNA	Iciar Abad	iabad@msps.es
SE	SALAR	Eva Leach	eva.leach@skl.se
FI		Matti Makela	matti.makela@thl.fi
EE		Madis Tiik	madis.tiik@e-tervis.ee
CH		Stefan Wyss	Stefan.Wyss@e-health-suisse.ch

List can be found on ProjectPlace here: https://service.projectplace.com/pp/pp.cgi/r473747871

7.5 Semantic Services (MVC and MTC)

This chapter deals with the handling of the semantics in the MS. It does not concern the technical conversion issues, but only how translation and transcoding should be handled by the MS before the start of epSOS, and during the epSOS running period as long as epSOS is in operation.

The chapter should be read by semantic experts and those in MS, who are maintaining the semantic structure.

In order to make the semantic flow work in epSOS, the Master Value Sets Catalogue (MVC) has been developed to apply the structured fields in PS, eP and eD. MVC consists of entries with subsets of concepts coming from different international classifications. MVC will secure the semantic interoperability between the countries in epSOS. Thus it would not be necessary to translate everything to every local language in epSOS.

The MS will have to use the MVC / MTC (The Master Translation Catalogue) in a service running on NCP in country A before sending PS, eP or eD to country B, transforming locally used codes to epSOS codes.

The Master Translation Catalogue MTC will be used in Country A to transcode the locally used codes included in the MVC, and in Country B NCP service, when receiving a patient PS, eP or eD in order to translate from English (pivot format) to the local language in country B.

epSOS provides the pilots with tools for handling the mapping processes on a central server: the epSOS Central Reference Terminology Server (eCRTS), provided by CareCom through the Healthterm tool . The Single point of contacts will also be offered instruction for two members in each country in using the tool and its functionality. When the different mapping tables are done and qualified they must be downloaded from the central server to the NCP. Each country is responsible for the content in the mapping and translation tables on the central server and when the files are in place on NCP. It is important the individual country attach the right national experts to perform the mapping and translation in the workflows on the central server using the central services.

7.5.1 Transcoding and Mapping

There are two kinds of mappings to be done prior to making the final pilot run:

1. Concept to concept mapping between national used classifications and epSOS MVC

   Data registration in each country uses national or maybe international concepts and classifications. All these concepts must be mapped to the concepts in MVC before the connection tests of epSOS take place.
   This mapping might be “many to one”. Thus the patient registration can use much more codes and this many codes have to be compressed by matching a much less number of codes in MVC. The mapping will lose information, and it is not possible to map back.

National code	Map to epSOS Code
KCJ	54885008
KCJA	54885008
KCJ1C	54885008
KCJB	54885008
KCJ300	54885008
KCJB10	54885008
KCJ320	54885008
KCJB30	54885008
KCJ399	54885008
.....	.....

Figure 15: Mapping example of nationally used codes matching the same epSOS code

Countries using the same international classification may cooperate and divide the mapping task in order to reduce the work to be done. The mapping has to be done by experts and qualified.

2. Physical mapping from fields in national databases to fields in PS, eP and eD

   Before the “concept to concept” mapping can take place, the fields in the sources (national databases from where the data are registered) must be matched to fields in PS or eP – this is a kind of physical mapping every country has to do on their own. This physical mapping will be used for two purposes:

   i. To detect which local or national classification is used in the field
   ii. To fill in data in PS or eP when responding a request from a country B

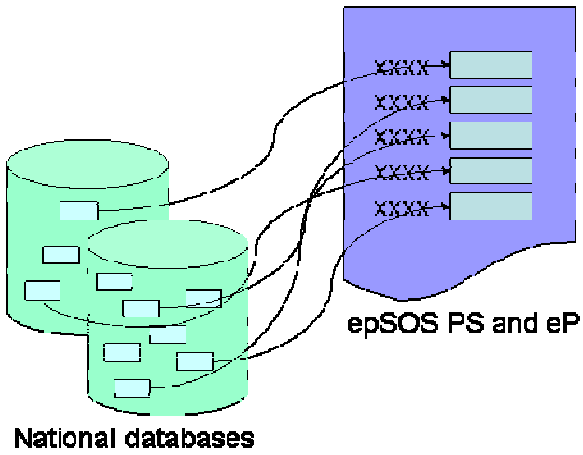


Figure 16: fields in the national databases mapped to fields in epSOS PS, eP and eD

This mapping will be teamwork between technical experts knowing the structure of the national databases from which the data are to be drawn and experts in coding on national level.

The Mapping allows to associate the sections/subsections of the Country A PS / eP/eD with the corresponding sections / subsections in the Pivot Document, based on CDA – PCC schema.

7.5.2 Translation

The MTC will be used for translating the epSOS codes from English (pivot format) to the language in country B. Non-codified data (like name and address) will not be translated. All countries in epSOS must translate codes in MVC to the language in their own country. The translation is included in the MTC of every specific Country. epSOS countries which are only acting as country A may not need to do a complete translation, because they do not receive data from foreign countries. The translation in MTC is used for displaying the concepts in country B.

There is no easy way to deal with the translation and it must be solid and correct. Therefore, it needs to be done by experts and reviewed by clinicians. The mapping tool can be used for managing the translation processes. However, in some cases, for the International standard coding system (e.g. ATC, ICD10) official translations in several languages are already available. In these cases, the official translation will be pre-loaded in the eCRTS.

Below is a Danish/Swedish example of the transcoding/translation process:

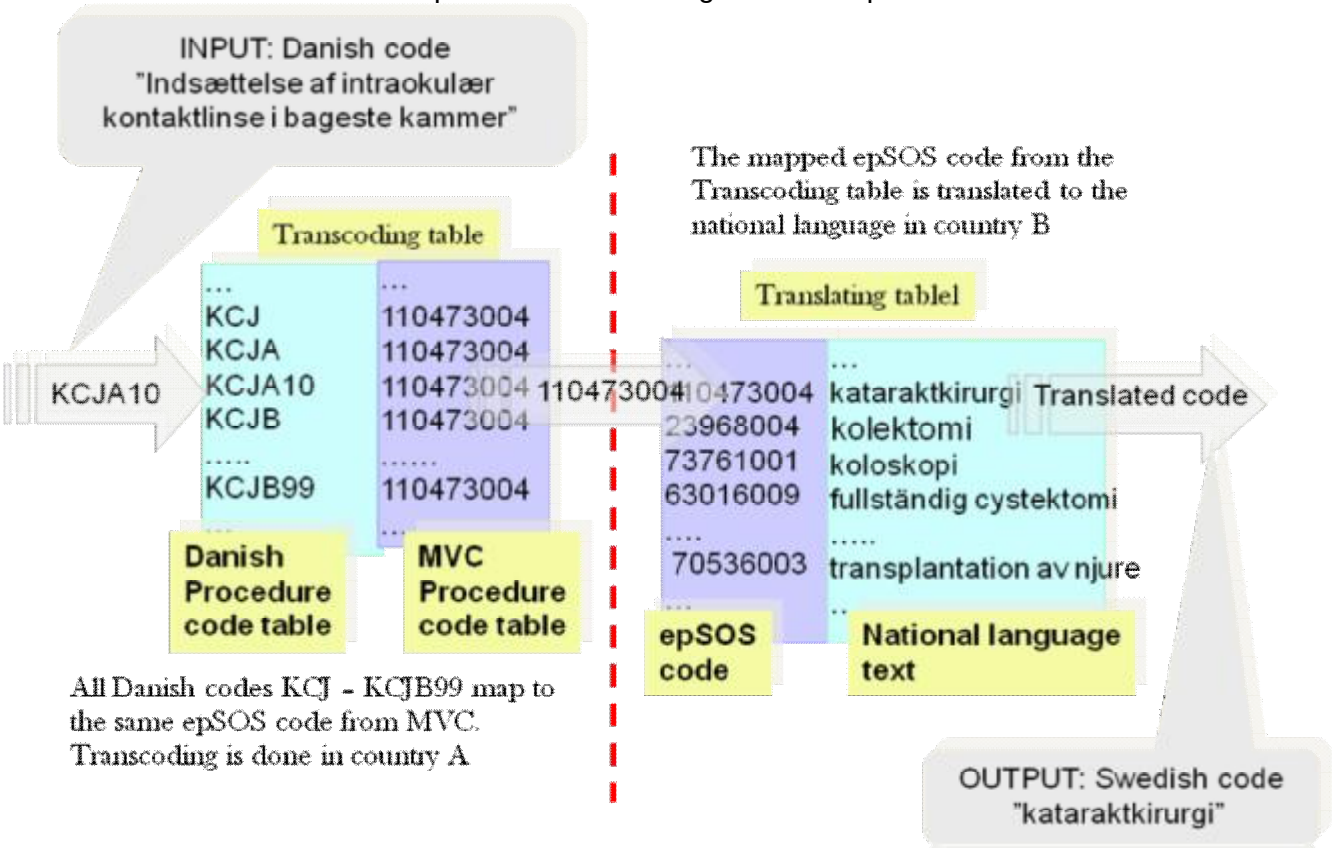


Figure 17 Danish/Swedish example of the transcoding/translation process

7.5.3 Semantic safety issues

- It is an agreement that the semantic transformation of the medicine is based on the active ingredients and not on brand name[24].
- When brand name substitution is of a product with a narrow therapeutic index and/or release, characteristics may be altered by a switch and patient safety considerations must be taken into account as alteration may result in either toxicity or under treatment.
- Differences in package size; the countries must be able to recognise or translate the original medicine independently of the Package size so it can be changed.
- If active ingredient, strength or pharmaceutical dose form of the medicine, as prescribed in country A, does not exist in country B, the medicine cannot be dispensed. Medicine can only be dispensed according to constitution of Country B.
- As a safeguard, the original prescription should be received by pharmacist in country B[25].
- Coding of information with currently available classification systems is strongly suggested to support semantic interoperability foreseen within the scope of the epSOS LSP.

7.5.4 MTC Maintenance

The activities related to MVC and MTC maintenance are describes in D3.9.1, Chapter 5.3.3. Additional material can also be found in the Appendix B1 and B2 of the same deliverable.

24 D3.1.2 Final definition of functional service requirements – ePrescription page 8

25 D3.1.2 Final definition of functional service requirements – ePrescription page 25

Some of the maintenance activities are triggered centrally, under the control of the epSOS Terminology Responsible.
Example of such category is:
• Align MVC to new version releases of the official code systems.
Activities centrally triggered, but managed by MS are:
• Align the epSOS MTC to the modified epSOS MVC.
Other activities are triggered by the MS, but managed centrally, such as:
• Add to the epSOS MVC the terms considered relevant by the MSs and the experts concerning the epSOS operation.
Finally some activities are triggered and managed by the MS, such as:
• Update the epSOS MTC with the necessary standard national changes.

The centrally managed maintenance activities require the supervision of the semantic expert team and the formal approval of the epSOS Terminology Responsible.
The activities managed by the MS have to be validated by the MS terminology Responsible, with the supervision of the epSOS Terminology Responsible.

It is highly advisable to exploit eCRTS and HealthTerm, to assure congruence and traceability of introduced changes.

8 Guidelines for epSOS pilot evaluation

8.1 Introduction: Scope and Intended Audience

Evaluation is an important part of the epSOS project in order to assess whether the epSOS infrastructure and pilot actually meet goals and expectations. Implementation and execution of the pilot is twofold for a large part as it takes place at NCPs and at the pilot sites in the MS. The evaluation must therefore to a considerable extent take place at NCP and pilot site level. Obviously the overall epSOS evaluation plan as thought out by the epSOS evaluation team needs to be contextualised, i.e. evaluation plans, designs, measurement tools and evaluation processes need to be adapted to the local context. This section is meant to provide guidelines for the implementation and execution of the local evaluation, thereby supporting (local) evaluators in performing their tasks at NCPs and MS pilot sites.

Scope
The guidelines address responsibilities and activities with regard to the set up of a local evaluation plan, the contextualisation and local evaluation process and the interaction with the central epSOS evaluation system and team. The guidelines support the local evaluation and ensure consistency, quality and timeliness of evaluation. They are also intended to mitigate the risks identified in D1.2.1: Chapter 6.

The guidelines are largely drawn from and refer to explicit and implicit requirements described in other epSOS documents and extended with recommendations. In particular 'WP1.2: overall epSOS evaluation' and 'WP4.2: site level preparation' have produced documents containing important requirements for evaluation.
Particularly important in this respect are the following documents:

- D1.2.1: Project evaluation methodology and plan;
- Pilot Project Initiation Document Template (a template provided by epSOS to the MSs as an aid for preparing the MS pilot also contains a section with evaluation guidelines);
- Short (3p.) document from WP1.3 providing the essential information about epSOS

Intended audience
It is important to realise that the guidelines address both NCP's and MS pilot sites. As they have different roles in the evaluation process different guidelines exist for NCPs and MS pilot sites. The guidelines for the NCPs may be further divided in guidelines for the 'country A role' (patient's home country) and the 'country B role' (guest country) as these are quite different. It is the responsibility of the SPOCs to decide which guidelines should be picked up by their NCP and pilot sites. Where appropriate we will indicate for whom the guidelines are meant, i.e. NCP or MS pilot site.

The guidelines can be divided in three categories:

- General guidelines, valid for both NCPs and pilot sites and meant to ensure consistency in evaluation;
- Contextualisation guidelines, for guiding the contextualisation of the local pilot evaluation;
- Interaction guidelines, about the interactions between the epSOS evaluation system and team and the local evaluation sites.

In the following sections guidelines for local evaluation are presented. They are related to the identified requirements and recommendations from other for epSOS material. The subdivision is based on the three types of guidelines, i.e. general, contextualisation and interaction guidelines.

8.2 General Guidelines

These guidelines are relevant for evaluators at both the NCP and pilot site level.

According to (D1.2.1; p.13) the activity of the epSOS services shall be monitored at all relevant levels, i.e. pilot sites, NCPs and flows of transaction between them. This means that several steps have to be taken at the NCP and pilot site level to devise of a local evaluation plan.

First an agreement on organisational responsibility needs to be arranged, i.e. an agreement on the (division of) responsibilities in the evaluation process at both NCP and pilot sites (D1.2.1 p.43). We recommend that a local evaluation team and/or local evaluation manager is appointed for each pilot site and NCP. A local instantiation of the overall evaluation model and evaluation plan needs to be produced by the local evaluation team (D1.2.1 p. 44). The local evaluation plan should be consistent with the evaluation guidelines described in 'Pilot Project Initiation Document Template'.
The plan should address the 'What, When, Where, Who and How' of the local evaluation i.e. it should contain the following elements:
Who & where:

- Who will be part of the evaluation;
    - § Patients, doctors & health care professionals, administrative/managerial personnel of health care provider, health care professional associations, health authorities);
    - § How they are involved and at which locations (pilot sites, points of contact).
  - o Who is responsible for the overall MS pilot evaluation.
  - o Who are responsible at the regional or local pilot sites and/or (clusters of) PoC.

When & where:

- When measurements/evaluation will take place and at which locations.

What:

- Which parts of the overall evaluation strategy will be covered, i.e. what will be measured.
- What instruments and materials will be used.

How:

- How the network of persons responsible for the local evaluation at pilot sites and (clusters of PoC) is organised;
- How fulfilment of responsibilities of the involved actors is monitored;
- How local evaluators will be briefed or will receive appropriate training for performing the evaluation;
- How consent from participating citizens will be verified;
- How testing of instruments and material will take place;
- How collecting, storing, aggregating and sharing of data is organised, e.g. what data is automatically collected from systems and how and by whom.

8.3 Contextualisation Guidelines

The measurement tools and procedures, e.g. questionnaires, need to be contextualised/adapted by the national/local evaluation team (D1.2.1 p. 48). Evaluation materials (questionnaires, procedures etc.) prepared by the epSOS evaluation team need to be translated and/or mapped onto the local context. To ensure timely availability the contextualisation needs to start as soon as epSOS level materials are final. Contextualised/adapted materials need to be tested, preferably with representatives from targeted group and feasibility of evaluation instruments in the context needs to be verified. Related to this pilot sites need to make sure that users and context have the right 'qualities', e.g. the right knowledge and/or experience level to handle the evaluation instruments such as questionnaires.

Participatory evaluation requires, by nature, the participation of those involved in the pilot (and other stakeholders), therefore the local evaluation team should have translated material ready (e.g. a flyer) to explain the epSOS project, the evaluation strategy and expected roles. As a basis the epSOS description developed in WP1.3 may be used. To ensure commitment and timeliness the required local participants and stakeholders should be identified and involved as early in the process as possible, to manage expectations and participation (e.g. organise an evaluation workshop with involved actors).

Specific contextualisation guidelines can be given for:

- Technical parameters
    - These will be available in a list distributed by epSOS (WP1.2 with WP3.9-.10) and the parameter labels will be translated in the local languages.
    - Local systems will assign their internal processes' indicators to the required epSOS indicators.
- Usage parameters/indicators
    - These will be contextualised around the selected dimensions following the guidelines of WP1.2.The contextualisation varies according to the typology of actors (agents vs. receivers (patients)), according to the process (dissemination activity, organisational activity, etc), according to the result, and according to the perception (ergonomy…) impact.
- Doctors
    - Guidelines for accessing its usual workstation when using epSOS
    - Guidelines for communicating with epSOS patients
    - Guidelines for evaluating their epSOS work
- Administrative staff

8.4 Interaction Guidelines

The pilot site or NCP evaluation managers should act as a contact person for the epSOS evaluation team. The Site/NCP evaluation manager needs to be focused on evaluating at least the minimum set of key-factors as identified by the epSOS evaluation team. The local evaluation manager may be involved in the analysis by epSOS evaluation team.

An agreement needs to be arranged on the way evaluation data is gathered, stored and shared between the epSOS evaluation team and local evaluation teams at NCP and pilot site level (D1.2.1. p. 51).

To support evaluation we further recommend that the epSOS evaluation team provides a 'help function' for the local evaluators.

9 Step-by-Step Description

This process describes what happens when a patient of Country A is asking for treatment in Country B - no matter if this is a hospital, a doctor's office or a pharmacy – and the HCP wants to access the regarding health data of the patient in Country A.
The following picture assumes that both participants are using an eID for identification, authentication and authorisation but the process itself will work with other methods too (see D3.6.2 for detailed descriptions of possible process flows and their variants).

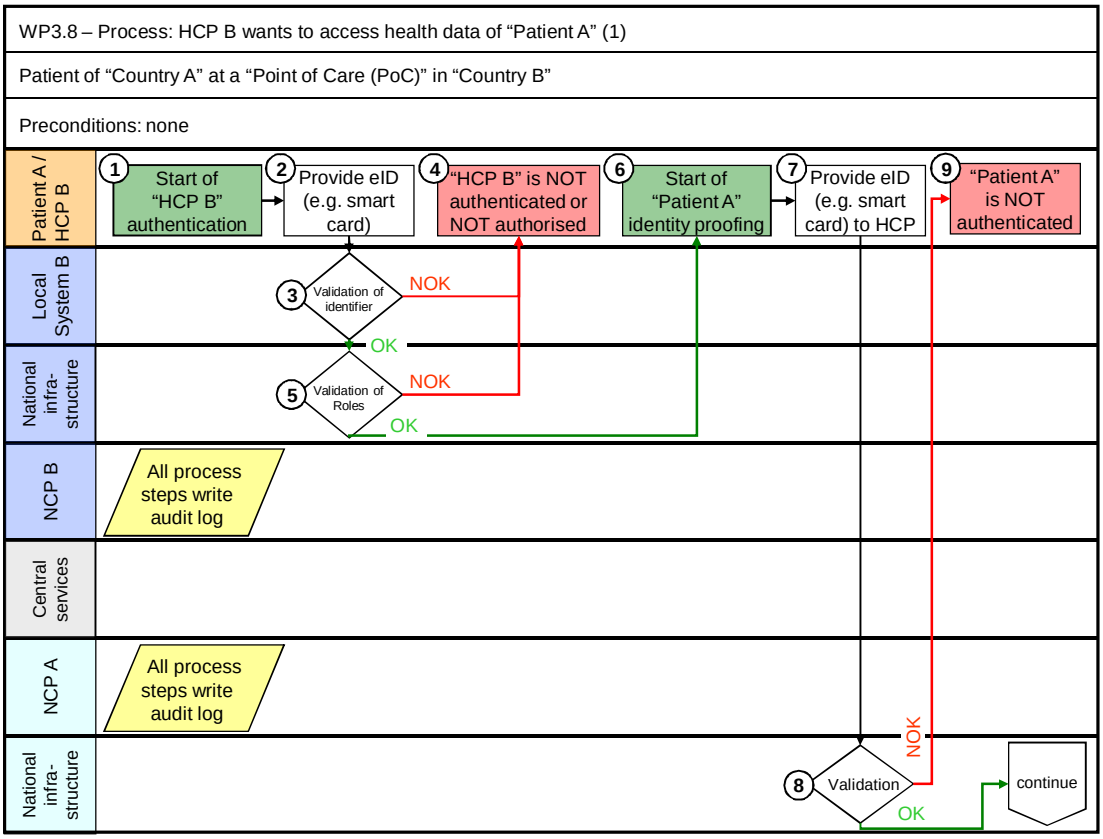


Figure 18: Simple Process of accessing health data of "Patient A" by "HCP B"

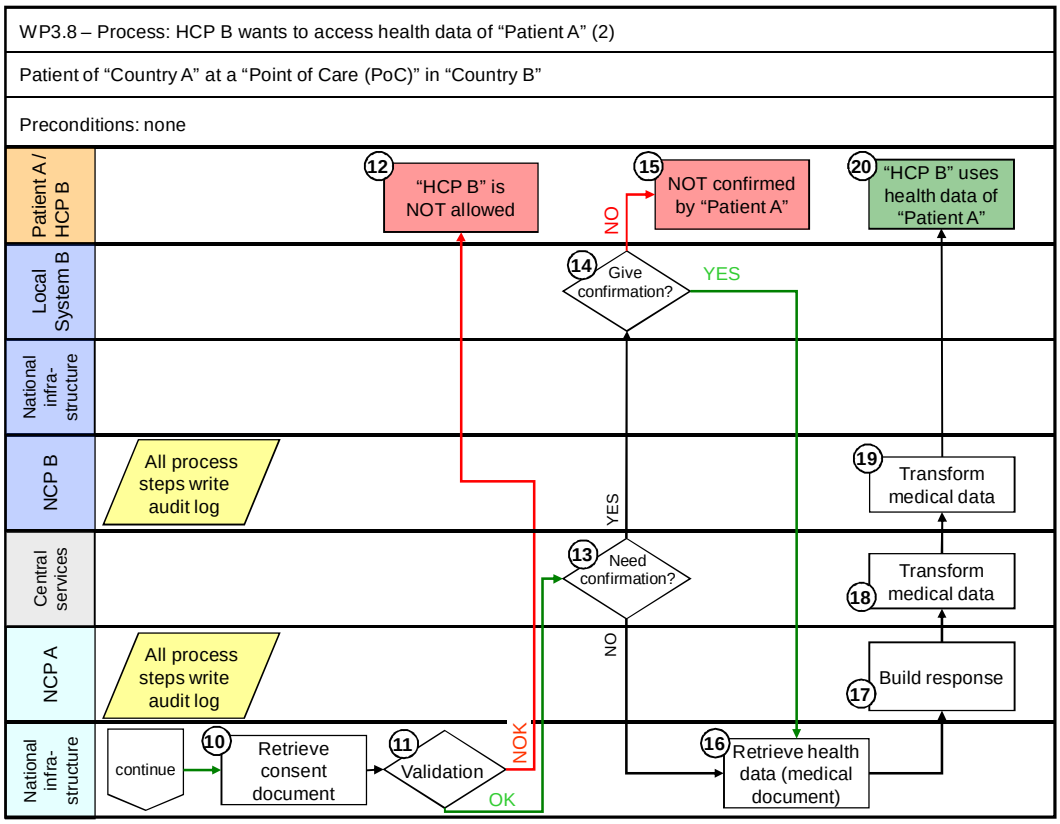


Figure 19: Simple Process of accessing health data of "Patient A" by "HCP B" (cont.)

The process in the above shown flow diagram (figures 1 and 2) consists of the following steps:

1. A patient of Country A wants to have a treatment or a dispensation in Country B and the consulted HCP needs/wants to access patient health data in the country of affiliation. The process starts with an identification, authentication and authorisation of the HCP B for epSOS (if this was not done before).

   Definitions of key roles and functions according to an information security policy ensure that the authentication process is done in accordance with FWA and national legislation. Authentication is a process to verify the claimed identity of a party before authorising a particular action to be performed. Authorisation Process is a process by which entitlement of a requestor, to access or use a given service is determined, for example the dispenser is a person legally authorised to dispense medicinal products. The identification and authentication process in country B is influenced by country B legislation standards and is the responsibility of each MS[26].

2. HCP B owns a unique identifier (e.g. located on a (smart) card electronically readable or a human readable one) and provides it for identification and authentication purposes.

   Note: Every other method for identification, authentication and authorisation of a HCP B (e.g. username/password) will fit into this process too. Legal aspects in Country B are important for choosing an appropriate method.

3. The provided unique identifier of HCP B is checked by the local system.

   One of the following results is returned:

   a. HCP's eID is authenticated by the local system (continue with step 5) or

   b. HCP's eID is not authenticated by the local system.

[26] D 3.6 Identity Management page 32

Note: This step is for guardian reasons only. Usually the HCP should be already identified and authenticated by the local system.

4. If the HCP B is either not authenticated by the local system or not authorised by the national infrastructure an appropriate message is returned and the process is finished.
5. The national infrastructure selects the actual role of the HCP B as part of the provided identifier. The actual role is checked against the predefined roles for epSOS LSP.

   One of the following results is returned:

   a. HCP's actual role is authorised to use the epSOS LSP environment or
   b. HCP's actual role is not authorised for using the epSOS LSP environment (go to step 4).
6. This is the start of the identification and authentication process of Patient A.
7. Patient A possesses a unique identifier (e.g. eID located on a smart card) and provides it to the HCP B for the identification and authentication process in epSOS LSP. The local system transmits this identifier information via NCP B and NCP A to the national infrastructure of County A.
8. The transferred unique identifier of the patient - together with some information about the requesting HCP B - is getting validated by the verification/validation service in Country A.

   One of the following results is returned:

   a. Patient A is authenticated by Country A (continue with step 10) or
   b. Patient A is not authenticated by Country A or
   c. HCP B's actual role is authorised by County A (continue with step 10) or
   d. HCP B's actual role is not authorised by Country A or
   e. If the received value for HCP B's "Level of trust" is equal to or higher than the defined minimum in Country A (continue with step 10) or
   f. The received value for HCP B's "Level of trust" is below the defined minimum in Country A.

   What the patient needs to do is to identify himself at the PoC. The HCP has to check if this identification is valid or not through his Dispense provider before accessing any data. In order to avoid legal issues, it is imperative that the patient is univocally identified so that patient identity can be ensured. The national authorities must run identity registers and provide necessary information to authorised epSOS actors participating in the project. The approved methods for patients identification are described by WP3.6 'Identity Management" as three valid processes of patient identification and authentication mechanism of Country A, of which one must be installed and maintained by participating MS;

   • With a unique identifier

   • With demographic data

   • Via internet portal.
9. An appropriate message is returned and the process is finished.
10. The request for Patient A's health data is handed over to the national infrastructure of Country A.
11. The infrastructure of Country A checks this request against the actual status of Patient A's consent.

    One of the following results is returned:

    a. Patient A has given consent for Country B (continue with step 13) or

b. Patient A has not given consent for Country B or

c. HCP B's actual role and the HCP B's level of trust is authorised by County A (continue with step 13) or

d. HCP B's actual role or the HCP B's level of trust is not authorised by Country A

Note: This is a simplified description of the process, not a guideline for programmers.

12. An appropriate message is returned and the process is finished.
13. The Central Services layer receives a request and selects the confirmation flag for Country A.
14. If Patient A must not give a confirmation, the process continues with step 16. If confirmation is necessary, it has to be given explicitly. The patient has to say "Yes" (HCP will tick a box and patient will confirm it). Before any information is going to be presented, the patients freely given, informed and specific information must be given. Patient identification is needed in two cases when consent is needed ;
    - When the patient needs a health service and visits a HCP in country B.
    - When the patient wants to check who accessed his health data (must be done through health administrator in country A).
15. If the confirmation was not positive the HCP will not have any access to patient's health data and the process is finished.
16. The national infrastructure in Country A retrieves the health data (medical information) from the national repository and sends it to NCP A.
17. NCP A builds the response to the original request of Country B for health data (medical information) and sends it to the Central Services. (Central Service is here understood as what happens in central Semantics and in the Semantic component (Transformer component) in the NCP)
18. The Central Services layer transforms the received data into a predefined pivot format of the epSOS LSP.
19. NCP B transforms the received data into a local format and transmits the response to the local system of HCP B.

HCP B uses the health data (medical information) of Patient A at PoC in Country B – the process is finished.

10 GLOSSARY

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.

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

Change Management in a support organisation aims to ensure that standardised methods and procedures are used for efficient handling of all changes in the technical set up, in the organisational set up or in practical matters in a MS.

Confidentiality has been defined as "ensuring that information is accessible only to those authorised to have access"

Configuration Management holds controls and issues information on all configuration items (CIs) and their components necessary for installing and operating an IT system.

Configuration Management DataBase (CMDB) hold the structured information on these CIs in terms of their attributes with value, their interrelationships etc.

Country A is the MS 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 MS 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 authorised 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 organisations 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 fulfil 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 MSs 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 organisational 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 fulfil 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 fulfil 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, authorised to provide health care services, unequivocally identified in the set of the Health Care Institutions” (epSOS D3.2.1)]

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

“Incident” is in Incident Management” any event which is not part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service.

Incident Management is to restore or to organise restoring of normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.

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.

Integrity is to be understood as data must not unauthorised be changed, distorted or destroyed

Legal entity is an individual or organisation 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 organisation 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.

Problem management is to find and resolve the root cause of a problem and prevention of incidents

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, organisation, 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 meet. 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.

Service Level Management is to list the epSOS Service Levels defined by the epSOS Consortium and to report on MSs Service Levels

Single Point of Contact (SPOC) MS's single point of contact for epSOS (MS SPOC):

- Acts as the single responsible point for communication epSOS-to-MS and MS-to-epSOS for all matters concerning the piloting activities of the MS.
- Can be an organisation or a person.
- Different aspects (organisational, legal, technical and clinical) can be covered by different persons/orgs.

Traceability means that any data access or attempt to access medical data through the epSOS LSP services must be fully transparent, traceable and reproducible e.g. by logging of "who" accessed, "which" medical data from "where" at "what" time under "whose" authority.

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.

11 ABBREVIATIONS

CA	Certificate Authority
CAB	Change Advisory Board
CC	Competence Centres
CDA-PCC	Clinical Document Architecture – Patient Care Coordination
CI	Configuration Items
CMDB	Configuration management Database
ConfigM	Configuration management
CoT	Circle of Trust
DP	Data Protection Authority
DPA	Data Protection Authorities
DPD	Data Protection Directive
D.x.y.z	Deliverable from WPx.y
ECJ	European Court of Justice
eCRTS	epSOS Central Reference Terminology Server
eD	Electronic Dispensation
EHR	Electronic Health Records
eP	Electronic Prescription
epSOS	Smart Open Services for European Patients
EU	European Union
F2F	Face to face meeting
FET	Fraunhofer/Elga/Tiani Spirit
FR	Functional Requirement
FWA	Legal Framework Agreement
GP	General Practitioner
HW	Hardware
HC	Health Care
HCO	Health Care Organisation
HCP(O)	Health Care Professional Organisation
ICT	Information and Communication Technology
ID	Identity
IPSec	Internet Protocol Security
ISMS	Information Security Managed System
IT	Information Technology
JWG	Joint Working Group WP3.8/3.9
LSP	Large Scale Pilot
MoU	Memorandum of Understanding
MS	Member State
MTC	Master Translation/Transcoding Catalogue
MVC	Master Value Sets Catalogue
NAB	National Authority Beneficiary
NCP	National Contact Point
NCP-A	National Contact Point in country A
NCP-B	National Contact Point in country B
NDA	Non-disclosure Agreements
PAT	Project-a-thon
PD3	Project Domain 3
PKI	Public Key Infrastructure
PoC	Point of Care
PR	Public Relations
PS	Patient Summary

PSB	Project Steering Board
QA	Quality Assurance
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Security Policy
SPOC	Single Point of Contact
SSL	Security Socket Layer
SW	Software
TPM	Technical Project Management
UPS	Uninterruptible Power Supply
WG	Working Group
WP	Work Package

12 LIST OF FIGURES

Figure 1: Milestones 11
Figure 2: Deliverables 11
Figure 3: Bird's perspective 12
Figure 4: Structure of the document 12
Figure 5: Required inputs from other epSOS WP 14
Figure 6: Outputs to other WPs 14
Figure 7: Time schedule D3.8.1 17
Figure 8: Time schedule D3.8.1 17
Figure 9: Conceptual Architecture of epSOS NCP Gateway 20
Figure 10: F.E.T. Design for NCP-A common components 22
Figure 11: F.E.T. Design for NCP-B common components 23
Figure 12: Virtual Central Service - proposed solution 28
Figure 13: Levels of Agreements 32
Figure 14: Communication structures 63
Figure 15: Mapping example of nationally used codes matching the same epSOS code 65
Figure 16: fields in the national databases mapped to fields in epSOS PS, eP and eD 1
Figure 17 Danish/Swedish example of the transcoding/translation process 66
Figure 18: Simple Process of accessing health data of "Patient A" by "HCP B" 71
Figure 19: Simple Process of accessing health data of "Patient A" by "HCP B" (cont.) 72
Figure 20: Danish Data Sources and Integrations Overview 98
Figure 21: Security Setup & Audit Traceability for NCP-A 99
Figure 22: Distributed and Central DB 100
Figure 23: Clinical Information Index 101
Figure 24: Spanish NCP Integration Architecture 101

13 Annex I: Security

This annex consists of three documents. The first is the NCP Security Policy which can now be found on ProjectPlace (https://service.projectplace.com/pp/pp.cgi/r492884389). The second, called NCP BSP details-compact.pdf can be found in the D3.8.2 folder on ProjectPlace (or by using this link: https://service.projectplace.com/pp/pp.cgi/r495440632) and the third is the security ncp bsp checklist.xls which can be found in the D3.8.2 folder on ProjectPlace (or by using this link: https://service.projectplace.com/pp/pp.cgi/r492869378).

14 Annex II: Sequential Implementation Guidelines

The sequential implementation guidelines are to be used by the member states in their implementation procedures. This is only a *sequential* addition to the main checklist with requirements and recommendations.

ID	Recommended steps for Technical implementation:	Start time	End time	OK	Open points	Remarks
1	Understand epSOS business use cases					
2	Understand epSOS architecture					
3	Analyse NCP-In-A-Box for national use					
4	Study epSOS Guidelines and epSOS Deliverables (WP3.1 - WP3.10)					
5	If the NCP-In-A-Box is to be used and a country is piloting as country A, understand National Connector for NCP A in your country Carefully study National Interface and integratebility with National / Regional Infrastructure					
6	If NCP-In-A-Box is to be used and a country is piloting as country B, understand National Connector for NCP B in your country					
7	Understand Portal Adapter and portal for NCP B if used in your country. Carefully study National Interface and integrability with National / Regional Infrastructure.					
8	If NCP-In-A-Box is used by a country piloting as country B and if a portal is used, understand Portal Adapter (National Interface) and portal for PoC interconnection.					
9	Describe National Infrastructure with the purpose of interfacing. Data sources, Data Structures and Dataflow (eP, eD and PS) to the NCP (both as NCP-In-A-Box and MS developed NCP)					
10	If using FET common components (NCP in a box): Describe the need for interfacing in your country.					
11	If developing the NCP describe your needed components for the NCP in your country					
12	If using Portal in a country B:					

	Describe how to use Portal to be sure of all data are available.					
13	Study Technical Security solution in your country according to epSOS rules and set ups (see security checklist) and apply it.					
14	Study how you can fulfil the technical solution for epSOS semantic service (perhaps perform a gap analysis) and apply it.					
15	Specify and develop the function to transform MS documents into the epSOS CDA (PDF), as input to NCP-In-A-Box (FET solution).					
16	Study and describe how your MS can use and comply with the functions in Central Services					
17	Synthesise Requirement Specification for your country from your descriptions, epSOS Guidelines and epSOS deliverables (WP3.1 – WP3.10)					
18	If appropriate, use the Requirement Specification for design and development, according to usual procedures in your country. As part of the epSOS you can use all epSOS documents					
19	If NAB/authorities in your country decide to perform call it can be Call for Information or Call for Tender (externally). In both cases you must follow the legal rules in your country for the calls. Use the Requirement Specification for your Call. You can use all released epSOS document in calls.					
20	Test of developed NCP/Interface components (i.e. National Connector) MUST be performed according to epSOS test rules. This complies to component test, system test, participating in Projectathon and field test. Descriptions in Guidelines and epSOS document are available					
21	Start of Piloting is according to epSOS decisions.					
	Recommended steps for understanding and implementing legal aspects:					
22	Appoint legal experts for epSOS-relationships in your country					
23	Understand NCP from a legal point					

	of view. Read 2.1.2. Study Frame Work Agreement (FWA). Understand Clinical aspects (Chapter 5.2). Understand National and European Rules (Chapter 5.3). Understand the Liability structure (Chapter 5.4).					
24	Localise FWA in your national language. Include national legal and professional requirements in the localised version of FWA.					
25	Form combined agreements with Pilot-sites, PoC, NAB, SPOC etc., according to FWA					
26	Explain in English the localised agreements and the agreement structure in your country.					
27	Agreements in MS must be signed for creating the necessary framework of the trusted domain (see signing of FWA in chap. 5.1.1.3). The signed agreements will be held locally in each MS.					
28	Set up the process and procedures to extend consent to export patient data abroad.					
29	Prepare the documents and the procedure to define the consent document (in Country A language and all Country Bs languages (or at least in English) to train HCP-B					
	Recommended Organisational steps:					
30	Decide if the national NCP organisation should be a recognisable part of the national ICT organisation in the country or it should be self-contained with necessary cooperating with the national ICT organisation					
31	Decide if the NCP organisation (or part of it) should be outsourced in your country					
32	Organise needed staff for setting up NCP organisation, staff for operating the NCP and for maintaining the NCP					
33	Make sure that the necessary organisational connections between units in your MS is in place (SPOC, Pilot-sites, PoC, HCP, HCPO, NAB i.e.)					
34	Set-up Service Level Agreements (SLA) for the NCP-organisation					

	and for operating NCP. Note the epSOS SLA- level in chapter 6.2.1.4 Needed contracts with companies running NCP or parts of it, if applicable.					
35	Agreement with data processor should be signed.					
36	Organise Service Desk for the NCP-organisation in MS. The Service Desk should handle epSOS calls from other epSOS countries as well as calls from epSOS Pilot-sites in the country.					
37	Make sure, that other Processes (ITIL), needed for operating epSOS is in place in the country. (Chap. 6.2.1)					
38	Insure that Technical, Organisational and Practical measures comply to required Security standard for epSOS and that it is documented. Go thought the Security-checklist for making sure, that all needed security is in place. (needed for auditing)					
39	Prepare documents for Auditing security according to epSOS security to be sent to PSB. (MS should perform auditing themselves and declare compatibility to epSOS standards					
40	Appoint or contract skilled (certified) auditors.					
41	Perform Security Auditing according to epSOS rules and time schedule.					
	Recommended steps in implementing Practical Issues					
42	Organise and set-up the epSOS communication structure for the country. See chapter 7.4 in Guidelines.					
43	Contact external partners in MS: Pilot sites, GPs Pharmacies, Hospitals, relevant authorities and others as patient associations, by sending epSOS information with invitation to plenum meeting about epSOS. epSOS web-site should be included in the information documents.					
44	Perform one or two information meetings dependent of the					

	situation in the country.					
45	Setting up the Master ValueSet Catalogue (MVC) and the Master Translation/Transcoding Catalogue (MTC) is a major task for the MS. epSOS cannot be running in a MS without those catalogues. Staff must be appointed, trained and the catalogue work started early in time.					
46	If needed in the country, define and sign the Contract for HealthTerm support					
47	Make sure that all practicalities for running the NCP is in place (read chapter 7.1.1). Refer to Organisational steps. Use the “Requirement and Recommendations Checklist”					
48	Organise production of manuals for epSOS procedures at the different epSOS sites.					
49	Ensure that all equipment for the NCP is in place (insourced or outsourced)					
50	Ensure that servers and server rooms are secure and maintaining is sufficiently prepared					
51	Training of staff must be planed and performed or contracted, dependent of the situation in the country.					
52	Non disclosure agreements for system administrators must be in place.					
53	After primary information meetings the marketing activities is needed in relation to the situation in MS. Public information policy is important to make sure that the citizens and patients are informed about epSOS - dependent of the situation in your country. Define your Country citizens information procedures (through institutional and or Media channels) Define other Countries citizens information procedures (through institutional and or Media channels)					
	Steps in implementing epSOS					

	evaluation:					
54	Appoint local evaluation teams for pilot sites and for the NCP organisation (Managers for the teams should also be appointed, - of course dependent of the situation in the country). Describe the evaluation in the MS to inform WP1.2.					
55	Training of evaluation teams carried out by WP1.2.					
56	The generic evaluation plan for the evaluation in MS should be localised (depending of the service evaluated). See chapter 8.2 in Guidelines					
57	Contextualisation/adaption of the measurements tools should be done as soon as the material has been released by the Evolution Team in epSOS (WP 1.2)					
58	The online tools build with the localisation and translation feedback of the countries, will be validated by the local evaluation team.					
59	Baseline visit organised in cooperation with WP1.2 and WP4.2.					
60	Evaluation performed by WP1.2 together with the local (MS) evaluation organisation according to rules from the epSOS Evaluation Team, WP 1.2					

Annex III: Danish example (per 15 July 2010) of using the Sequential Implementation Guidelines

The Danish example is based on the first version of the sequential guidelines. Therefore, the steps are slightly different from the now recommended sequential guidelines.
This is preliminary and can be subject to changes along the way.

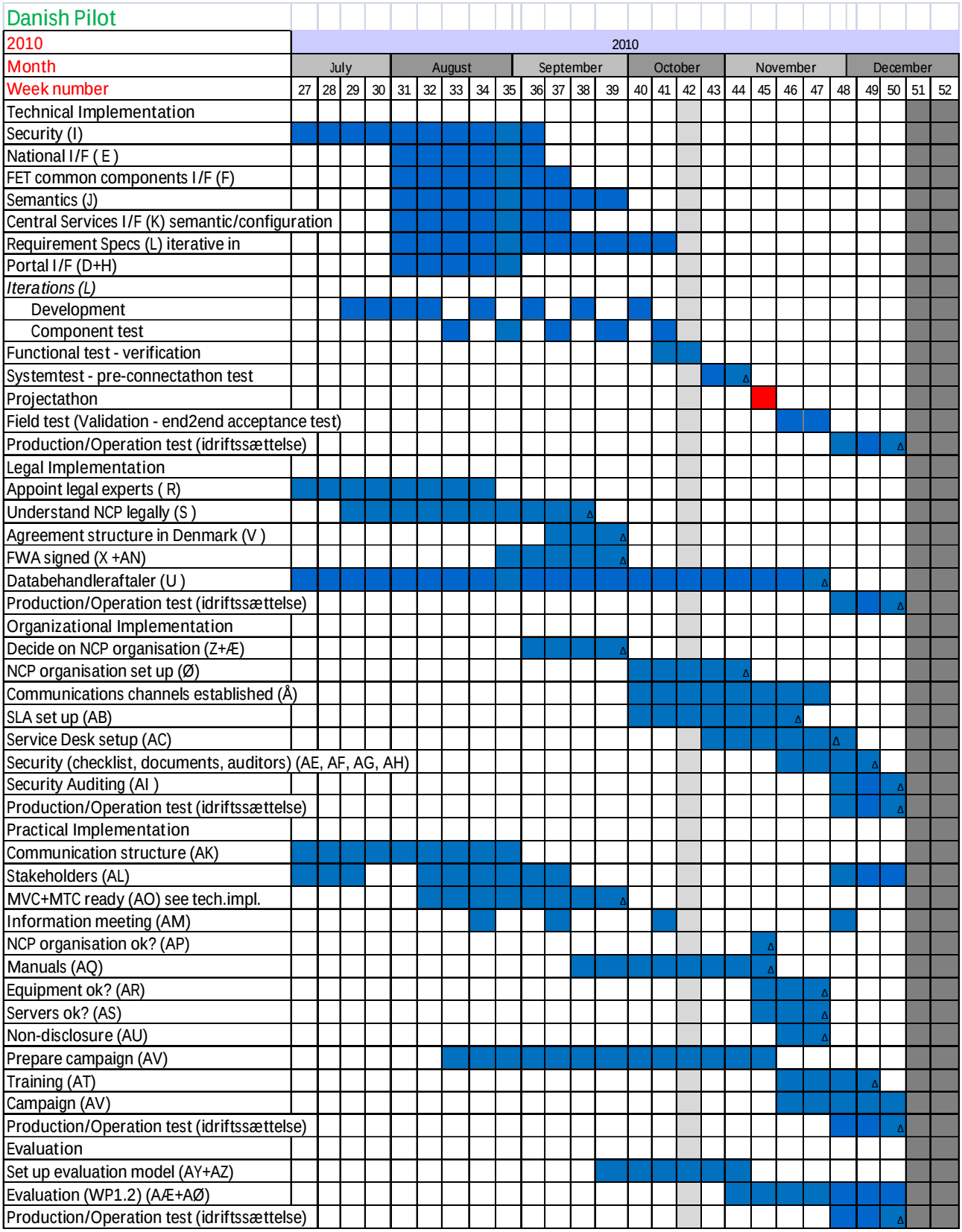
No.	Recommended steps for Technical implementation:	Start time	End time	OK	Open points	Remarks
A	Understand epSOS architecture			√		
B	Understand National Connector for NCP A in your country			√		
C	Understand National Connector for NCP B in your country			√		
D	Understand Portal Adapter and portal for NCP B if used in your country		03.09			
E	Describe National Infrastructure with the purpose of interfacing. Data sources and Dataflow (eP, eD and PS)		10.09			
F	If using FET common components (NCP in a box): Describe the need for interfacing in your country.		17.09			
G	If developing the NCP describe your needed components for the NCP in your country		N/A			
H	If using Portal in a country B: Describe how to use Portal to be sure of all data are available.		03.09			
I	Study and apply Technical Security solution in your country according to epSOS rules and set ups.		10.09			
J	Study and apply how you can fulfil the technical solution for epSOS semantic service		01.10			
K	Study and describe how your MS can fulfil the functions in Central Services		17.09			
L	Synthesise Requirement Specification for your country from your descriptions, epSOS Guidelines and epSOS deliverances (WP 3.1 – WP 3.9)		15.10			An iterative development process is run in Denmark
M	If NAB/authorities in your country decide to develop the NCP or NCP interfacing yourself (internally): Use the Requirement Specification for design and development, according to usual procedures in your country. As part of the epSOS you can use all epSOS documents		N/A			

N	If NAB/authorities in your country decide to perform call it can be Call for Information or Call for Tender (externally). In both cases you must follow the legal rules in your country for the calls. Use the Requirement Specification for your Call. You can use all released epSOS document in calls.		N/A			
O	Test of developed NCP/Interface components (i.e. National Connector) MUST be performed according to epSOS test rules. This complies to component test, system test, participating in Projectathon and field test. Descriptions in Guidelines and epSOS document are available		05.11 26.11 17.12			Iterative development resp. System field production test
P	Start of Piloting is according to decisions in WP 4.2		01.01 2011			
Q	**Recommended steps for understanding and implementing legal aspects:**					
R	Appoint legal experts for epSOS-relationships in your country.		27.08			
S	Understand NCP from a legal point of view. Read 2.1.2. Study Frame Work Agreement (FWA). Understand Clinical aspects (Chapter 5.2). Understand National and European Rules (Chapter 5.3). Understand the Labiality structure (Chapter 5.3.		24.09			
T	Localise FWA in your national language. Include national legal and professional requirements in the localized version of FWA.		N/A			Expect to keep the English version
U	Form combined agreements with Pilot-sites, PoC, NAB, SPOC etc., according to FWA		26.11			Data processor agreements with data controller (SST+LMS)
V	Explain in English the localised agreements and the agreement structure in your country.		01.10			Does epSOS have a deadline?
X	Agreements in MS must be signed for creating the necessary framework of the trusted domain (see signing of FWA in chap. 5.1.1.3). The signed agreements will be held locally in each MS.		30.09			
Y	**Recommended Organisational steps:**					
Z	Decide if the national NCP organisation should be a		01.10			

	recognisable part of the national ICT organisation in the country or it should be self-contained with necessary cooperating with the national ICT organisation					
Æ	Decide if the NCP organisation (or part of it) should be outsourced in your country		As above			
Ø	Organise needed staff for setting up NCP organisation, staff for operating the NCP and for maintaining the NCP	01.10	05.11			
Å	Make sure that the necessary organisational connections between units in your MS is in place (SPOC, Pilot-sites, PoC, HCP, HCPO, NAB i.e.)		26.11			
AB	Set-up Service Level Agreements (SLA) for the NCP-organisation and for operating NCP. Note the epSOS SLA- level in chapter 6.2.1.4.1.1. Needed contracts with companies running NCP or parts of it, if applicable.		19.11			
AC	Organise Service Desk for the NCP-organisation in MS. The Service Desk should handle epSOS calls from other epSOS countries as well as calls from epSOS Pilot-sites in the country.		03.12			
AD	Make sure, that other Processed (ITIL), needed for operating epSOS is in place in the country. (Chap. 6.2.1)					
AE	Insure that Technical, Organisational and Practical measures comply to required Security standard for epSOS and that it is documented. Go thought the Security-checklist for making sure, that all needed security is in place. (needed for auditing)		10.12			
AF	Prepare documents for Auditing security according to epSOS security to be sent to PSB. (MS should perform auditing themselves and declare compatibility to epSOS standards		10.12			
AH	Appoint skilled (certified) auditors in the country, if they are not already part of national organisation in MS. If necessary contracts with external must be		10.12			

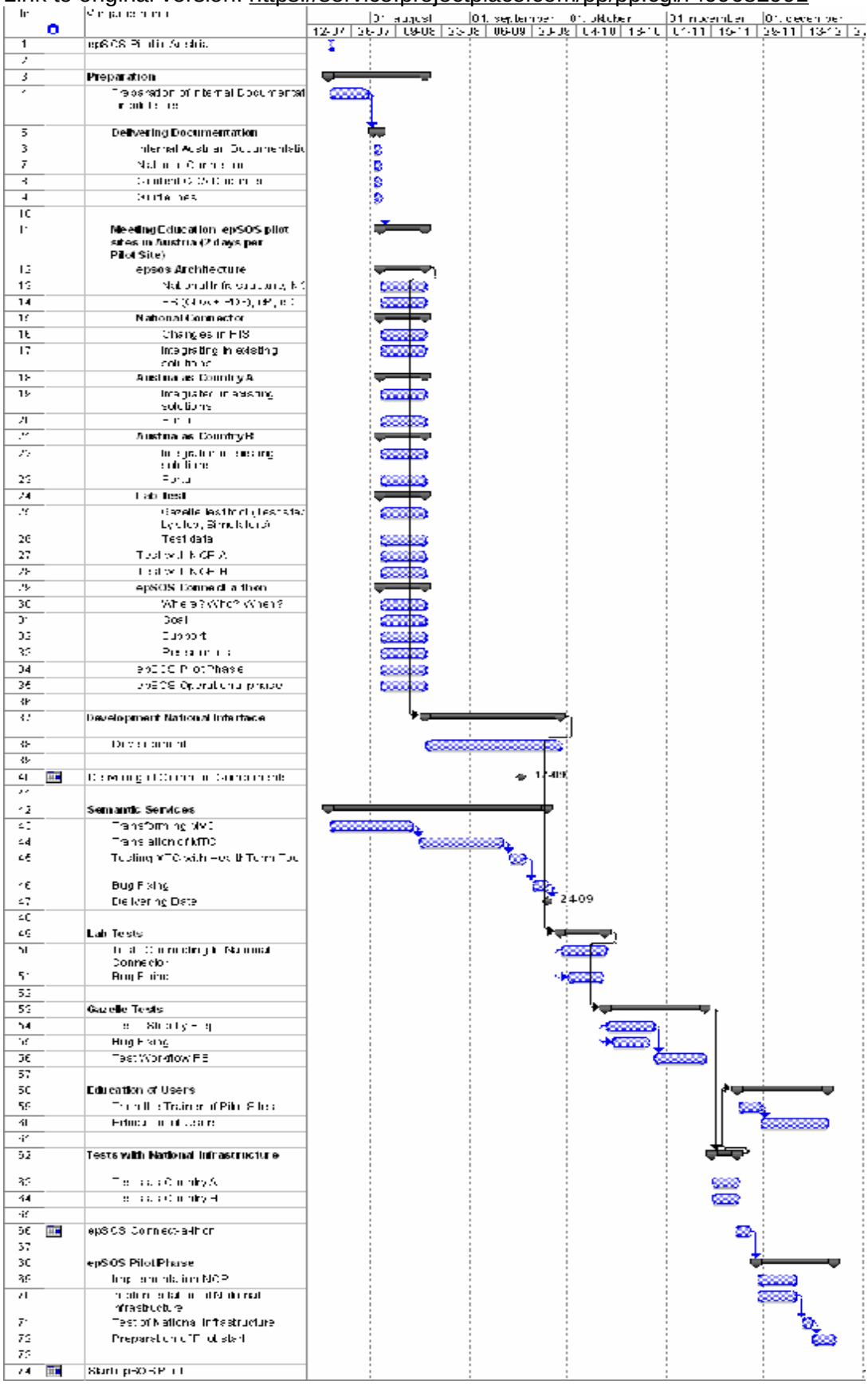
	signed.					
AI	Perform Security Auditing according to epSOS rules and time schedule.		17.12			
AJ	**Recommended steps in implementing Practical Issues**					
AK	Organise and set-up the epSOS communication structure for the country. See chapter 7.4 in Guidelines.		03.09			
AL	Contact external partners in MS: Pilot sites, GPs Pharmacies, Hospitals, relevant authorities and others as patient associations, by sending epSOS information with invitation to plenum meeting about epSOS. epSOS web-site should be included in the information documents.		ongoing through the epSOS project			
AM	Perform one or two information meetings dependent of the situation in the country.		week 34 + 37 + 41+48			
AO	Setting op the Master ValueSet Catalogue (MVC) and the Master Translation/Transcoding Catalogue (MTC) is a major task for the MS. epSOS cannot be running in a MS without those catalogues. Staff must be appointed, trained and the catalogue work started early in time.		01.10			
AP	Make sure that all practicalities for running the NCP is in place (read chapter 7.1.1). Refer to Organisational steps. Use the “Requirement and Recommendations Checklist”		12.11			
AQ	Organise production of manuals for epSOS procedures at the different epSOS sites.		12.11			
AR	Be sure that all equipment for the NCP is in place (insourced or outsourced)		26.11			
AS	Ensure that servers and server rooms are secure and maintaining is sufficiently prepared		26.11			
AT	Training of staff must be planed and performed or contracted, dependent of the situation in the country.		10.12			Pharmacies and doctors just before operation
AU	Non disclosure agreements for system administrators must be in place.		26.11			
AV	After primary information meetings	16.08	12.11			

	the marketing activities is needed in relation to the situation in MS. Public information policy is important to make sure that the citizens and patients are informed about epSOS - dependent of the situation in your country					
AX	**Steps in implementing epSOS evaluation:**					
AY	Appoint local evaluation teams for pilot sites and for the NCP organisation (Managers for the teams should also be appointed, - of course dependent of the situation in the country). Describe the evaluation in the MS to inform WP1.2.		05.11			
AZ	Written local model or plan for the evolution in MS (See chapter 8.2 in Guidelines)		05.11			
AÆ	Contextualisation/adaption of the measurements tools should be done as soon as the material has been released by the Evolution Team in epSOS (WP 1.2)		17.12			
AØ	Evaluation performed by the local (MS) evaluation organisation according to rules from the epSOS Evaluation Team, WP 1.2		17.12			

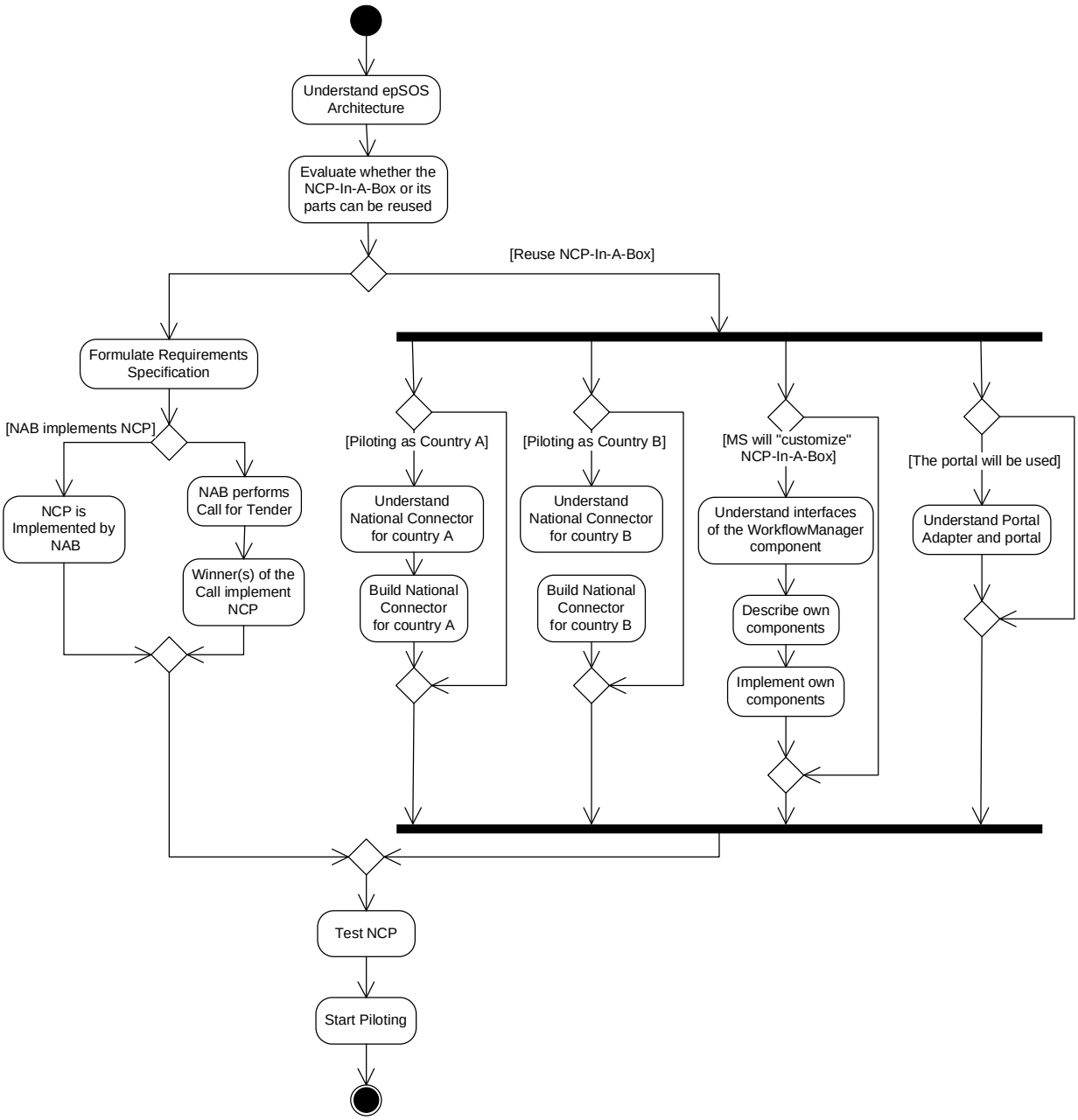

Danish Pilot
2010
2010
Month
July
August
September
October
November
December
Week number
27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Technical Implementation
Security (I)
National I/F (E)
FET common components I/F (F)
Semantics (J)
Central Services I/F (K) semantic/configuration
Requirement Specs (L) iterative in
Portal I/F (D+H)
Iterations (L)
Development
Component test
Functional test - verification
Systemtest - pre-connectathon test
Projectathon
Field test (Validation - end2end acceptance test)
Production/Operation test (idriftssættelse)
Legal Implementation
Appoint legal experts (R)
Understand NCP legally (S)
Agreement structure in Denmark (V)
FWA signed (X +AN)
Databehandleraftaler (U)
Production/Operation test (idriftssættelse)
Organizational Implementation
Decide on NCP organisation (Z+Æ)
NCP organisation set up (Ø)
Communications channels established (Å)
SLA set up (AB)
Service Desk setup (AC)
Security (checklist, documents, auditors) (AE, AF, AG, AH)
Security Auditing (AI)
Production/Operation test (idriftssættelse)
Practical Implementation
Communication structure (AK)
Stakeholders (AL)
MVC+MTC ready (AO) see tech.impl.
Information meeting (AM)
NCP organisation ok? (AP)
Manuals (AQ)
Equipment ok? (AR)
Servers ok? (AS)
Non-disclosure (AU)
Prepare campaign (AV)
Training (AT)
Campaign (AV)
Production/Operation test (idriftssættelse)
Evaluation
Set up evaluation model (AY+AZ)
Evaluation (WP1.2) (AÆ+AØ)
Production/Operation test (idriftssættelse)

15 Annex IV: Austrian Example

Link to original version: https://service.projectplace.com/pp/pp.cgi/r499682991



16 Annex V: Visualisation of the Sequential Implementation Guidelines



17 Annex VI: Requirements and Recommendations - checklist

The checklist for requirements and recommendations is a living document which should only be used digitally. Therefore, you can find it via this link:

https://service.projectplace.com/pp/pp.cgi/r511702212

18 Annex VII: NCP Customisation

18.1 Danish NCP Example

Provided here, courtesy of Danish epSOS pilot project, is a integrations overview showing the three main Danish data sources, a common web service enveloped access through a decentralised web service integrations platform, as well as a security & audit overview.

18.1.1 Overview of Data Source and Selected Integrations

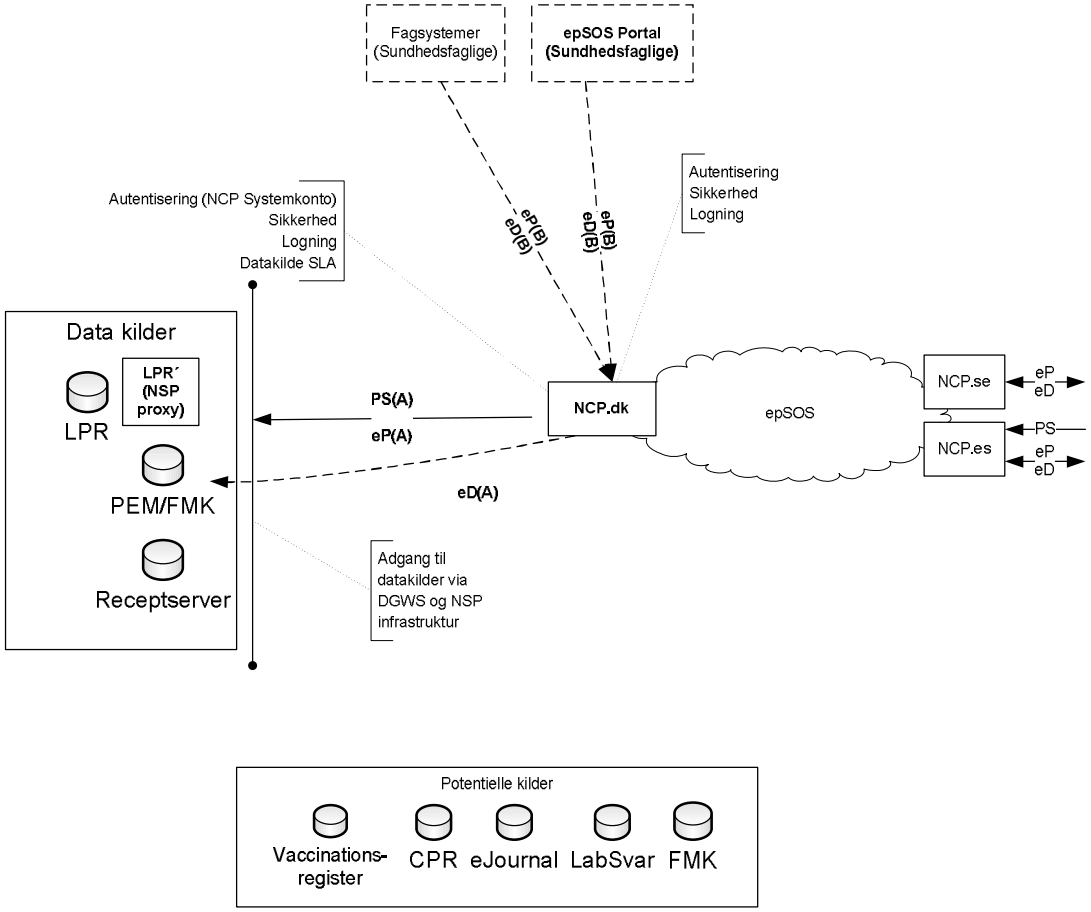


Figure 20: Danish Data Sources and Integrations Overview

The Danish integrations for the Danish version of the NCP are done to central data sources which gather data on patients in Denmark. Denmark has many central health data sources, which simplified the access to data for the NCP. To access the data sources through the same security-model, SLA and Audit mechanisms the access is done through a common de-central web service platform and through a common web service envelope.

18.2 Security Authentication & Audit Traceability

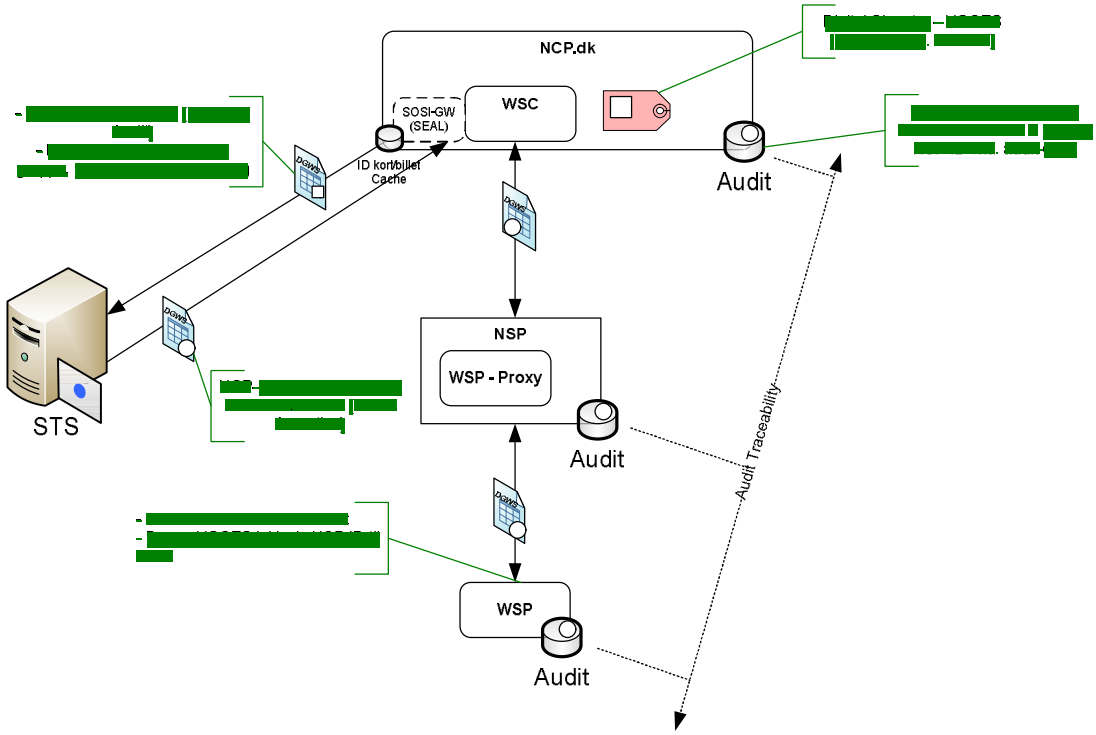


Figure 21: Security Setup & Audit Traceability for NCP-A

The Danish security setup uses a SAML token based web service access to data sources. The design for requesting the SAML assertion (ticket) involves a common certificate for all TRC – sessions (one for the NCP-A). Upon requesting the STS ticket the HCP & Patient identifiers are added to the request, thus a new ticket is issued for each Treatment-Relationship session making security audit traceable for each session. Audit logs will be maintained in the NCP (Common Components), in the decentralised platform (National Service Platform - NSP) and at the data source. Message transport is not signed in the Danish infrastructure in the current versions, however the transport is through a secured eHealth only network (based on agreements).

18.3 Spanish NCP Example

18.3.1 Motivations and State of the Project

Spain is divided in 17 regions (autonomous communities) each managing its own health system that should provide service to local population, Spanish population from other communities and citizens for other countries. At national level, two different situations were considered: when a Spaniard is travelling temporarily from one community to another where only relevant data should be shared; but also the case when a citizen moves permanently to a new location, situation under which access to complete EHR is required.

Another special feature of the system is that it should be able to handle data in four different languages: Spanish (used through the country) and also Basque, Catalan (also Valencian and Balearic) and Galician.

In this scenario, the main motivations for developing a national EHR in Spain were:

- The EHR is widespread in Spain (more than 90 % in primary health care).
- There are different models for EHR in different regional health systems.
- Different languages are used by HCPs and citizens in different regions.
- We need to make regional health systems interoperable with each other because patients travel and move within Spain, and even sometimes they are receiving particular healthcare services at regions different from the one they live in.

The project started in 2006 and is nowadays being deployed at the different regions that are the healthcare providers.

The first steps in the project consisted of achieving a consensus in the documents to be included in the national EHR project. In the Spanish project, not only the PS is accessible but also some other clinical documents as discharged hospital letters and other reports from any speciality, primary care reports, nurse care reports, radiology (images and reports), laboratory reports.
A common national structure for the PS was also defined, its main features are:

- There should be only one PS in each region for the same patient.
- PS has to be strongly summarised to show a useful general view that can be consulted quickly.
- It must contain all the data that is interesting for any HCPs (nurses, GPs, specialist) to give health care assistance to the patient, but nothing that is not essential. It contains every data which its ignorance will mean a risk for patient health.
- It is a structured document and it is interoperable.
- Most of its content (if not everything) must be automatically fulfilled from the whole EHR.
- It must be accessible for doctors and nurses at the all NHS but only when the patient seeks health care.
- The patient should have access to his/her own PS (not to professional subjective comments)

18.3.2 Functional Architecture

There is a Central Node of the National Health System (NHS-CN) sited at the Ministry of Health and Social Policy (ESNA) that:

- Centralises identification of patients providing a unique Identification for each single patient throughout Spain, linked to the regional identification code.
- Controls the access of professionals, certified by each regional authority.

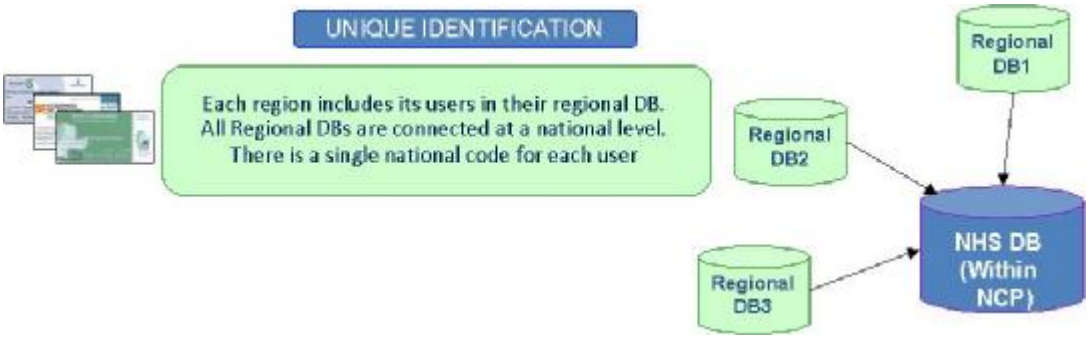
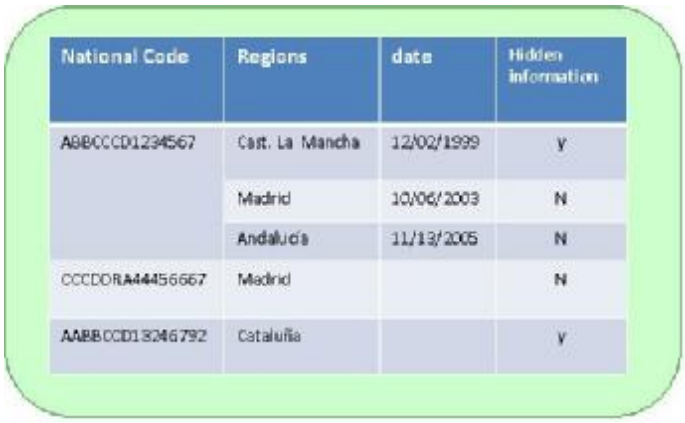


Figure 22: Distributed and Central DB

- Maintains a national Clinical Information Index, which registers the name of the regions where information related to each patient is stored. It can “on the fly” collect information from the regional’s nodes and present a list of documents that a patient have in all the regions, but no clinical data is stored.



National Code	Regions	date	Hidden information
ABBCCCD1234567	Cast. La Mancha	12/02/1999	Y
	Madrid	10/06/2003	N
	Andalucía	11/13/2005	N
CCCDDRA44456667	Madrid		N
AABBCCD13246792	Cataluña		Y

Figure 23: Clinical Information Index

From one side, regional health systems of different autonomous communities are being integrated with this NHS-CN according to the next architecture:

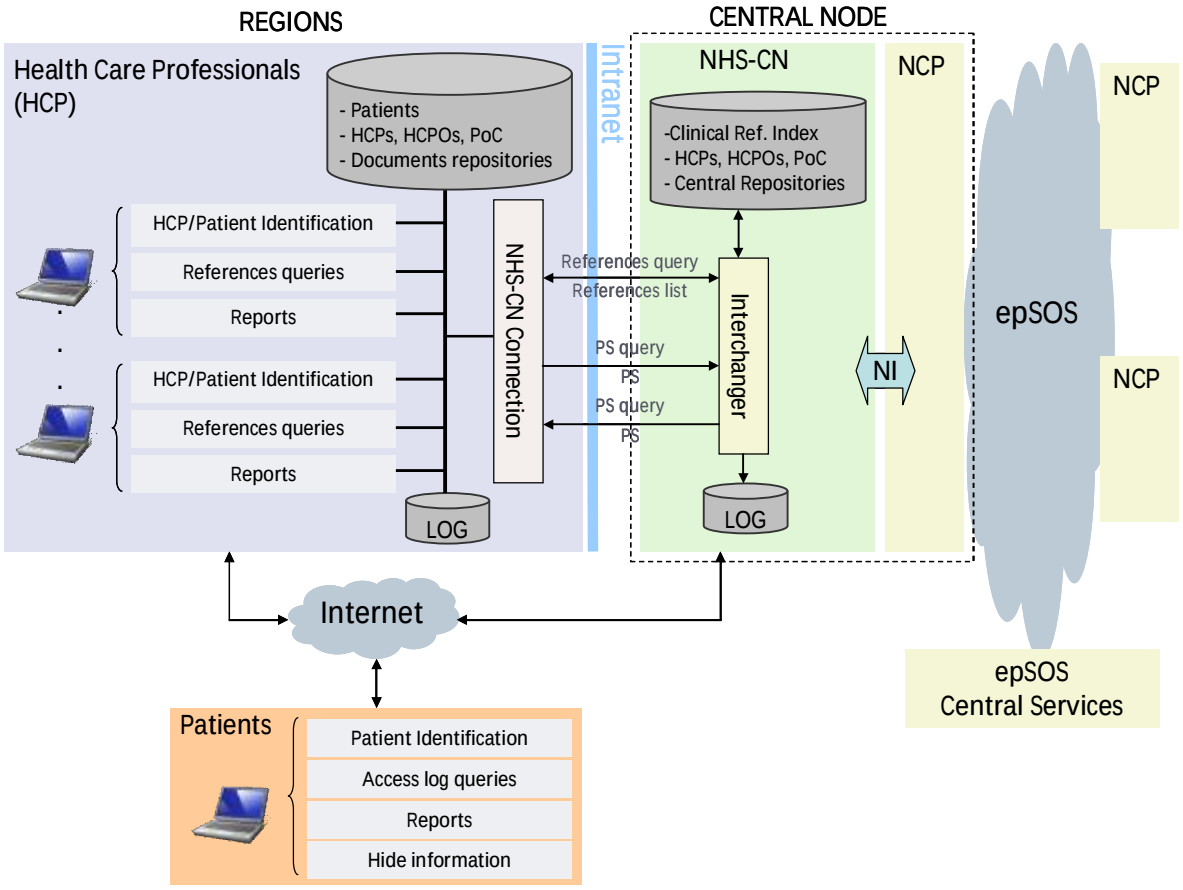


Figure 24: Spanish NCP Integration Architecture

And from the other side, the NHS-CN will be integrated with the epSOS components and services to build the Spanish NCP and provide connectivity to other MSs.

Regarding the use of standards in the Spanish case, the next ones are being used:

- XML for data interchange

- HL7 CDA level 1 for clinical information interchange
- pdf for Final documents
- DICOM and JPG for images

The Spanish NCP has been built based on the following relevant decisions in relation to the functional architecture:

- Identification means: Unequivocal identification based in the health card database (different from insurance database that can have more than one person under the same number)
- Authentication means:
  - HCPs: Electronic certificate + (e-ID card or professional card)
  - Patients: Electronic certificate or e-ID card.
- Patient Consent: Implicit if the patient is seeking for health care
- Access to PS: HCPs (doctors and nurses) and patients. The patient has the right to hide information and the HCP to know that some information has been hidden (but not what information).
- Security strategy: Based on identification and authentication system + subsequent audit access control. The subsequent control is based in a committee of administrators that can periodically audit the system but also in the possibility of the patient to consult the accesses made to his/her documents. If an access it is non-authorised he/she has the possibility to make a complaint from the same webpage.

18.3.3 Lessons Learned

In the Spanish case it has been very important to involve and achieve consensus among all relevant actors, including health professionals, citizens and different regional administrations, to coordinate functional and technological aspects.

It is important to notice that until today several problems were solved and therefore we can describe them together with the solutions:

Topic	Problem	Solution
PS Content	To identify which part of the personal history should be included in the PS	To include the possibility to drop down the inactive or closed problem list
Required Infrastructure and Resources	To have an up-to-date and accessible PS for all citizens requires heavy activity in the health regional systems.	Some regions have developed a “on the fly” system, but a maximum of one week update would be considered
Patient Consent	Explicit Patient Consent means electronic survey + electronic signature to every patient.	In the Spanish law, if the patient asks for health care to a HCP within the NHS, the consent is implicit.
Single PS	The objective was to have a single national PS where all contents of all EHRs would be integrated. To include different contents in the same section is possible in addition. The problem is to integrate information in a consisted way: to define automatic rules to choose the most relevant content, between several similar ones from different EHRs.	At that moment: one PS per region to have quality ones.

Project Management	Coordinating projects with a lot of different levels of responsibility is slow and difficult.	Being patient!
Different official languages and different catalogues between the regions	PS as an interoperable and understandable dataset in all languages.	Several catalogues are used only for several sections of the PS. Subsets of SNOMED CT are being developed to serve as a central terminology catalogue to be mapped to the existing ones and to have multilingual possibilities.