eHealth Network

Guideline on an Organisational Framework for the National Contact Point for eHealth

Release 2

Adopted by the eHealth Network on 12/11/2020

TABLE OF CONTENTS

I. Introduction

One of the main challenges in supporting the eHealth Network (eHN) 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 evolve, a set of simple but well-aligned instruments needs to be prepared. One of the crucial instruments is an Organisational Framework that describes, in a commonly understandable language, the principles and requirements for the 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.

Terms referenced in this document are defined in the eHDSI Glossary[1].

1.1 Purpose of this document

The purpose of the Guidelines on an Organisational Framework for the National Contact Point for eHealth (Organisational Framework) is to support the governance, establishment and operation of an NCPeH towards the provision of Cross-Border eHealth Information Services (CBeHIS).

1.2 Scope

The Organisational Framework describes the eHDSI compliance establishment process, NCPeH 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 (PS) and ePrescription/eDispensation (eP/eD), but can also serve others that may be formalised by the eHN with possible necessary adaptations. The document represents the fundamental baseline for a rich and enduring Organisational Framework for National Contact Points for eHealth.

1.3 Objectives

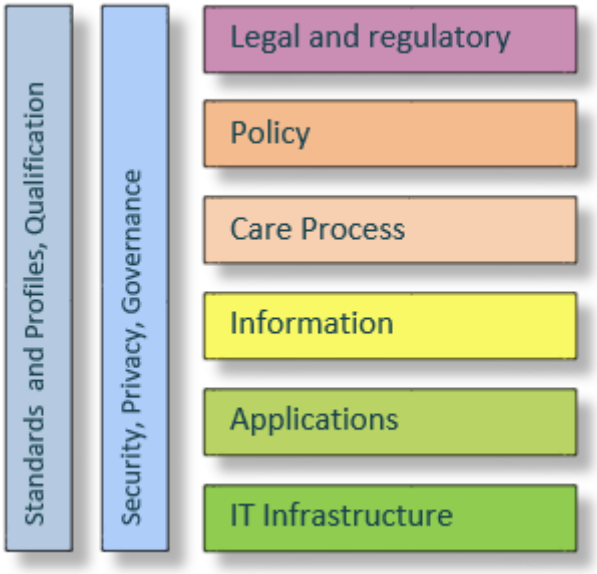
Provide an Organisational Framework for the NCPeH, addressing the key stakeholders' mandates and responsibilities:

- 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 MS relationship relating to EU level coordination, which governs access to the EU network and sets the requirements for compliance in the applicable domains i.e. (legal, organisational, information security, semantic and technical).

[1] https://ec.europa.eu/cefdigital/wiki/x/a0YZAg

1.4 Initial considerations

This Organisational Framework was designed based on the European Interoperability Framework 2 (EIF2) and the ReEIF (Refined eHealth European Interoperability Framework[2]).



eHealth EIF	Organisational Framework perspective
PRINCIPLES	The overarching principles are defined by the Directive 2011/24/EU and Commission Implementing Decision 2011/890/EU providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, as amended. 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 are stated and described in the Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services (Agreement)
Interoperability level: organisational	The Organisational Framework provided in this document is the core instrument for this interoperability level regarding CBeHIS.
Interoperability level: semantic	The Semantic Specifications and Master Value Set Catalogue (and Master Translation Catalogue) as well as the semantic

[2] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf

	catalogues' governance procedures are the key aspects at this interoperability level regarding CBeHIS[3].
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 Organisational Framework 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[5]
Interoperability guidelines	The Organisational Framework takes into consideration the following eHN guidelines: • General Guidelines on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2[6] • Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 ePrescriptions and eDispensations[7] • Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU Release 2 Patient Summary for unscheduled care[8]
Use cases (CBeHIS)	Within the scope of the Organisational Framework, the use cases taken into consideration are the: • Patient Summary • ePrescription (eDispensation) Other use cases may be added by decision of the eHealth Network.

II. eHDSI establishment process

2.1 Rationale

The eHealth Network has a central role in coordinating the European eHealth specific policy aspects, as stated in Article 14 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

In 2015, the eHealth Network decided to set up the eHDSI to enable the cross-border exchange of health data.

[3] https://ec.europa.eu/cefdigital/wiki/x/30QZAg
[4] https://ec.europa.eu/cefdigital/wiki/x/30QZAg
[5] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co06_en.pdf
[6] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co092_en.pdf
[7] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co091_en.pdf
[8] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20161121_co10_en.pdf

2.2 eHealth DSI

The eHealth Digital Service Infrastructure is an infrastructure, enabling the exchange of health data between National Contact Points for eHealth.

2.3 Data protection

The NCPeHs data protection responsibilities within eHealth DSI are listed in the Commission Implementing Decision 2011/890/EU providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, as amended.

2.4 NCPeH process to join the CBeHIS

Before an NCPeH is allowed to start exchanging electronic health data across borders, it has to

(1) follow the NCPeH process to join the CBeHIS - be tested and audited to prove its compliance with the eHealth DSI requirements and specifications

(2) obtain the required decisions to join the CBeHIS.

To join the CBeHIS each NCPeH needs to follow the eHDSI compliance establishment process As a result, an NCPeH will be able to summarise its testing and audit results in the MS Overall Readiness Statement[9], containing the following

- the Outcome Summary Test Report, as stated by the Test Framework[10];
- the Audit Reports[11];
- the Signed Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services[12].

2.5 Obtaining decisions to join the CBeHIS[13]

To obtain the eHMSEG Decision to be authorized to start Production Environment Tests, MS needs to follow the eHDSI Procedure 3.

To obtain the eHN Decision to start the NCPeH in new service routine operations, MS needs to follow the eHDSI Procedure 4.

To obtain the eHMSEG Decision to start the NCPeH new exchange for the service already in routine operations MS needs to follow the eHDSI Procedure 5.

To obtain the eHMSEG Decision to continue the NCPeH Routine Operations after the annual Upgrade Pre-Production Tests MS needs to follow the eHDSI Procedure 6.

To obtain the eHMSEG Decision to restore an NCPeH affected service(s) back in to Routine Operations MS needs to follow the eHDSI Procedure 7.

[9] https://ec.europa.eu/cefdigital/wiki/x/WKgSB
[10] https://ec.europa.eu/cefdigital/wiki/x/4UQZAg
[11] https://ec.europa.eu/cefdigital/wiki/x/vxlAAg
[12] https://ec.europa.eu/cefdigital/wiki/x/WKgSB
[13] https://ec.europa.eu/cefdigital/wiki/x/WKgSB

2.6 Role of the Commission

The eHDSI Service Catalogue, Delivery and Overall Deployment Plans[14] contains the list of services included in eHDSI Core Services and plan (content and time) committed by eHDSI Solution Provider to release digital services updates. Those services are necessary at EU level for the CBeHIS.

2.7 Role of Member States

The exchange of data takes place directly between Member States National Contact Points for eHealth (peer to peer). The NCPeH are the main architectural element of the Organisational Framework. The NCPeH constitutes country's communication gateway that assures the interface, between the National Infrastructure and the EU network of other Member States' NCPeH, as well as with the eHDSI Core Services.

III. NCPeH establishment process

3.1 Rationale

Each MS needs to organise/set up one NCPeH to act as a communication gateway with other MS and 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, information security, 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 means the preparation, setting-up, deployment and operations of the NCPeH for CBeHIS.

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

[14] https://ec.europa.eu/cefdigital/wiki/x/kpNDDQ

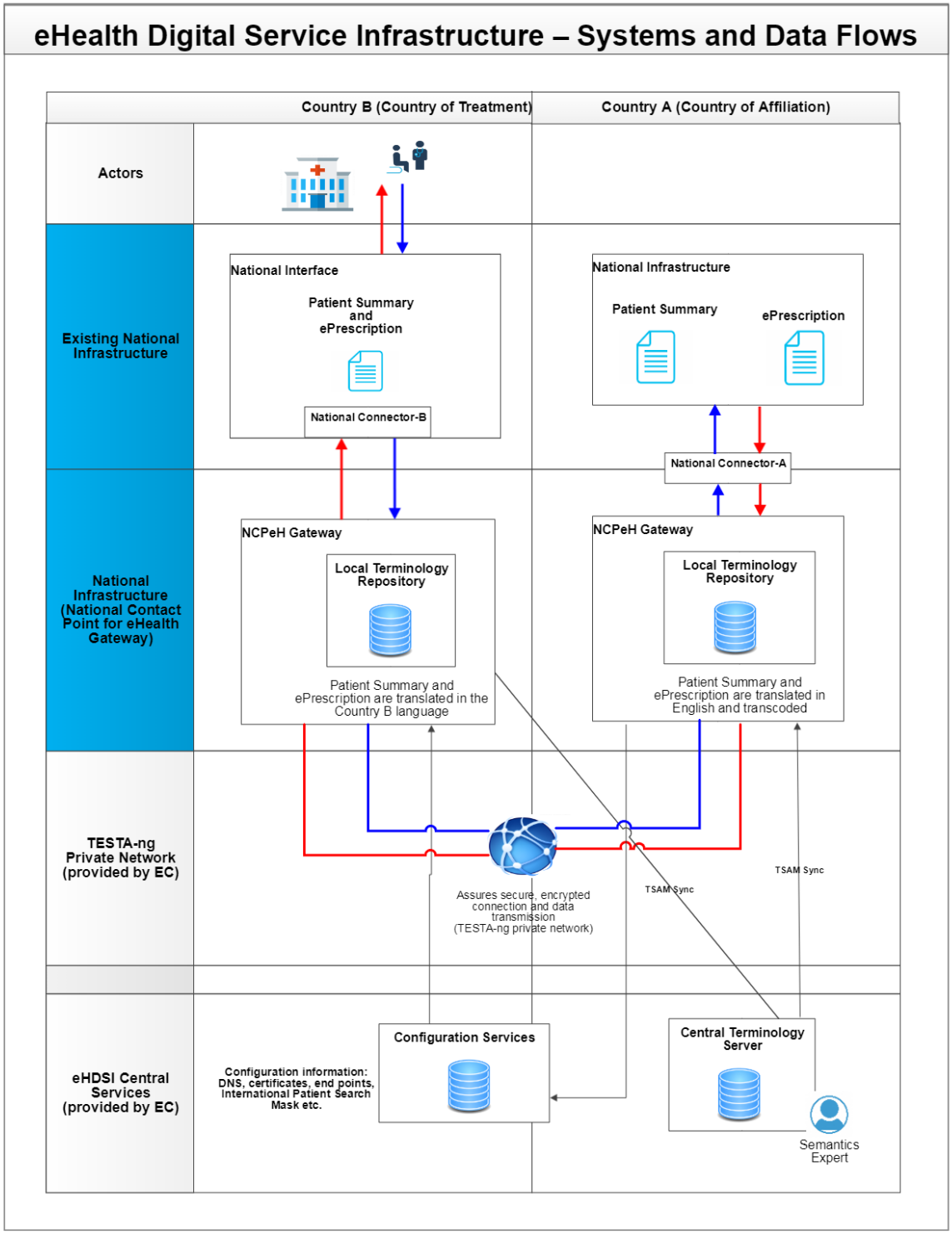


Figure 1[15] eHealth Digital Service Infrastructure – Systems and Data Flows

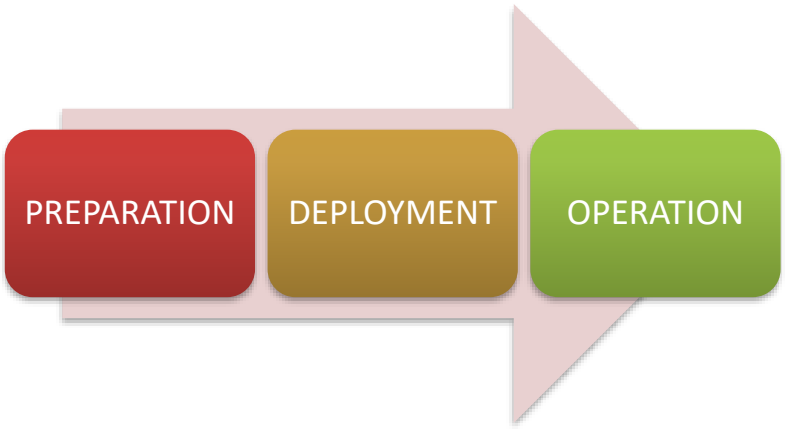
[15] https://ec.europa.eu/cefdigital/wiki/x/WKgSB

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

3.2 NCPeH establishment process

The NCPeH establishment process 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.



3.3 Supporting eHDSI Normative Artefacts and tools

The goals defined for each stage are supported by the eHDSI Normative Artefacts or tools that guide MS towards each stage as well as providing evidence based on which the governing body might take decisions regarding "readiness level" and "quality of service".

3.3.1 Preparation stage

SUPPORT	PURPOSE
Member State Service Deployment and Improvement Plan[16]	Allow the MS to share a national vision and intentions towards CBeHIS provision.
eHDSI Requirements[17]	Support the MS to set up and adopt measures required for the optimal establishment of the NCPeH.

[16] https://ec.europa.eu/cefdigital/wiki/x/C4OVEQ
[17] https://ec.europa.eu/cefdigital/wiki/x/DAFVBg

3.3.2 Deployment stage

DOCUMENT	PURPOSE
eHDSI Audit Framework[18] eHDSI Readiness Criteria Checklist[19]	Verify NCPeH compliance with CBeHIS requirements (legal, organisational, information security, semantic and technical) before joining the routine operations. Measure and report the MS readiness regarding CBeHIS provision.
eHDSI Test Framework[20]	Provide prerequisites and guidelines for the test planning, test design, test implementation, test execution and test evaluation processes.

3.3.3 Operation stage

DOCUMENT	PURPOSE
eHDSI Operations Framework[21]	Design and state MS intentions and willingness towards CBeHIS provision, as well as arrangements for keeping the level of service.
eHDSI Audit Framework[22]	Verify NCPeH service(s) in operations compliance with CBeHIS requirements.
eHDSI Test Framework[23]	Provide prerequisites and guidelines for upgrade to the next Wave specifications.

IV. Organisational Framework for an NCPeH

4.1 Principles

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

(2) Whereas the Organisational Framework 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.

(3) The Organisational Framework is the blueprint, which must be transposed into agreements at national level as 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:

[18] https://ec.europa.eu/cefdigital/wiki/x/vxlAAg
[19] https://ec.europa.eu/cefdigital/wiki/x/vxlAAg
[20] https://ec.europa.eu/cefdigital/wiki/x/4UQZAg
[21] https://ec.europa.eu/cefdigital/wiki/x/FRSHAw
[22] https://ec.europa.eu/cefdigital/wiki/x/vxlAAg
[23] https://ec.europa.eu/cefdigital/wiki/x/4UQZAg

- 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.

(4) The Organisational Framework provides guidance and requirements towards the following perspectives (further specified in section Organisational Framework):

- Definition of an NCPeH;
- Core characteristics of an NCPeH;
- General responsibilities and duties of an NCPeH;
- Interaction between the NCPeH and the EU core services.

(5) The Agreement handles patient consent principles and requirements.

(6) 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 are duly respected by all parties.

(7) With respect to privacy and data protection, the NCPeHs should consider the provisions of the European and National legislation on data protection in force.

4.2 Organisational Framework

4.2.1 Set-up of an NCPeH

(1) MS participating in the CBeHIS should set up an NCPeH compliant with the Organisational Framework. 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.
(2) "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) 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.
(4) 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 **Error! Reference source not found.**).
(5) Entry into operation of an NCPeH requires the explicit approval of the coordination mechanism established for the CBeHIS environment.
(6) Participating MS should establish NCPeH adequate monitoring procedures.
(7) It is recommended that national training materials and activities be provided to support CBeHIS operation.

(8) It is recommended that participating MS engage Health Professionals in specification updates and other clinical concerns related to the operation of services.
(9) It is recommended that participating MS inform citizens about CBeHIS provisions.

4.2.2 Core characteristics of an NCPeH

(1) The NCPeH must establish the connection with the national infrastructure, ensuring that appropriate processes and procedures are in place (security measures, safeguards etc.).
(2) Describe the national infrastructure with the purpose of interfacing (e.g. services available, data sources).
(3) 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 applicable[24].
(4) The responsibility for the accuracy and integrity of the process is with each national designated competent entity for such semantic processing.
(5) 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).
(6) The NCPeH must undergo an audit for legal, organisational, information security, semantic, and technical requirements.
(7) The NCPeH must enforce patients' identity validation.
(8) The NCPeH must maintain the national versions of the controlled vocabularies used in semantic transformation.

4.2.3 General responsibilities and duties of an NCPeH

(1) The NCPeH shall establish appropriate security and data protection systems to conform to CBeHIS requirements as well as all applicable national requirements.
(2) The NCPeH shall take all reasonable steps to ensure data security (including data confidentiality, integrity, authenticity, availability and non-repudiation).
(3) The NCPeH shall enforce identity validation of Health Professionals that use CBeHIS.
(4) 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.
(5) The NCPeH must ensure that CBeHIS data is not transmitted to MS not belonging or allowed into the CBeHIS environment.
(6) The NCPeH shall establish and maintain an incident management solution to support Health Professionals, Healthcare Providers and citizens in its territory.

4.2.4 Interaction between the NCPeH and the EU core services

(1) The NCPeH must ensure the security (confidentiality, integrity, availability, non-repudiation, authenticity and auditability) of data processed on their territory.
(2) The NCPeH shall guarantee that all CBeHIS agreed service requirements and specifications (legal, organisational, semantic and technical) are fulfilled.
(3) The NCPeH shall collaborate actively on the harmonisation of guidelines and appropriate practices to facilitate the establishment of the CBeHIS environment.

[24] https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Semantic+Services+Specification

(4) The NCPeH shall adopt a national Organisational Framework on CBeHIS that comprise commonly adopted policies, processes and audit mechanisms.
(5) The NCPeH must ensure the appropriate interface with the core services set up at EU level.

4.2.4.1 NCPeH security policy[25]

(1) Participating MS must ensure that they are fully compliant with the CBeHIS Security Policy objectives as set out in detail in this chapter.
(2) The NCPeH Security Policy Baseline creates a general security and data protection baseline adapted to CBeHIS needs.
(3) The NCPeH Security Policy Baseline addresses all elements of data flows in the CBeHIS, including national and cross-border data flows.
(4) 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.

4.2.4.1.1 Security Principles and Objectives

(1) 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.
(2) Information security is generally characterised as the protection of:
- Confidentiality (information is protected from unauthorised access or unintended disclosure – only authorised users have access to the information and other system resources);
- Integrity (information is protected from unauthorised modification);
- 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) 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:
- To make CBeHIS actors sensitive to the operated means of protection and the risks which they cover;

[25] https://ec.europa.eu/cefdigital/wiki/x/30QZAg

- 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;
- To promote cooperation between various CBeHIS actors in order to jointly elaborate and put in place those measures, instructions and procedures;
- To enhance Health Professionals and patient trust in the information system;
- To ensure that the information system in place respects national and European legislation on privacy and data protection in force;

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