JASEHN
Joint Action to Support the eHealth Network

Co-funded by
the Health Programme
of the European Union

GUIDELINE

on

Proposal for an Organisational Framework for eHealth National Contact Points

Document Information:

Document status:	For adoption by the members of the eHealth Network at their 8th meeting on 23 November 2015
Document Version:	v2.0
Document Number:	D5.1.1
Document produced by:	Joint Action to support the eHealth Network • WP5: Interoperability and standardization • Task 5.1: Trusted eHealth National Contact Points
Author(s):	Licinio Mano, SPMS (Portugal) Henrique Martins, SPMS (Portugal) Hämäläinen Päivi, THL (Finland)
Member State Contributor(s):	A TNA (Austria), THL (Finland), ASIP (France), FRNA (France), GEMATIK (Germany), 3DHHR (Greece), ÀEEK (Hungary), DH (Ireland), VULSK (Lithuania), HDIR (Norway), SPMS(Portugal), SeHA (Sweden), SENA (Sweden)
Stakeholder Contributor(s):	EC, DG SANTE, eHN Legal Subgroup, HOPE

TABLE OF CHANGE HISTORY

Version	Date	Subject	Modified by
0.1	2015-04-10	Basic draft document	Licinio Mano
0.2	2015-04-13	Draft proposal	Henrique Martins
0.3	2015-04-14	Enriched proposal with "Initial Considerations for the Framework"	Henrique Martins Licinio Mano
0.4	2015-04-21	Task members (review comments) + EXPAND workshop discussions	Licinio Mano
0.5	2015-04-24	Informal evaluation by JAseHN members	Licinio Mano
0.6	2015-04-27	Review by European Commission JAseHN PSC members	Licinio Mano
0.7	2015-09-07	Rebranding	Licinio Mano
0.7.1	2015-09-07	Revision by Paivi	Hämäläinen Päivi
0.8	2015-09-22	Revised according to epSOS FWA and EXPAND TLA	Licinio Mano
0.9	2015-09-29	Revision after F2F meeting	Licinio Mano
0.10	2015-10-09	Incorporated EXPAND and eHN Legal SG suggestions - Submitted for JAseHN sPSC review (from 12th to 19th)	Licinio Mano
0.11	2015-10-14	- Corrected previous version numbering (from 1.0 to 0.10) - Reinforced the importance of having a coordination mechanism to enforce the OFW-NCPeH - OFW-NCPeH added principles & requirements: 1.1.1, 1.3, 3.3.1 - Included peer review and PDCA methodology for operational audits	Henrique Martins Licinio Mano

		- Proposed "Governance Stability" principle regarding the revision of the OFW-NCPeH - Updated the definition annex by adding terms emerging from the compliance establishment process.	
0.12	2015-10-23	Consolidated with JAseHN sPSC reviewers	Licinio Mano
0.13	2015-10-28	Reviewed in light of discussions held in Subgroup for Implementation meeting on 19 October. Major changes on OFW requirements: 1.1, 1.1.1 and 1.1.2, concerning the number of NCPeH foreseen for each MS.	Henrique Martins Licinio Mano
0.14	2015-10-29	Added content to "ANNEX D: Security Policy", reusing the epSOS FWA – Annex III: epSOS SECURITY POLICY	Henrique Martins Licinio Mano
0.15	2015-10-30	Change requests from HOPE project: minor typos in the text	Licinio Mano
0.16	2015-10-31	Includes suggestions made during the sPSC meeting and request by EC DG SANTE regarding the eHN decision on the provision of generic services under the eHDSI mean the preparation, setting-up, deployment and operations of the NCPeH Added 4.3.1 Following sPSC meeting Annex A will be eliminated; V.0.16 will include the changes from Annex B→ Annex A; C→ B and D→ C	Henrique Martins Licinio Mano
1.0	2015-11-04	Submitted for adoption at the 8th eHN meeting (23 November 2015)	Licinio Mano
2.0	2015-11-10	Grammar amendments. Accepted comments by the European Commission regarding the "Coordination mechanism" description and consistency across the document, as well as refined references to EU eHealth core and generic services	Licinio Mano

TABLE OF CONTENTS

Index of figures

Index of tables

I. Introduction

One of the main challenges in supporting the eHN (eHealth Network) ambitions for sustainability policies regarding assets in the field of eHealth cross-border interoperability is the bond between policies and service provision by Member States (MS).

In order to establish the bond and allow it to grow and endure, a set of simple but well-aligned instruments needs to be prepared. One of the crucial instruments is an Organisational Framework which describes, in a commonly understandable language, the principles and requirements for National Contact Points for eHealth (NCPeH).

The Cross Border eHealth Information Services (CBeHIS) mean the infrastructure and the operations used to exchange of real patient related data, in particular health data, between its members.

1.1 Purpose of this document

Propose an Organisational Framework guideline to support the governance, establishment and operation of NCPeH towards the provision of Cross-Border eHealth Information Services (CBeHIS).

The main architectural element of the Organisational Framework is the National Contact Point for eHealth (NCPeH). These NCPeH constitute the country's communication gateway that assures the interface, not only technical, between the National Infrastructure and the EU network of other Member States' NCPeH, as well as with the central EU services.

Under the eHealth Digital Services Infrastructure (eHDSI) terminology, the provision of generic services in the Member State mean the preparation, setting-up, deployment and operations of the National Contact Point for eHealth (NCPeH) for the Cross Border eHealth Information Services (CBeHIS).

The core services, to be provided by the European Commission, refer to those services that are necessary at EU level for the CBeHIS.

1.2 Scope

The Guidelines on the Organisational Framework for NCPeH (OFW-NCPeH) were prepared in close alignment with several activities taking place in the same time frame, namely:

- European guidelines on Patient Summary (2013) and ePrescriptions (2014)
- The Multilateral Legal Agreement (MLA) prepared by the eHN Legal Subgroup (LSG)[1];
- The CEF eHealth DSI call for proposals preparation;
- The EXPAND revision of organisational, semantic and technical requirements and specifications;

[1] After the 8th eHN meeting on 23 November 2015, the eHN LSG will be merged with JAseHN as task 6.2

- Other JAseHN task forces, namely the ones preparing the:
  - D5.1.2 Country guide for implementation of eHealth NCP
  - D5.6.1 Assess MS technical readiness
  - D5.6.2.1 Annual report on operational support for OpenNCP usage
- The Patient Registries Joint Action.

The OFW describes the set-up requirements, core characteristics, responsibilities and duties of an NCPeH, taking into consideration the crucial role played in the MS towards CBeHIS provision. These are not exclusively limited to well-established use cases such as the Patient Summary and ePrecription/eDispensation (eP/eD), but can also serve others that may be formalised by eHN with possible necessary adaptations.

1.3 Objectives

Provide an Organisational Framework for the eHealth NCP, addressing the key stakeholders' mandates and responsibilities:

- set organisational principles and requirements towards the establishment of the National Contact Point for eHealth,
- present a process to guide MS along the path of "Preparation; Deployment; and Operation" of CBeHIS,
- stress the the relationship with EU level coordination, which governs the access to the EU network and sets the requirements for compliance (legal, organisational, semantic and technical).

1.4 Time frame

This document's life cycle takes into consideration the following major milestones:

- eHealth Network (approval for adoption mechanism)
  - Adoption: 23 November 2015;
  - Revision: November 2017.
- CEF eHealth DSI[2] (possible financing mechanism):
  - Call for publication: November 2015;
  - Deadline for proposal: March 2016;
  - Grant agreements: by December 2016;
  - Start of activities: towards the end of 2016.

[2] Information kindly provided by SANTE D3 – eHealth and HTA Unit on 10 September 2015

1.5 Initial considerations

This proposal for an OFW-NCPeH was designed on the basis of the European Interoperability Framework (EIF). Future updates and revisions will take into consideration the ReEIF (Refined eHealth European Interoperability Framework).

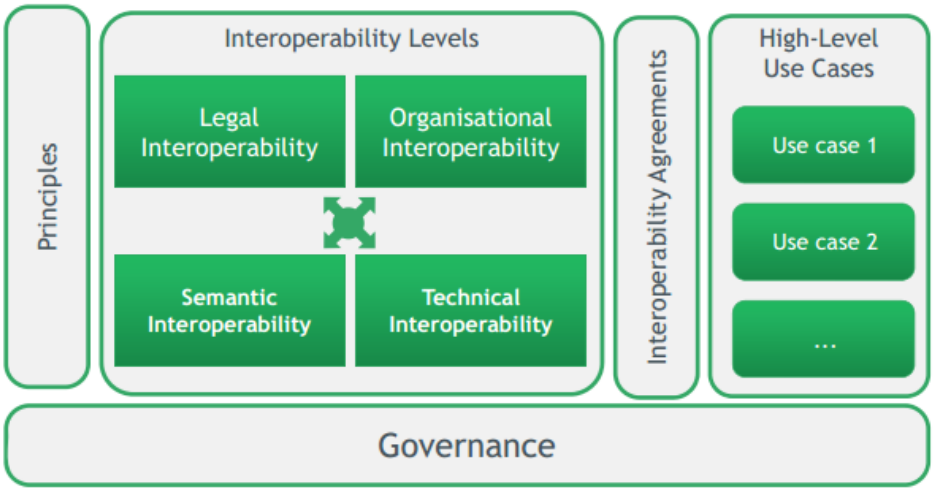

Figure 1 – Resulting eHealth EIF structure[3]

The OFW-NCPeH focuses as much as possible on the organisational principles and requirements and is in alignment with several other important arrangements that have been prepared by other projects (e.g. Antilope, EXPAND, epSOS, eHN LSG).

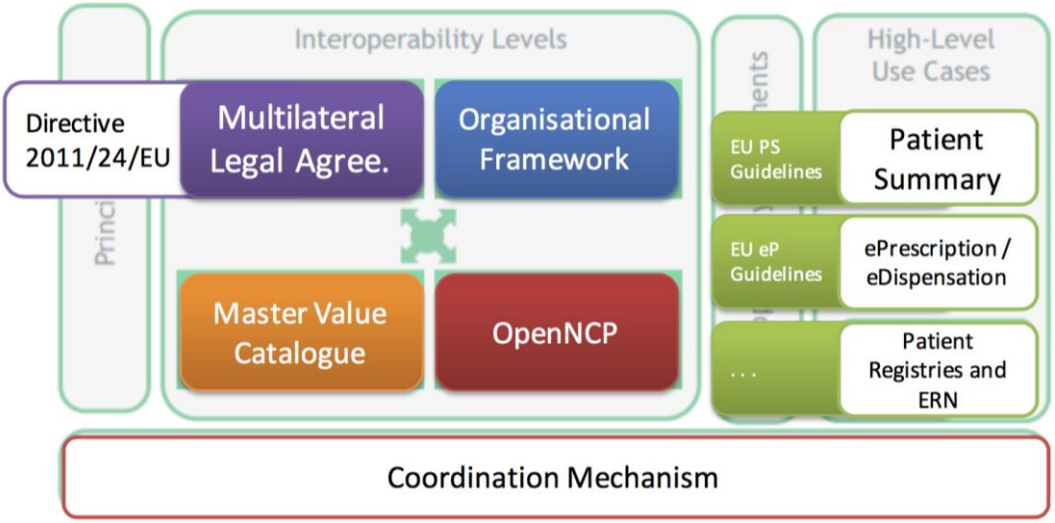

Figure 2 – OFW-NCPeH alignment with related instruments

Figure 2 provides a better understanding of how the OFW-NCPeH suits the eHealth EIF and how it interacts with several other arrangements taking place.

[3] DG CONNECT eHealth EIF – D3 Vision on eHealth EIF, Version 1.2 14 February 2013

Table 1 - NCPeH perspective on the eHealth EIF

eHealth EIF	OFW-NCPeH perspective
PRINCIPLES	The overarching principles are defined by Directive 2011/24/EU The eHealth Network established under the Directive adopts all guidelines applicable to the CBeHIS and NCPeH.
Interoperability level: legal	The Legal principles and requirements applied to CBeHIS will be stated and described in the Multilateral Legal Agreement (MLA) being prepared by the eHN Legal SG
Interoperability level: organisational	The OFW-NCPeH provided in this document is the core instrument for this interoperability level regarding CBeHIS.
Interoperability level: semantic	The Master Value Set Catalogue (and Master Translation Catalogue) as well as the semantic catalogues' governance procedures are the key aspects at this interoperability level regarding CBeHIS.
Interoperability level: technical	The technical specifications and OpenNCP[4] reference implementation are the key aspects at this interoperability level regarding CBeHIS.
Coordination mechanism at EU level	The OFW-NCPeH stresses the relationship with the EU level coordination mechanism and its role for setting the compliance requirements and grant access to the CBeHIS. The coordination mechanism is described in the document on Governance model for the eHealth Digital Service Infrastructure during the CEF[5]
Interoperability guidelines	The OFW-NCPeH takes into consideration the following eHN guidelines: • EU Patient Summary Guidelines • EU ePrescription Guidelines
Use cases (CBeHIS)	Within the scope of the OFW-NCPeH, the use cases taken into consideration are the: • Patient Summary • ePrescription (eDispensation) Other use cases may be added by the eHealth Network later[6].

[4] For more information about OpenNCP, please see https://openncp.atlassian.net/wiki/
[5] To be adopted by the eHealth Network 23 November 2015.
[6] Such as the Patient Registries and European Reference Networks.

Since several instruments are being prepared, matured and delivered simultaneously, it is expected that some overlaps and gaps may require further attention in their revised versions to ensure that the components are a perfect fit for each other.

Namely, there was initially a significant overlap between the MLA (being prepared by the eHN Legal SG) and the OFW-NCPeH (prepared by JAseHN T5.1). Although most of the issues that overlap have been identified and sorted out to differing extents, the current version may require fine-tuning and further enhancements to guarantee that all principles and requirements are correctly addressed in accordance with each specific instrument.

On the other hand, there is the need for a clear perspective on how the OFW-NCPeH will connect with other instruments such as the JAseHN T5.1 and T5.6 deliverables:

- D5.1.2 Country guide for implementation of eHealth NCP;
- D5.6.1 Assess MS technical readiness;
- D5.6.2.1 Annual report on operational support for OpenNCP usage.

The JAseHN deliverables listed above need a clear mandate on how to build on the EXPAND work in progress and monitor possible or potential duplications of effort in order to avoid content overlaps.

In this way, as shown in the following figure, the JAseHN deliverables will focus on aligning the usage of the technical instruments provided by EXPAND[7], according to relevant OFW-NCPeH compliance establishment processes (explained in section 0 4.2 Process) and guidelines.

[7] Likewise, EXPAND WP 5 Deployment Shop may further explore, from 24 November 2015 until the end of the project (31 December 2015), some concrete challenges and mechanisms for deploying the OFW-NCPeH in each MS.

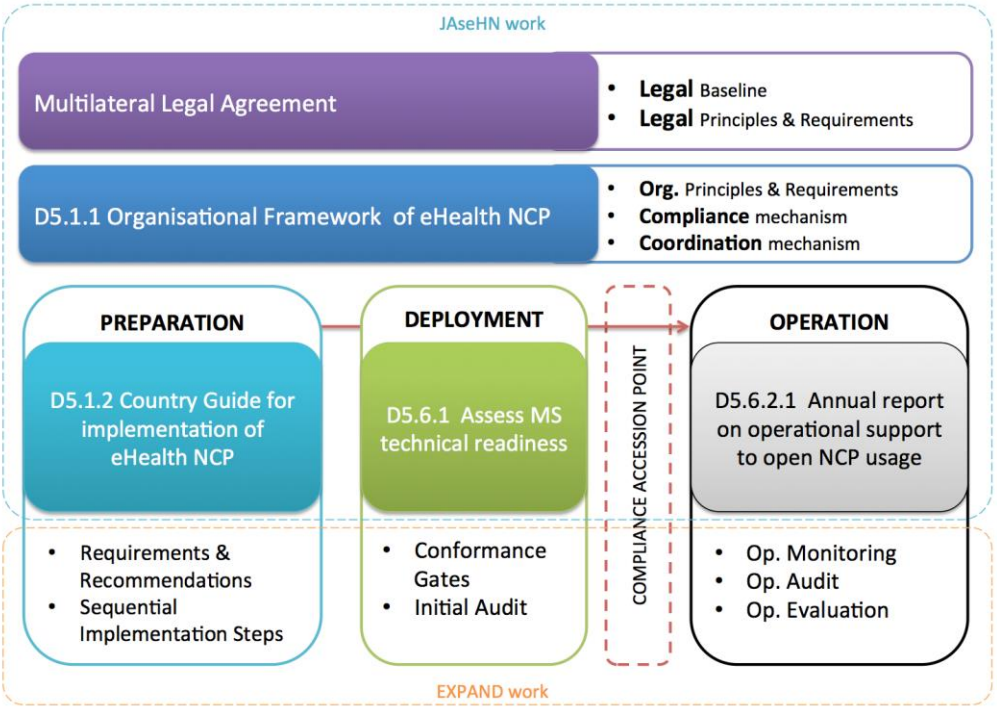

Figure 3 – Alignment of CBeHIS instruments and work in progress

II. National Contact Points for eHealth (NCPeH)

MS that have previously experienced CBeHIS (pilots or real/live services) have shown that it is necessary for MS to set up a National Contact Point for eHealth (NCPeH).

Each MS needs to organise/set up one NCPeH to act as a communication gateway with other MS and also as a mediator for delivering services.

As such, an NCPeH should be identifiable in both the EU domain and its national domain, and remain an active part of the CBeHIS environment if compliant with the legal, organisational, semantic and technical requirements.

The NCPeH should also act as an interface with existing national infrastructures.

> The provision of generic services in the Member State under the eHDSI mean the preparation, setting-up, deployment and operations of the NCPeH for CBeHIS.

The following diagram demonstrates the basic elements of the CBeHIS environment.

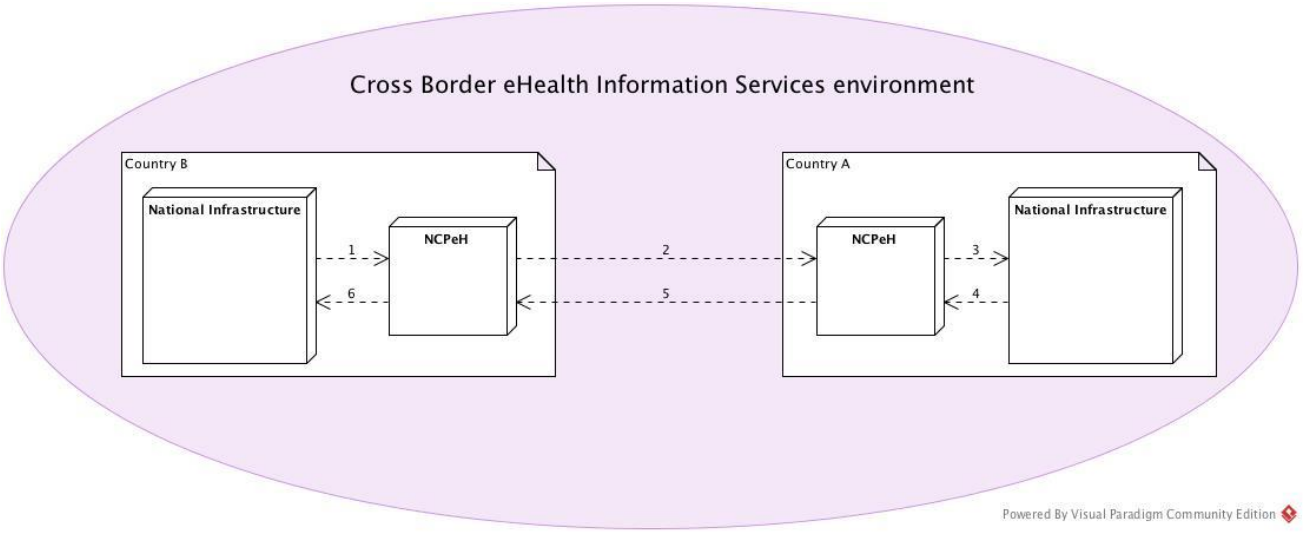

Figure 4 – CBeHIS basic architectural elements

The core characteristics, responsibilities and duties of the NCPeH (and its national partners, where applicable) are presented in these Organisational Framework guidelines, so that the NCPeH, once established, may enter into agreements on a common basis to deliver CBeHIS to patients.

The NCPeH profile is quite different (e.g. different services provided, different entity, different governance, different requirements) from the National Contact Point described in Article 6 of Directive 2011/24/EC. There is however some overlap concerning the obligation for provision of information to patients with regard to the processing of their personal data (Patient Information Notice) specific to their rights with respect to the Data Protection Directive.

III. Organisational Framework for eHealth NCP

BASELINE CONSENSUS STATEMENT

This first version of the Organisational Framework for eHealth NCP (OFW-NCPeH) is considered by the eHealth Network to be the foundational instrument for involving the National Authorities for Cross-Border eHealth Information Services (CBeHIS) provision in the process of localising this blueprint in their national reality.

Provision was made so that, after localisation is completed, this blueprint could be reviewed in terms of the amendments needed to better match its European-wide application.

3.1 Principles

- While the Multilateral Legal Agreement (MLA) sets overarching legal principles and requirements, the Organisational Framework for NCPeH (OFW-NCPeH) provides specific and commonly agreed organisational guidelines for the successful provision of Cross-Border eHealth Information Services (CBeHIS).

- This Organisational Framework (OFW) provides guidelines for coordination and compliance mechanisms towards the provision of CBeHIS supporting patient care delivery to European citizens outside their usual state of residence by means of a shareable electronic Patient Summary and ePrescription.
- These Organisational Framework for NCPeH (OFW-NCPeH) guidelines is the blueprint which must be transposed into agreements at national level in so far as it is necessary to comply with national laws or customs. It is imperative that EU level interoperability is secured at all instances and times. This may be achieved by:
    - Ensuring that any additional requirements do not create conflicts with these agreements;
    - Raising new issues identified in the process of their specific interest collaboration for consideration and policy update at EU level;
    - Maintaining transparency within the framework of EU coordination mechanism.
- This Organisational Framework for NCPeH (OFW-NCPeH) provides guidance and requirements towards the following perspectives (further specified in section 0 3.2 Organisational Framework):
    1. Definition of an NCPeH;
    2. Core characteristics of an NCPeH;
    3. General responsibilities and duties of an NCPeH;
    4. Interaction between NCPeH and with EU core services.
- The MLA handles patient consent principles and requirements.
- For health data to flow across borders, it is necessary to establish the required level of compliance and trust to ensure that Health Professionals can rely upon the integrity of the data that will support their decisions, that suitable systems of security exist to ensure that data cannot be accessed by unauthorised parties, and that patients' rights of informed consent to data sharing are duly respected by all parties.
- With respect to privacy and data protection, the principle of free movement of goods, services and persons gives rise to the need to process personal data across borders. Directive 95/46/EC regulates how personal data is processed in these cases with the aim to protect personal integrity. While MS have all recognised data contained in medical documentation as "sensitive personal data" subject to a higher level of protection, there is broad national diversity in the way the Data Protection Directive has been implemented in national provisions, which in some cases creates barriers to the free movement of data.
- While the prospective data protection regulation and the eIDAS regulation in force and their foreseen implementation may address some of the barriers identified (e.g. in the epSOS Large Scale Pilot), there is a need for the eHealth Network to discuss and come to

an agreement on a number of common policies and measures concerning privacy and security such as for identification and authentication, foreseen in Article 14 of Directive 2011/24/EU.

- Until such common measures are sufficiently reflected in appropriate legal EU level instruments, these may be expressed as requirements for countries to be addressed when setting up their NCPs for eHealth.

3.2 Organisational Framework

3.2.1 Set-up of an NCPeH

3.2.1.1 MS participating in the CBeHIS should set up an NCPeH compliant with the OFW-NCPeH. This should be unique to each MS in its relationship with other MS, i.e. a single NCPeH communication gateway should be responsible for interaction with other MS NCPeH communication gateways for cross-border services.

3.2.1.1.1 "Regional replicas" of both the technological and organisational arrangements of a typical NCPeH, would constitute a Regional Contact Point (RCPeH), are possible and follow the same principles and requirements.

3.2.1.1.2 If a MS has two or more Regional Contact Points, it needs to nominate one to act as an NCPeH, to act as the national gateway vis-à-vis other MS.

3.2.1.2 Participating MS should make adequate arrangements to ensure NCPeH readiness for operation of CBeHIS and level of service sustainability (by following the compliance establishment process described in section 0 4.2 Process).

3.2.1.3 The entry into operation of an NCPeH requires the explicit approval of the coordination mechanism established for the CBeHIS environment.

3.2.1.4 Participating MS should establish NCPeH adequate monitoring procedures.

3.2.1.5 It is recommended that national training materials and activities be provided to support CBeHIS operation.

3.2.1.6 It is recommended that participating MS engage Health Professionals in specification updates and other clinical concerns related to the operation of services.

3.2.1.7 It is recommended that participating MS inform citizens about CBeHIS provisions.

3.2.2 Core characteristics of an NCPeH

3.2.2.1 The NCPeH must establish the connection with the national infrastructure, ensuring that appropriate processes and procedures are in place (security measures, safeguards etc.).

3.2.2.1.1 Describe national infrastructure with the purpose of interfacing (e.g. services available, data sources).

3.2.2.2 The NCPeH must ensure that semantic transformation (e.g. translation and mapping), which is needed for the cross-border information exchange, is performed according to the

semantic requirements and specifications provided in 6.4 Appendix D: Semantic requirements and specifications.

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

3.2.2.2.2 Liability for errors in the semantic transformation will be described in the MLA.

3.2.2.3 The NCPeH must provide a gateway service, a request port and a semantic transformation service in order to enable it to execute the core steps in the CBeHIS (e.g. Patient Summary, ePrescription).

3.2.2.4 The MS must ensure that the NCPeH for the CBeHIS has clearly identified the responsible data controller and data processor in accordance with the provisions of Directive 95/46 EC.

3.2.2.5 The NCPeH must ensure an auditing mechanism for legal, organisational, semantic and technical requirements.

3.2.2.6 The NCPeH must enforce foreign patients' identity validation of foreign patients.

3.2.2.7 The NCPeH must maintain the national versions of the controlled vocabularies used in semantic transformation.

3.2.3 General responsibilities and duties of an NCPeH

3.2.3.1 The NCPeH shall establish appropriate security and data protection systems to conform to CBeHIS requirements as well as all applicable national requirements.

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

3.2.3.2.1 The NCPeH shall enforce identity validation of Health Professionals that use CBeHIS.

3.2.3.2.2 The NCPeH shall establish an appropriate system of audit trail, allowing authorised official bodies to duly inspect the established mechanisms for data collection, processing, translation and transmitting.

3.2.3.3 The NCPeH must ensure that CBeHIS data is not transmitted to MS not belonging or allowed into the CBeHIS environment.

3.2.3.3.1 Non-EU countries may operate in line with the CBeHIS with the explicit approval eHealth Network.

3.2.3.4 The NCPeH shall establish and maintain an incident management solution to support Health Professionals, Healthcare Providers and citizens in its territory.

3.2.4 Interaction between NCPeH and with EU core services

3.2.4.1 The NCPeH must ensure the security (confidentiality, integrity, availability, non-repudiation, authenticity and auditability) of data processed on their territory.

3.2.4.2 The NCPeH shall guarantee that all CBeHIS agreed service requirements and specifications (legal, organisational, semantic and technical) are fulfilled.

3.2.4.3 The NCPeH shall collaborate actively on the harmonisation of guidelines and appropriate practices to facilitate the establishment of the CBeHIS environment.

3.2.4.4 The NCPeH shall adopt a national OFW-NCPeH on CBeHIS that comprise commonly adopted policies, processes and audit mechanisms.

3.2.4.5 The NCPeH must ensure the appropriate interface with the core services set up at EU level.

3.2.5 NCPeH security policy

3.2.5.1 Participating MS must ensure that they are fully compliant with the CBeHIS Security Policy as set out in detail in 7.1 Annex A: Security policy.

3.2.5.1.1 The NCPeH Security Policy Baseline creates a general security and data protection baseline adapted to CBeHIS needs.

3.2.5.1.2 The NCPeH Security Policy Baseline addresses all elements of data flows in the CBeHIS, including national and cross-border data flows.

IV. Compliance establishment process

4.1 Rationale

The following Member State Service Operation Audit process, describes a method for ensuring that NCPeH compliance can be established, maintained and reinforced through a pre-defined set of activities and responsibilities, namely

a) The eHDSI governance structure can establish a peer-to-peer process to validate organisational arrangements between MS and at EU level (core services);

b) Checking and endorsing NCPeH organisational readiness for starting operation of CBeHIS;

c) Following up and endorsing developments in the MS after the initial audit.

d) Ensuring a level of service of the NCPeH during operation in the CBeHIS environment.

One of the key building blocks for OFW-NCPeH is the procedure through which the coordination mechanism (explained in 0) and the MS monitor progress regarding preparation, deployment and operation of cross-border care services.

Lessons learnt from previous Cross Border eHealth Information Services (CBeHIS) initiatives point to the following:

- There must be an accession process for MS into the CBeHIS environment, with clear role assignments, once all (Legal, organizational, Semantic and Technical) requirements have

been fulfilled and verified through interoperability testing, peer review and other appropriate methods.

- This process shall allow for the contractual agreements established at national level to be (peer) reviewed and assessed as compliant with MLA and OFW-NCPeH. This process should consider international, well established principles of certification.
- There must be a monitoring and support mechanism for ensuring continuing capacity (comply with principles and requirements and perform according to expected service level's) to be part of the CBeHIS environment.

4.2 Process for Member State Service Operation Audit

The current process goal is **to ensure that NCPeH compliance can be established, maintained and reinforced**.

The process is composed of three main stages:

- PREPARATION, where MS design the national deployment plan and perform national preparatory activities towards the provision of cross-border eHealth services;
- DEPLOYMENT, where MS test (nationally and internationally), audit and provide evidence of the readiness level towards the provision of services.
- OPERATION, where MS provide evidence about the quality and level of service provided, as well as Key Performance Indicators about service provision.

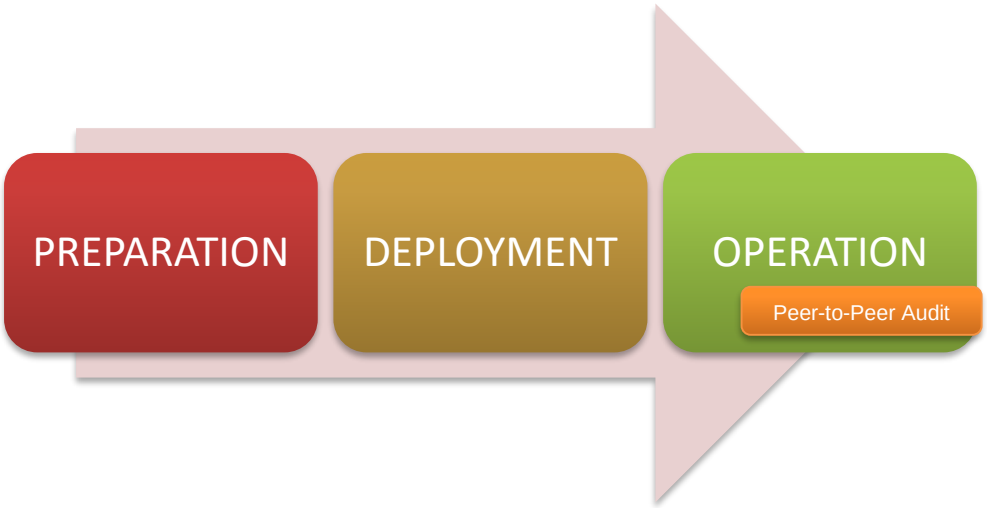

Figure 5 – Compliance establishment process

The goals defined for each stage may be supported by a set of tools and mechanisms that guide MS towards each stage as well as providing evidence on the basis of which the governing body may take decisions regarding "readiness level" and "quality of service".

Preparation

- Member State Service Deployment [PLAN]
- Member State Requirements and Recommendations [CHECKLIST]
- Member State Preparation Progress [REPORT]

Deployment

- Member State Service Readiness [CHECKLIST]
- Member State Service Initial Audit [REPORT]

Operation

- Member State Service Operation [PLAN]
- Member State Service Operation Monitoring [REPORT]
- Member State Service Operation Audit [REPORT, Peer-to-Peer Review]*
- Member State Service Operation Evaluation [REPORT]

* Audits must be performed by third party entities. In order to promote knowledge exchange and fluent convergence of practices between Member States, audits should be performed by peer Member States that may already be in operation.

This principle should be understood as a continuous improvement mechanism according to the **PDCA** (**plan–do–check–act** / **plan–do–check–adjust**) iterative four-step management method that will boost quality and MS liaison towards the provision of CBeHIS.

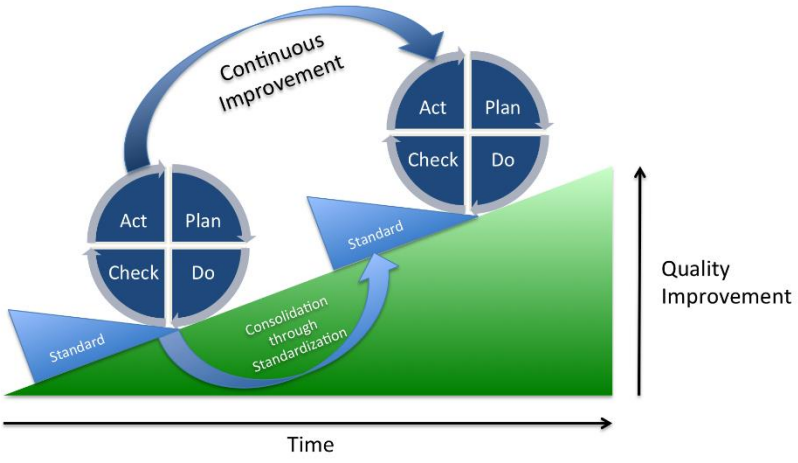

Figure 6 – PDCA iterative management method

4.3 Decision to admit a NCPeH to join the CBeHIS

The eHealth Network has the broad mandate to (as stated in Article 14, 2011/24/EU):

> *"work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare".*

The eHealth Network has a central role in coordinating eHealth-specific policy aspects within the more general EU level governance for interoperability.

The OFW-NCPeH requires that the coordination mechanism enforces the legal, organisational, semantic and technical principles and requirements underlying an entry into operation in the CBeHIS environment, the Coordination Function should be complemented by a Technical Committee that would support the necessary MS compliance assessment.

The coordination mechanism should consider a steering group composed by MS representatives.

The eHealth Network takes the decision on admitting an NCPeH to join the CBeHIS, based on the audit report.

4.4 Supporting tools and mechanisms

4.4.1 Preparation

Table 2 - Compliance establishment process - Stage 1: Preparation - tools and mechanisms

DOCUMENT	PURPOSE	VALUE ADDED
Member State Service Deployment [PLAN]	Allow the MS to share national vision and intentions towards CBeHIS provision	Knowledge about MS aims and plans, in a comparable structured way
Member State Requirements and Recommendations [CHECKLIST]	Support the MS to set up and adopt measures required for the optimal establishment of the NCPeH	Guide the MS on establishing the NCPeH
Member State Preparation Progress [REPORT]	Allow the MS to report on preparation of NCPeH activities in a structured and shareable way	Knowledge about MS status, activities in progress and known issues

4.4.2 Deployment

Table 3 - Compliance establishment process - Stage 2: Deployment - tools and mechanisms

DOCUMENT	PURPOSE	VALUE ADDED
Member State Service Readiness [CHECKLIST]	Measure and report MS readiness regarding CBeHIS provision	MS quantified readiness status for operating CBeHIS
Member State Service Initial Audit [REPORT]	Verify NCPeH compliance with CBeHIS requirements (legal, organisational, semantic and technical)	Evidence, provided by a third party, on MS readiness for operating CBeHIS

4.4.3 Operation

Table 4 - Compliance establishment process - Stage 3: Operation - tools and mechanisms

DOCUMENT	PURPOSE	VALUE ADDED
Member State Service Operation [PLAN]	Design and state MS intentions and willingness towards CBeHIS provision, as well as arrangements for keeping the level of service	Understanding practices and arrangements adopted by MS for keeping level of service
Member State Service Operation Monitoring [REPORT]	Provide an insight into the NCPeH activities performed during the operation period	Commonly agreed and structured way of understanding the NCPeH level of service
Member State Service Operation Audit [REPORT]	Verify NCPeH compliance maintenance with CBeHIS requirements (legal, organisational, semantic and technical) during operation	Evidence, provided by a third party, on NCPeH compliance for operating CBeHIS
Member State Service Operation Evaluation [REPORT]	Measure and indicate the usage and impact achieved with CBeHIS provision, as well as known issues to be addressed and improved	Service provision impact and value added (e.g. for citizens and Health Professionals) and improvement opportunities

V. Closing remarks

The current document represents the fundamental baseline for a rich and enduring Organisational Framework for National Contact Points for eHealth (OFW-NCPeH).

At this point, the nature of the OFW-NCPeH represents a commitment based on lessons learnt from previous Cross-Border eHealth Information Services (CBeHIS) initiatives and the overarching perspective that will be established under the Multilateral Legal Agreement (MLA).

The current OFW-NCPeH:

- sets organisational principles and requirements towards the establishment of the National Contact Point for eHealth (NCPeH),
- presents a process to guide MS along the path of "Preparation; Deployment; and Operation" of CBeHIS,
- stresses the need for a coordination function to act as an accession point regarding requirements compliance (legal, organisational, semantic and technical).

The proposed OFW-NCPeH requires a coordination mechanism to be enforced. It is expected that a coordination mechanism could be endorsed during the 8th eHN meeting.

The proposed OFW-NCPeH should be revised and enhanced, taking into consideration the maturity and experience emerging from service provision.

However, in order to fulfil the principle of governance stability, profound changes should not occur before a 2-year (two-year) maturation cycle (by November 2017). Until then, enhancements should focus on fine-tuning the OFW-NCPeH without touching the underlying principles and requirements.

VI. Appendices

6.1 Appendix A: Glossary

TERM	DESCRIPTION
CBeHIS	Cross-Border eHealth Information Services
CEF	Connecting Europe Facility
DSI	Digital Service Infrastructure
EC	European Commission
eHDSI	Term used for the generic and core services for the cross border services of eP and PS during CEF financing
eHN	eHealth Network
eHN-LSG	eHealth Network Legal Subgroup
EIF	European Interoperability Framework
EU	European Union
IOP	Interoperability
HP	Health Professional
JAseHN	Joint Action to support the eHN
LOST	Legal, Organisational, Semantic, Technical
MLA	Multilateral Legal Agreement
MS	Member States (of EU)
NCP	National Contact Point
NCPeH	National Contact Point for eHealth
NI	National Infrastructure
OFW	Organisational Framework
OFW-NCPeH	Organisational Framework for eHealth National Contact Point
PoC	Point of Care
ReEIF	Refined eHealth European Interoperability Framework
PARENT JA	Patient Registries Joint Action

6.2 Appendix B: Definitions

CONCEPT	DEFINITION
CBeHIS	Cross-Border eHealth Information Services within the scope of the current document, namely Patient Summary and ePrescription (may include eDispensation)
CBeHIS environment	Stakeholders, relations between them and favourable infrastructures to allow CBeHIS to flourish
CEF eHealth DSI	EU financial (€7.5M) mechanism (based on call for proposals) that will be launched by November 2015 and may be used by MS to support CBeHIS provision (preparation, deployment and operation of NCPeH - meaning generic services in CEF)
Communication gateway	MS system that manages CBeHIS transactions with other MS and which connects to the NI. This is an entry/exit point from the MS, acting on behalf of a HP and citizen (at a Point of Care), that ensures the exchange of the patient's medical data in a controlled environment.
Compliance establishment process	A well-defined set of activities and evidence used to ensure that NCPeH compliance can be established, maintained and reinforced.
Country A	The country of affiliation. This is the country that holds information about a patient, where the patient can be unequivocally identified and his or her data may be accessed.
Country B	The country of treatment, i.e. the country where cross-border healthcare is provided when the patient seeks care abroad.
Framework	A real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful.
Guideline	A suggested way of compliance when doing something. It is visible to those using or supporting the use of a particular service but there are no sanctions if it is not followed.
Guideline for adoption	Intended to present to the eHealth Network's members a clear guideline, with the intention for it to be adopted and optionally implemented by the EU MS at national level in the next step.
National infrastructure	The healthcare IT infrastructure, which manages patient and HP/HCP[8] identification and healthcare records in MS.
NCP	National Contact Point as referred to in Article 6 of Directive 2011/24/EU
NCPeH	National Contact Point for eHealth, which may act as an organisational and

[8] see Article 3 (f) and (g) of Directive 2011/24/EU

	technical gateway for the provision of eHealth Cross-Border Information Services
NCPeH deployment	Set of activities aiming to ensure NCPeH compliance with the full range of requirements (LOST) established towards CBeHIS provision
NCPeH implementation	Process of preparing, deploying and operating an NCPeH
NCPeH operation	Set of activities performed by the MS while providing services to citizens and Health Professionals
NCPeH preparation	Set of activities aiming to set up an NCPeH
Organisational Framework	Defines core characteristics, duties and responsibilities of an NCPeH
PoC	A location where an EU citizen may seek healthcare services. This may be a hospital, pharmacy or any other facility in the healthcare system of Country B.
Requirement	Definition of relevant needs (business, functional, non-functional, technical and technological) for system specification and implementation

6.3 Appendix C: References

This document is based upon several reference materials, beyond epSOS FWA, provided by EXPAND and other EU eHealth projects. The following list provides an exhaustive identification of the material considered until the present version of this document:

- Framework Agreement on National Contact Points in the context of epSOS (epSOS FWA)
- epSOS Interoperability Framework and Key Interoperability Layers (D.3.3.3)
- epSOS National Pilot Set Up and Deployment Guide (D3.8.2)
- epSOS FINAL SECURITY SERVICES SPECIFICATION DEFINITION (D.3.7.2.), namely SECTION III SUITABILITY ANALYSIS
- epSOS Testing Methodology, Test Plan and Tools (D3.9.2)
- epSOS Recommendations (D2.2.7)
- Antilope Refinement Definition document (D1.1)
- EXPAND Scope and transferability of key outcomes of epSOS and corresponding actions for transferability and scale up (D5.1 Draft)

Project pilot tools that can be reshaped and adapted for large-scale services were also used and enhanced, including:

- epSOS Participating Nation Pilot Plan;
- epSOS Requirements and Recommendations – Check List;
- epSOS Participating Nation Member State Progress Report;
- epSOS Participating Nation Initial Audit Report
- epSOS D4.D.3 Report on readiness to pilot

6.4 Appendix D: Semantic requirements and specifications

- Provided by:
    - GUIDELINES ON MINIMUM/NONEXHAUSTIVE PATIENT SUMMARY DATASET FOR ELECTRONIC EXCHANGE IN ACCORDANCE WITH THE CROSS-BORDER DIRECTIVE 2011/24/EU
    - GUIDELINES ON ePRESCRIPTIONS DATASET FOR ELECTRONIC EXCHANGE UNDER CROSS-BORDER DIRECTIVE 2011/24/EU
- To be provided: EXPAND, a consolidated version of epSOS Semantic Requirements and Specifications.

VII. Annexes

7.1 Annex A: Security policy

1. Need and scope

Security is a critically important issue for CBeHIS. Without adequate security in place none of the CBeHIS can be used in real-life environments. The CBeHIS Security Policy aims to create a secure operational environment for the service deployment, which will be sufficient for protecting the CBeHIS data and processes, implementable and agreed by all MS. The CBeHIS Security Policy provides a secure operational environment for CBeHIS and helps develop a 'chain of trust' among CBeHIS actors. The CBeHIS Security Policy also specifies the requirements of service providers and users and must be implemented and periodically audited by all CBeHIS actors, as described below.

2. Principles

All CBeHIS data and processes must be adequately protected. The network built among the CBeHIS MS should also not add any unacceptable new risk within any participating organisation. Appropriate technologies and procedures must be used to ensure that data is stored, processed and transmitted securely over the network built among the CBeHIS actors and is only disclosed to authorised parties.

Information security is generally characterised as the protection of:

a. *Confidentiality (information is protected from unauthorised access or unintended disclosure – only authorised users have access to the information and other system resources),*
b. *Integrity (information is protected from unauthorised modification) and*
c. *Availability (resources are available, without unreasonable delay - authorised users are able to access information and the related means when they need it).*

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

3. Objectives

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

More specifically, the CBeHIS Security Policy objectives are:

a. *To make CBeHIS actors sensitive to the operated means of protection and the risks which they cover.*
b. *To create a general security framework adapted to the CBeHIS information system needs, which should be observed by those in charge of CBeHIS processes; it should be implemented by putting in place*

measures and procedures in order to ensure the CBeHIS information and CBeHIS information system and infrastructure security.

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

d. *To enhance user and patient trust in the information system.*

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

The CBeHIS security policy is constructed in line with the principle of a well-proportioned answer to the incurred risk.

4. Security rules

- To be adopted by the eHealth Network[9].

[9] The eHealth Network will consider them as soon as provided by JAseHN T5.1, they will have as foundation the epSOS Security Policy, but will be curated (jointly with JAseHN T6.2) to be in perfect alignment with the MLA.