Co-funded by
the Health Programme
of the European Union

JASEHN

Joint Action to Support the eHealth Network

DISCUSSION PAPER

on

Policies Regarding Interoperability of Electronic Professional Registries

Document Information:

Document status:	For discussion by the members of the eHealth Network at their 12th meeting on 28 November 2017
Approved by JAseHN sPSC	Yes
Document Version:	v3.4
Document Number:	D5.2.2
Document produced by:	Joint Action to support the eHealth Network • WP5 Interoperability & Standardization • Task 5.2 Electronic Identification for eHealth
Author(s):	Manne Andersson, Swedish eHealth Agency (Sweden) Beatrice Streit, GEMATIK (Germany) Jürgen Wehnert, GEMATIK (Germany) Sören Bittins, Fraunhofer FOKUS (Germany)
Member State Contributor(s):	Heiko Zimmermann (Luxemburg) Jeremy Thorpe (United Kingdom) Robert Scharinger (Austria)
Stakeholder Contributor(s):	CPME

TABLE OF CHANGE HISTORY

VERSION	DATE	SUBJECT	MODIFIED BY
0.0	2016-09-16	ORIGINAL VERSION	JÜRGEN WEHNERT (GEMATIK), MANNE ANDERSSON (SWEDISH EHEALTH AGENCY)
0.1	2016-09-21	DRAFT SUBMITTED "FOR REVIEW" BY JASEHN WP3	JÜRGEN WEHNERT (GEMATIK)
0.2	2016-10-05	V1	JÜRGEN WEHNERT (GEMATIK)
0.3	2016-10-13	COMMENTS INCORPORATED FOR V2	BEATRICE STREIT (GEMATIK)
0.4	2016-10-14	DRAFT SUBMITTED "FOR REVIEW" BY JASEHN WP3	BEATRICE STREIT (GEMATIK)
0.5	2016-12-12	STRUCTURE OF DOCUMENT CHANGED	BEATRICE STREIT (GEMATIK)
0.6	2017-01-19	STRUCTURE OF DOCUMENT CHANGED	BEATRICE STREIT (GEMATIK)
0.7	2017-01-20	SCOPE SPECIFIED	BEATRICE STREIT (GEMATIK)
0.9	2017-01-24	OBJECTIVE SPECIFIED	BEATRICE STREIT (GEMATIK)
1.0	2017-03-02	STRUCTURE OF DOCUMENT UPDATED	BEATRICE STREIT (GEMATIK)
1.1	2017-03-03	ADDING REFERENCES AND APPENDICES	BEATRICE STREIT (GEMATIK)
1.2	2017-03-06	ADDING MATERIAL FROM MSS	BEATRICE STREIT (GEMATIK)
1.3	2017-03-09	REVISING STRUCTURE OF DOCUMENT	BEATRICE STREIT (GEMATIK)
1.4	2017-03-13	REVISING SCOPE	BEATRICE STREIT (GEMATIK)
1.5	2017-03-15	REVISING OBJECTIVES	BEATRICE STREIT (GEMATIK)
1.6	2017-03-16	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
1.7	2017-03-17	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
1.8	2017-03-21	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
1.9	2017-03-22	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
2.0	2017-03-23	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
2.1	2017-03-24	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
2.2	2017-03-27	REVISING CONTENT	BEATRICE STREIT (GEMATIK)

2.3	2017-03-28	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
2.4	2017-03-29	REVISING CONTENT	BEATRICE STREIT (GEMATIK)
2.5	2017-04-20	INCORPORATING SPSC'S COMMENTS	BEATRICE STREIT (GEMATIK)
2.6	2017-09-05	INCORPORATING FINDINGS OF THE EID WS IN BERLIN	SÖREN BITTINS (FRAUNHOFER FOKUS)
2.7	2017-09-11	REVIEWING AND UPDATING	BEATRICE STREIT (GEMATIK), JÜRGEN WEHNERT (GEMATIK)
2.8	2017-09-15	STRUCTURE OF DOCUMENT UPDATED	BEATRICE STREIT (GEMATIK)
3.0	2017-09-26	FINAL REVISION FOR 1ST SPSC REVIEW	SÖREN BITTINS (FRAUNHOFER FOKUS) JÜRGEN WEHNERT (GEMATIK)
3.0	2017-09-29	WP3 QUALITY CHECK	RADU PIRLOG (BBU), ANDREEA MARCU (BBU)
3.1	2017-10-17	INCORPORATING COMMENTS RECEIVED	BEATRICE STREIT (GEMATIK)
3.2	2017-10-20	FINAL REVISION FOR 2ND SPSC REVIEW	BEATRICE STREIT (GEMATIK)
3.3	2017-11-08	INCORPORATING SPSC'S COMMENTS	BEATRICE STREIT (GEMATIK)
3.4	2017-11-09	WP3 QUALITY CHECK	RADU PIRLOG (BBU), ANDREEA MARCU (BBU)

LIST OF ABBREVIATIONS

ACRONYM	DEFINITION

Agreement	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;
	FORMER MULTILATERAL LEGAL AGREEMENT (MLA);
	FOR EASIER IDENTIFICATION IN THE TEXT WRITTEN IN ITALICS: *Agreement*

CBeHIS	CROSS-BORDER EHEALTH INFORMATION SERVICES
CEF	CONNECTING EUROPE FACILITY
CPME	STANDING COMMITTEE OF EUROPEAN DOCTORS
DSI	DIGITAL SERVICE INFRASTRUCTURE
EC	EUROPEAN COMMISSION
eHDSI	EHEALTH DIGITAL SERVICES INFRASTRUCTURE
eHN	EHEALTH NETWORK
eHN-LSG	EHEALTH NETWORK LEGAL SUBGROUP
EIF	EUROPEAN INTEROPERABILITY FRAMEWORK
eP	ELECTRONIC PRESCRIPTION
EU	EUROPEAN UNION
IOP	INTEROPERABILITY
HP	HEALTH PROFESSIONAL
IMI	INTERNAL MARKET INFORMATION (SYSTEM)
JAseHN	JOINT ACTION FOR SUPPORT THE EHN
LOST	LEGAL, ORGANISATIONAL, SEMANTIC, TECHNICAL
MLA	SEE “AGREEMENT”
MS	MEMBER STATES (OF EU)
NCP	NATIONAL CONTACT POINT FOR CROSS-BORDER
NCPeH	NATIONAL CONTACT POINT FOR EHEALTH
NI	NATIONAL INFRASTRUCTURE
OFW	ORGANISATIONAL FRAMEWORK
OFW-NCPeH	ORGANISATIONAL FRAMEWORK FOR EHEALTH NATIONAL CONTACT POINTS
PARENT JA	PATIENT REGISTRIES JOINT ACTION
PoC	POINT OF CARE
PS	PATIENT SUMMARY
ReEIF	REFINED EHEALTH EUROPEAN INTEROPERABILITY FRAMEWORK

LIST OF TABLES

TABLE OF CONTENTS

1. 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 grow and endure a set of simple but well-aligned instruments need 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). Another important instrument is the Policy Paper on the Interoperability of Registries for healthcare professionals, which discusses the current state of the art concerning interoperability requirements for Registries for healthcare professionals for electronic cross-border services under the Cross-border eHealth Information Services (CBeHIS). Cross-Border eHealth Information Services that are processed via NCPeH for the purpose of cross-border healthcare, as they were agreed by the eHN (Patient Summary for unscheduled care; ePrescriptions and eDispensations) and as they will be agreed by the eHN in the future.

1.2 Purpose of the document

The purpose of this document is to sum up the current situation concerning Registries for healthcare professionals and their interoperability in the light of the provision of Cross-Border eHealth Information Services (CBeHIS).

The Policy Paper on the Interoperability of Registries for healthcare professionals was prepared based on accomplished activities and in close alignment with still ongoing activities, namely (but non-exhaustively):

- Organisational Framework for eHealth National Contact Points (OFW-NCPeH) adopted by eHealth Network
- 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*) adopted by the eHealth Network and to be signed by the competent national authorities.
- eID specific framework for eHealth Release 1 and Release 2 to be adopted by the eHealth Network.
- Final results of the work of PARENT for patient registries “Methodological guidelines and recommendations for efficient and rational governance of patient registries”.[1]
- Technical Delta Analysis on eID and related topics[2]
- Policy work done by organizations like CPME[3] for specific roles in eHealth “Ensuring the secure use of telemedicine and e-health applications in an integrated Europe – Towards a Common Policy Agreement on Electronic ID Systems for Physicians”

[1] see http://patientregistries.eu/ and http://parent-wiki.nijz.si/

[2] Input document for the eID workshops on the 22nd and 23rd August 2017 in Berlin, which was updated afterwards with the results of discussions in the workshops and comments received.

[3] see http://www.cpme.eu/cpme-policy-ensuring-the-secure-use-of-telemedicine-and-e-health-applications-in-an-integrated-europe-towards-a-common-policy-agreement-on-electronic-id-systems-for-physicians/

1.2 Scope

The Policy Paper on the Interoperability of Registries for healthcare professionals outlines and discusses Registries for healthcare professionals in MSs with a focus on cross-border interoperability aspects - considering the legal basis for CBeHIS provision in Europe.

The Policy Paper on the Interoperability of Registries for healthcare professionals will help MSs to be aware of open questions, problems and possible solutions for Registries for healthcare professionals and to start detailed discussions towards a future common usage of Registries for healthcare professionals in CBeHIS. The far reaching implications of legal requirements laid out in this policy paper suggest to not only consider them on a per country basis. Indeed, it has to be considered if and how the requirements can be met across Europe to support the required use cases: Also it needs to be clarified which support format should be chosen, such as a Guideline for Interoperability.

This Policy Paper was conceived with a view to the initial use cases Patient Summary (PS) and ePrescription/eDispensation (eP/eD). However, it is designed to cater for further use cases for which adaptions or amendments maybe necessary without challenging the overall principles.

1.3 Objectives

The Policy Paper on the Interoperability of Registries for healthcare professionals builds a common understanding of Registries for healthcare professionals and the importance for CBeHIS provision and discusses especially interoperability related aspects and open questions. An electronic health professionals register is required for cross-border data exchange to identify if a person or an entity is entitled to access particular sets of data. The Policy Paper also contains a proposal for next steps in order to initiate suiteable activities to be ready for future waves of CBeHIS.

1.4 Initial Considerations

The overall structure presented in the Guideline on an Organizational Framework for eHealth National Contact Points (OFW-NCPeH) foresees several instruments to support CBeHIS in its preparation, deployment and operation phase. Each Member State aiming to participate in the eHDSI shall undergo all three phases. For every phase JAseHN provides supportive documents. The Policy Paper on the Interoperability of Registries for healthcare professionals is one of these documents which address the Preparation and Deployment Phase as well as the Operation Phase.

Interoperability of professional health registries is required to enable, control, and regulate access to health related information across and between jurisdictions, domains, and concepts. It is not possible and also not required that the concepts, owners, granularities etc. of registries are made the same across jurisdictions as long as sufficient common ground can be found. This common ground has to be large enough to support identified use cases for cross border health care. While the common ground may be quite small it is imperative that it is encompassing all four domains of the refined eHealth European Interoperability Framework (ReEIF), i.e. legal, organisational, semantic and technical aspects.

The Policy Paper on the Interoperability of Registries for healthcare professionals was designed with reference to the ReEIF.

2. Executive Summary

The eHealth Network Members are asked to discuss the following recommendations:

- Each Member State participating in CBeHIS shall make available an electronic access means to their health professional directory to other Member States participating in CBeHIS.
- Each Member State participating in CBeHIS shall make the replies of the Registry for healthcare professionals to electronic information requests competent and authoritative for the eHealth domain.
- Each Member State participating in CBeHIS shall provide such access in a singular fashion that in case of more than one Registry for healthcare professionals existing nationally, the NCPeH encapsulates the communication as a single point of contact for all other Member States.
- Registries for healthcare professionals shall offer unified access, technical interoperability, and security.

The following tasks were identified, which should be carried out by a collaboration of eHDSI Solution Provider and eHMSEG:

- A commonly shared and understood vocabulary shall be defined in order to transform, translate, and encode the national health provider information into a pan-European format.
- The to-be designed controlled vocabulary shall furthermore define a minimum list of terms to be supported without restricting Member States to exceed this minimum. An exhaustive list of critical data elements, such as the authorisation to exercise activities in the healthcare sector – health professional credentials – shall be identified and then standardised.

3. Registries for healthcare professionals

For the purpose of this document, a *registry for healthcare professionals* is defined as an organized electronic system that provides the data and information about each individual belonging to a group of people defined by a particular *professional role*, and that serves predetermined scientific, clinical or/and public health (policy) purposes.

A healthcare *professional* means

- a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or
- another professional exercising activity in the healthcare sector, which are restricted to a regulated profession as defined in Article 3 (1) (a) of Directive 2005/36/EC, or
- a person considered to be a health professional according to the legislation of the Member State of patient treatment.

For the purpose of this document, the role of professionals and with that their entitlements to access data are of special interest.

There are various purposes for Registries for healthcare professionals. According to *ISO 21091:2013 Health Informatics – Directory services for healthcare providers, subjects of care and other entities* sixteen different healthcare scenarios for Registries for healthcare professionals were identified. They contain a wide range of administrative as well as treatment related scenarios including *patient care in another country* (see scenario A.4.12). Each healthcare scenario is shortly described and the services needed for a suitable Registry for healthcare professionals (thery are called healthcare directory) are named. This Policy Paper takes the requirements of scenario *patient care in another country* into account and includes relevant aspects for use cases in CBeHIS.

As the intended purpose of a Registry for healthcare professionals plays a significant role for their design, the national legal basis needs to be considered carefully by each MS. If national jurisdiction limits the scope of the Registry for healthcare professionals to national or specific scenarios only, the usage of that Registry would probably not cover the cross-border scenarios of CBeHIS.

3.1 Registries for healthcare professionals in Member States

This section gives a short overview on some already existing Registries for healthcare professionals in Member States. It is a non-exhaustive list, providing illustrative examples.

Switzerland has a couple of different registers. The national register for qualified health staff (Nationales Register für Gesundheitsfachpersonen, NAREG) does e.g. exclude doctors, veterinaries, chiropractors, dentists and pharmacists who are listed in the Medizinalberuferegister, MedReg. Health professionals with psychological qualifications will be registered in a third system.

In **Luxembourg** a national healthcare provider directory is in place, providing information about authorized health professionals and institutions under Luxemburgish law.

The content of the directory is governed and managed by the Ministry for Health, the service is provided by Agence eSanté as part of the eSanté platform. The HPD is used by different authorized systems to provide information to support their access-control and authorization process, as well as it provides data for public online directories.The **Swedish Professional Health Registry (HOSP)** is an updated register of licensed health care professionals in Sweden, which contains all national certified professionals and is governed and manageded by *The National Board of Health and Welfare.* A unique id is used to identify the licensed health care professional.

Depending on the purpose, a health care professional in Sweden has a license (e.g. to practise medicine) or a temporary license (e.g. being a foreign doctor, a doctor in training or a medical student). For licenses general rules are provided by the Patient Safety Law. Each eligible individual must apply to the *The National Board of Health and Welfare* and gets registered in the *Swedish Electronic Professional Registry*. For temporary licenses rules are provided by regulation of *The National Board of Health and Welfare.*

The right to prescribe is differentiated in Sweden: Licensed doctors can prescribe drugs for the treatment of humans. Only licensed pharmacists are allowed to dispense medical products. Dentists, dental hygienists, midwives and some nurses and optician can prescribe a limited selection of medicines. A non-licensed physician must prescribe only within the framework of the mandate. Doctors' right to prescribe is not completely unlimited, special rules apply for some drugs. These Rules are governed and managed by *Medical Products Agency* and *The National Board of Health and Welfare*.

The following issues for the Swedish Professional Health Registry were identified in Sweden:

- Public vs private health care provider electronic access to the registry is limited due to the registers regulation in an ordinance (2006: 196) about the register of healthcare professionals. Not all temporary licenses are registered in a formal national registry.

The Austrian **e-Health-Verzeichnisdienst** (eHVD) is a registry for healthcare professionals which is based on national legislation (*Gesundheitstelematikgesetz*) and provides data on health care professionals and their roles.

The eHVD's primary objective is to confirm the identity and role of health care professionals for electronic communication of health data and by doing this to enhance data security. eHVD enables role based qualified data access to e-Health systems and portals. Additionally eHVD serves as the basis for secure, cross-border data exchange in European and international collaboration.

Being a national and cross-institutional body the Austrian MoH is currently the provider of the eHVD. It is foreseen to technically and/or organizationally link the eHVD with already existing directories and data bases of viable institutions. These existing directories and data bases will not be replaced.

4. Interoperability of Registries for healthcare professionals

The following sections lay down concerns, challenges and known possibilities or recommendations regarding Registries for healthcare professionals and their Interoperability. They are structured following the LOST approach according to refined eHealth EIF complemented by additional sections where needed.

4.1 General Considerations, Responsibilities and Duties

In order to provide sustainable interoperability between Registries for healthcare professionals in MS towards CBeHIS provision it is necessary to take a look at the following general considerations especially towards responsibilities and duties of relevant actors.

- It is the obligation of the NCPeH of the MS to establish the communication with the national Registry or Registries for healthcare professionals.

- The national Registry for healthcare professionals supports the sufficient and documented identification and authentication of (healthcare) professionals in this MS according to its national jurisdiction.

- A professional may have one or more roles and may be affiliated with multiple organisations.

- EU Alert Mechanism – Providing Safety and Mobility: From 18th January 2016 on, EU countries are required to warn each other through the Internal Market Information (IMI) system about professionals working in the fields of health or education of minors who have been prohibited or restricted from practice in one EU country, or who have used falsified diplomas in support of their application for the recognition of their qualification. The alert mechanism[4] will provide strong data protection safeguards for the professionals, and safeguard people who use the professional services.

[4] http://ec.europa.eu/internal_market/imi-net/library/question_sets_forms/index_en.htm
http://ec.europa.eu/internal_market/imi-net/statistics/index_en.htm#maincontentSec4

- The regulated professions database based on directive 2005/36/EU[5] and set up by DG GROW[6] has harmonized minimal levels for these professions: Doctors, Dentists, Nurses, Pharmasist and Midwifes for Europe.

MS need to consider all the above to provide access to their Registry(ies) for healthcare professionals either directly or to assess the rightfulness of a communication request via the NCPeH and the national eHealth infrastructure.

4.2 Legal Environment

This section provides a non-exhaustive description of the legal environment on European level for Registries for healthcare professionals.

The main foundation of the Guidelines on the interoperability of Registries for healthcare professionals is the eIDAS Regulation and the General Data Protection Regulation, which applies to several domains, not specifically to eHealth. The eIDAS Regulation and General Data Protection Regulation shall be followed by all Member States and shall be transferred into national legislation regardless of whether they participate in CBeHIS or not.

The recitals 10 and 12 of eIDAS Regulation explicitly state that the domain eHealth has been taken into consideration. The eIDAS regulation applies for cross-border patient data exchange with online-services such as Patient Summary and/or ePrescription services even though it is intended to serve needs beyond domain boundaries. The eIDAS set-up allows for optional agreed extensions based on the individual domain's needs and upon the domain's request.

On the 27th of April 2016 the EC published a regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive). The General Data Protection Regulation makes it explicitly clear that personal data concerning health and health care services as referred to in the cross-border directive 2011/24/EU were taken into consideration, see recital 35.

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) lays down legal boundaries for the CBeHIS provision on the grounds of eIDAS regulation and several other applicable laws. The Agreement was adopted by the eHealth Network in May 2017 and is to be signed by the competent national authorities after receiving the opinion of the Art. 29 Working Party. Among several other clauses the Agreement refers to the identification and authentication of patients, health professionals and healthcare providers as well as to the authorization of a health professional.

The legal foundation for the interoperability of Professional Registries comprises of the eIDAS regulation, the GDP Regulation and the *Agreement*. However, national legislation for setting up and operating existing or future national Professional Registries may vary significantly between MS for example in their content, scope, use case and level of detail.

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0036&from=DE

[6] http://ec.europa.eu/growth/tools-databases/regprof/

4.3 Organisational and Policy Requirements

A professional requesting health data about a patient in care from another country is only entitled to receive information for which he is authorized to process in his own jurisdiction. In epSOS terminology this means that the data source in country-A (the place of residence or insurance of a patient) has to take an informed decision about the specific legitimacy of the data disclosure request from the health professional of the other country. While the access control decision of country-A is entirely based on national jurisdiction, almost all available information (health professional authentication, professional role, existence of a specific consent, etc.) to justify such cross-border access is provided by country-B. In addition to the typical challenges regarding the semantic interoperability and expressiveness of processing electronic identity attributes provided by another country, another critical issue is to balance the responsibilities and entitlements of the at least two involved jurisdictions, as the health professional operates exclusively under country-B's national law, while the data-disclosing country-A is regulated by its own national provisions. Furthermore, to assure non-interference between the relevant participants, any national specialties of one jurisdiction need to be indicated in a way that avoids imposing unjust or unfair burden onto the other, for instance regarding the permissions of a health professional or the specific mean of subject authentication. For example, it would be deemed as interference and unjust for country-A to impose specific encoding and classification rules onto the local Identity Provider in country-B in order to simplify country-A's responsibilities towards their own access control. Consequently, a mediating facility following the concept of a national contact point or single point of contact and operated under the responsibility of the national competent authority may provide such a fundamental service of mapping between a local identity management, professional qualifaction, and their pan-European equivalent without imposing on local health IT nor constraining the national access control responsibilities of country-A.

Traditionally, the data disclosure (access control) decision as well as the agreement on the providence and stability of supporting information has been predominately taken solely based on a contractual agreement (e.g. with 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) between all participants and was only partially supported and enforced by technology. At the time of the original epSOS, neither appropriate technical systems, nor pan-European legal frameworks regulating such technology were available in order to fully automate the decision on data disclosure requests. Consequently, the access control systems in country-A were unable to independently validate and verify any claims and were effectively trusting in the proper implementation of country-B's contractual obligation to properly authenticate and authorise their health professionals. While country-A did perform some verification steps on the data received from country-B, both the expressiveness and stability of this information was insufficient to satisfy the requirements towards an *informed* access control decision and its subsequent technical enforcement. Effectively, country-A was only capable of generating an Audit Trail outlining the circumstances of the clinical information request for addressing potential future disputes and simply accepted any requests granted that the request itself was structurally complete. This caused the access control systems of traditional epSOS to operate under a *positive bias*, which is contrary to the best practices in information security.

According to the *Agreement* between Member States and the technical specifications any request for clinical data needs to undergo a series of a-priori tests either organisationally or technically before a disclosure decision is taken:

- is a complete and valid patient consent recorded that fits the legal conditions, technical assurances, and organisational context of the request?
- is the ***type of requester*** (e.g. a general practitioner or a nurse) entitled to receive the requested data according to country-A - the health professional's country – national/regional legislations and rules?
- is the ***type of requester*** (e.g. a general practitioner or a nurse) entitled to receive the data according to country-A- the data source's country - legislations and rules?
- is any form of acceptable entitlement or authorization for data retrieval applicable:
    - formal authorisation (regular means of being authorised as a health professional)?
    - overriding circumstance (e.g. emergency situations)?
- is the ***actual requester*** matching the below profile requirements:
    - is the providence of information about the requester complete?
    - can both types of requesters and their assigned entitlements (permissions) be successfully and meaningfully combined and processed in and satisfying the jurisdiction of country-A?
    - are overriding circumstances present and are those applicable in country-A?
    - how recent is this information?
- sufficient and documented ***authentication*** of the actual requester has to be undertaken in country B. Country A must be provided with a document assertion of a completed trust establishment (trust bootstrapping) between country-A and B in order to be able to trust and act upon requests leading to a disclosure of its governed patient data.

The verification of the entitlement according to the original epSOS specification requires special attention as country-B is not only providing a fundamental warranty about the requestor being authorised to exercise activities in the healthcare sector, which are restricted to a regulated profession, but also includes a set of nationally applicable permissions. This means that epSOS distinguished between what requestors *are* and what these requestors *are authorised to do* in their applicable national jurisdiction. The combination of both, authorisation to operate as a health professional on one hand and the explicit authorisation to perform specific tasks on the other hand form the *entitlement* of a health professional.

For expressing the latter, all applicable national entitlements have been represented in a controlled vocabulary, the HL7 permission catalogue and sent alongside with the authorization of the requestor performing work as a health professional. As an example in a country doctors, hospital nurses and midwives might be entitled to request and read patient summaries. This concept enables a transparent view on what principal actors are entitled to which cross-border functions for communicating countries. Regarding the authorisation to operate as a health professional, a similar correlation facility is implemented, which translates the national function or role of the health professional to the concepts of the regulated professions database of Directive 2005/36/EU. It is to be analysed if this mapping table is still needed if the adoption and signature of the *Agreement* introduces a legal basis for CBeHIS. This depends especially on clause II.4.1 Security Principles of the *Agreement* concerning trust between Member States.

A further consideration regards functional units in the outpatient and inpatient sector of healthcare. It has to be considered if e.g. a hospital meeting certain requirements shall be entitled by patients for hospital-wide use of their data by defined qualified staff. The same applies to doctor's offices, medical centres and other bodies of the outpatient sector.

1) **Each Member State participating in CBeHIS shall make available an electronic access means to their health professional directory to other Member States participating in CBeHIS.**

Independent electronic access to a health provider directory is a prerequisite to the application and enforcement of appropriate access control and sensitive data disclosure management of country-A with a specific reference to the requirements of such a system being operated according to the following principles:

- the *non-interference principle* as outlined 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
- the *state-of-the-art* as referenced by Article 32 GDPR as the foundation of systemic security
- the *proportionality* as balance between benefit and burden

Maintaining an independent, electronic verification means for country-A by the national competent authority of country-B significantly strengthens the enforcement of appropriate confidentiality and privacy rights of the patient. Removing the need for country-B to provide and encode information that is only applicable nationally for subsequent processing in country-A within technical artefacts of the security architecture unburdens, strengthens, and maintains an interference-free enforcement of the patient rights. Concentrating the need for semantic interoperability of such a registry for healthcare professionals minimizes the managerial and operational burden for maintaining interoperability and optimizes the benefits through a single point of contact/responsibility for the semantic interoperability and a much less complex security architecture. A single point of contact/responsibility ultimately supports the concept of proportionality by balancing the burdens of operating such a registry with the increased ability to exercise rights of the patients. Since the original epSOS design Registries for healthcare professionals, especially in the eHealth domain, have evolved into standard commercial off-the-shelf technology with a wide support of relevant international standards. Today it is thus feasible to meet advanced requirements more easily.

Furthermore, Registries for healthcare professionals may be considered fundamental infrastructure components to support, enable, and motivate future use cases, especially when a specific addressing, localisation, and pre-screening of health professionals of another country are required. Common examples are:

- the a-priori specific authorisation of a particular health professional in another country within a patient consent

- initiation of an ad-hoc, unscheduled health care episode with a patient-controlled release of clinical information
- initiation of a scheduled yet temporary health care episode in reference to continued care operations (provision of prescription medication during vacation)
- efficient and secure exchange of security artefacts (such as electronic certificates, encryption keys, etc.) to support an uninterrupted application of end-to-end security based on the eIDAS trust services

2) **Each Member State participating in CBeHIS shall make the replies of the Registry for healthcare professionals to electronic information requests competent and authoritative for the eHealth domain.**

All replies of the national façade to the Registry for healthcare professionals towards other Member States shall be considered authoritative, correct, up-to-date, and trustworthy by the relying Member State. All data received shall be considered entirely fit-for-purpose in the enforcement of the patients' rights and the fullfilment of legal obligations of the relying Member State. It is the sole responsibility of the individual Registry for healthcare professionals to assure that all managed information is correct, authentic, up-to-date, and complete.

Mandating replies to be authoritative for the eHealth domain, enabling the Registry for healthcare professionals to serve as an Attribute Source for national and international Identity Management and Access Control Systems, and to be interoperable across border does not imply to specifically enable nor to prohibit "*Binding between the electronic identification means of natural and legal persons*" according to Annex 2.1.4 of the Commission Implementing Regulation (EU) 2015/1502.

3) **Each Member State participating in CBeHIS shall provide such access in a singular fashion, meaning that in case of more than one Registry for healthcare professionals existing nationally, the NCPeH encapsulates the communication as a single point of contact for all other Member States.**

In case a country's NCPeH does fan out into various other NCPeHs or in case there is not one but many professional health registries in a country then it is the obligation of the national NCPeH of that country to be the only addressed gateway irrespective of the Member State's internal fragmentation. Member States shall expose a singular, standards-based, and interoperable façade for interacting with the Registry or Registries for healthcare professionals of their country.

4) **Registries for healthcare professionals shall offer unified access, technical Interoperability, and security.**

The exposed façade of a Registry for healthcare professionals in the eHealth domain needs to feature uniform access mechanisms that are based on open, proven, and international standards as well as a common technical data transport protocol to assure its effective and efficient consumption by the other Member States within CBeHIS. Agreement on a technical standard to access this façade may not impose unjust or undue burden on the internal implementation of the underlying professional registries in a Member State. Furthermore, the technical standard needs to support the simultaneous operation of national extensions independent to the operation of the CBeHIS means. Simultaneously, the façade shall sufficiently decouple national specialties and potentially proprietary provisions to avoid imposing unnecessary complexity to a cross-border requester. The façade is anticipated to mimic the Single-Point-Of-Contact (SPOC) principle behind the NCPeH as it is transparently brokering communication between the national registry implementation and a cross-border requester through a commonly agreed technical access means as well as anchoring the legal responsibility and liability.

The technical specification of the access means shall also provide a guideline on the informational security regarding data retrievals from a Registry for healthcare professionals to enable a trustworthy processing (in terms of originator authenticity and integrity) of the retrieved information at the relying Member State as well as prohibiting illegitimate access to the registry façade itself.

Alongside with the technical interoperability, the data provided by the Registry for healthcare professionals is explicitly anticipated to be consumed by another Member State in a cross-border fashion. **Therefore, a commonly shared and understood vocabulary shall be defined in order to transform, translate, and encode the national health provider information into a pan-European format.** Relying Member States may choose to work with the common vocabulary or to translate and transcode this information in order to fullfil their respective obligations and duties. The currently used mappings and other technical artefacts of the epSOS and eHDSI specifications are already performing those data conditioning functions and may serve as a blueprint for the semantic facilities. All Member States participating in CBeHIS shall comply to at least the minimum data set.

The to-be designed controlled vocabulary shall furthermore define a minimum list of terms to be supported without restricting Member States to exceed this minimum. **An exhaustive list of critical data elements, such as the authorisation to exercise activities in the healthcare sector – from now on referred to as health professional credentials – shall be identified and then standardised, e.g. by a yet to be appointed task force to assure a common understanding and equivalency across borders.**

This document outlines the benefit and burden as well as elaborates on the impact for Registries for health professionals for CBeHIS on a policy level. It furthermore attempts to provide the outline of such services and functions with a particular emphasis on maximising their technical and semantical interoperability while respecting the non-interference principle as much as possible. Consequently, the specific design, implementation, documentation, testing, and operation for all commonly exposed services and technical artefacts needs to be undertaken mutually between the responsible entities, for instance the Member State Competent Authorities and the Solution Provider.

4.4 Semantic Requirements

The proper fulfilment of obligations within the CBeHIS requires participating Member States to provide and process a minimum list of data elements regarding the health professional authentication and authorisation. For Access Control and Audit Trail purposes, at least the:

1. professional credentials (entitlements, licenses, etc.); and
2. a unique, traceable identifier of the health professional

shall be provided by country-B to country-A in a semantically interoperable and traceable fashion.

Additional data elements may be included to further support meaningful execution of obligations as well as strengthening exercising the relevant patients' rights, such as enabling granular patient consents. Those may include specific professional roles, specialities, and addresses. Any potential situational qualifications shall also be defined and governed regarding their specific semantics but shall not be included in any Registry for healthcare professionals due to their volatile and short-term applicability.

4.5 Technical Requisites

In reference to the health professional authentication, any CBeHIS application is required to fulfil the

1) Check if patient has given a **consent**.
2) **Authenticate** the *(health care)* professional, i.e. assure the electronic identity of the subject properly correlates with the natural/legal person of the *(health care)* professional.
3) **Authenticate** the **formal qualifications** (authorization) of the *(health care)* professional to use the CBeHIS.
4) Check the **situational qualifications** (also authorization) of the access. For example, does the *(health care)* professional have valid health care relation.

Taking into account the ISO 21091:2013 scenario A.4.12 '*Patient care in another country*', a technical scenario of using Registries for healthcare professionals to support communication of authorization credentials across jurisdictions for access control decisions may be implemented as follows:

> *"The patient (subject of care from country A) falls ill while visiting another country (country B). The patient contacts a local health professional in country B (country of treatment) and provides, according to country B's regulation, his consent. The health professional authenticates towards the local health IT using the nationally mandated credentials and authentication means. As soon as an eHealth Application is invoked, the local authentication is forwarded to a A regional or national Identity Provider (IdP) operated by or through a mandate of a competent authority. This IdP determines the specific requirements of the invoked eHealth application (such as Patient Summary or ERN) and generates an attribute retrieval request towards the national Registry for healthcare professionals. The latter validates and verifies the provided technical credentials, fetches the requested attributes (such as HP identifier), transcodes or translates all terms according to the specific eHealth application, and generates an attribute statement as reply to the IdP. After receiving the complete attribute statement from the Registry for healthcare professionals, the IdP populates the required attributes within the authentication with the contents of the attribute statement, reissues the authentication in the commonly agreed format, and vouches for its correctness, completeness, and originator authenticity by applying an electronic signature.*
>
> *The health professional obtains the authentication and proceeds with requesting clinical information about a patient through the eHealth application this authentication was issued for. Using the Patient Summary (PS) as an example, the authentication of the health professional is sent alongside with the clinical data request from country-B to country-A. Country-A processes the data request and ancillary information in an initial security context, in which the claims, evidences, and the requests' contextual circumstances are checked against the appropriate safeguards, such as the patient consent and the national security policy. The Access Control Systems (ACS) of country-A are validating the request and authentication, and are then issuing an attribute request towards the Registry for healthcare professionals of country-B using the received HP identifier to obtain the credentials of the HP as well as any additional attributes that country-A requires to fulfil its professional and security policies. With the reply from the Registry for healthcare professionals of country-B, the ACS obtained confirmation about the professional credentials (entitlement) of the health professional and can take an informed access control decision regarding the request for clinical data disclosure."*

This ISO21091:2013 inspired clinical data access scenario imposes particular requirements on the involved actors:

- responsibility (by competent authorities), liability, trust, and verification/validation obligations must be properly assigned throughout the CBeHIS
- cross-border facilities to establish, express, and verify trust relationships must be provided
- end-entity identification and authentication shall be operated mandatorily for all exposed electronic services and technical artefacts
- the authenticity, origin, integrity, and to a lesser degree confidentiality of the provided claims and evidences need to be validated even across borders
- appropriate non-repudiation and Audit Trail mechanisms need to be applied by all involved actors for all critical operations
- critical technical artefacts need to assure their fitness for cross-border processing by adhering to commonly agreed syntax and semantic criteria.

5. Registries for healthcare professionals Data Set

This section provides some MS examples for Registries for healthcare professionals' data sets and proposes a minimum data set for interoperability for CBeHIS:

5.1 Example Registries for healthcare professionals' Data Set from MSs

It is a non-exhaustive list of Registries for healthcare professionals' Data Sets from MSs, which only provides illustrative examples.

The Swedish Registry for healthcare professionals (HOSP) includes the following data:

1. Name, social security number or other similar identifiers and sex
2. Registered residence[7]
3. Profession
4. Base profession, educational institution, country and date of issue of graduation
5. Specialist skills
6. Issue date of license and proof of specialist skills
7. Date when a time constrained license according to 6 expires
8. Decision on the partial admittance
9. Decision on probation and revocation of license
10. Identity code and scope of the right to prescribe
11. Technical and administrative information necessary to register the objectives to be met.

The Austrian Registry for healthcare professionals (eHVD) includes the following data according to GTelG2012 §10. (1): *Daten des eHealth-Verzeichnisdienstes*:

§10. (1) In den eHVD sind folgende Daten aufzunehmen:

[7] Registered Residence is is only retrievable from the The Swedish Tax Agency if needed.

1. Name sowie akademische Grade oder Bezeichnung des Gesundheitsdiensteanbieters,
2. die Bezeichnung des Rechtsträgers, wenn der Gesundheitsdiensteanbieter keine natürliche Person ist,
3. Identifikatoren des Gesundheitsdiensteanbieters einschließlich der eindeutigen elektronischen Kennzeichen gemäß §8 E-GovG,
4. Angaben zur beruflichen, postalischen und elektronischen Erreichbarkeit des Gesundheitsdiensteanbieters,
5. die Rolle(n) sowie besondere Befugnisse oder Eigenschaften des Gesundheitsdiensteanbieters,
6. die eindeutige Kennung (OID) und den symbolischen Bezeichner,
7. die Staatsangehörigkeit des Gesundheitsdiensteanbieters,
8. die zur Verschlüsselung von Gesundheitsdaten erforderlichen Angaben oder die elektronische Adresse, an der diese Angaben aufgefunden werden können,
9. die Angabe, ob es sich um einen ELGA-Gesundheitsdiensteanbieter handelt,
10. Angaben zur geografischen Lokalisierung des Gesundheitsdiensteanbieters,
11. Angaben über das Leistungsangebot des Gesundheitsdiensteanbieters,
12. die Bezeichnung jener Registrierungsstelle gemäß §2 Z4, von der die Daten in den eHVD eingebracht wurden, und gegebenenfalls die Bezeichnung der Herkunftsquelle der Daten sowie
13. das Datum der Aufnahme der Daten in den eHVD sowie das Datum der letzten Berichtigung.

5.2 Minimum Registry for healthcare professionals' Data Set

Taken from the JAseHN Guidelines[8] it can be expected that registries contain at least the following data elements which may be sufficient for satisfying the initial requirements for technical and semantic interoperability as well as the needs for the initial CBeHIS applications, with mandatorily providing:

- a unique identifier of the health professional (including a realm identifier such as an ISO3166 country code)
- a statement about the health professionals' credentials (professional authorisation, entitlement) and optionally:
  - the name and address of the health professional[9]
  - the health professional organisation identifier, name and address,
  - the issue and expiration date of the healthcare professional's credentials to practise,
  - the specialty may be recorded in line with national practice as the prescribing of some medicinal products may be restricted
- relationship to professional applications, networks, and identifiable entities (CBeHIS, ERN, etc.)

5.3 Registries for healthcare professionals' Structure and Data Set according to IHE Health Professional Directory Profile (Informational)

One possible interoperable solution for an exposed façade to a Registry for healthcare professionals is the Integrating the Healthcare Enterprises integration profile on a Health Professional Directory. This profile

[8] GUIDELINES on Electronic exchange of health data under the Cross-Border Directive 2011/24/EU

[9] Address of the health professional does not mean the private address of the health professional but a functional one, related to his practice as health professional.

defines a structure, data set, data exchange protocols, access means, and interaction patterns and is provided as information background within this guideline to outline a possible solution.

The table in section 8 Annex (Informational) lists the currently supported data elements with their specific optionality, encoding, and a brief functional description.

6. Closing Remarks

The present document describes to the current situation of Registries for healthcare professionals and builds a common understanding in MSs on Registries for healthcare professionals and what is needed for their interoperability for CBeHIS.

In order to establish sustainable principles and requirements for the interoperable retrieval of information from Registries for healthcare professionals in MSs for CBeHIS it is vital to receive information for the Art. 29 Working Party on the suitability of patient consent with a particular emphasis on patient consent enforcement and recommendations on what identity information needs to be exchanged and processed.

7. References

7.1 Legal references

- 2011/24/EU directive on the application of patients' rights in cross-border healthcare (cross-border directive)
- 2014/910/EU regulation on the electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation) and delegated acts
- 2015/296/EU Commission implementing decision establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of eIDAS regulation
- 2015/1501/EU Commission implementing regulation on the interoperability framework pursuant to Article 12(8) of eIDAS regulation
- 2015/1502/EU Commission implementing regulation on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of eIDAS regulation
- 95/46/EU directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- 2016/679/EU regulation on the protection of natural persons with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation)
- 2005/36/EU directive on the recognition of professional qualifications

7.2 Standards

- Health Informatics – Directory services for healthcare providers, subjects of care and other entities (ISO 21091:2013)

7.3 Content-related references

- eHealth Network documents
  - Organisational Framework for eHealth National Contact Points (OWA-NCPeH)
  - General Guidelines on electronic exchange of health data under cross-border Directive 2011/24/EU (Release 2)
  - Guideline on Patient Summary for unscheduled care (Release 2)
  - Guideline on ePrescription and eDispensation (Release 2)
  - 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*)
  - eID specific framework for eHealth Release 1
  - eID for eHealth: towards EU governance
  - eID for eHealth: towards coherence with the proposal of the Commission for eID regulation
- e-SENS document
  - WP4 Implication of eIDAS Regulation for eHealth (final draft available)
- PARENT document
  - "Methodological guidelines and recommendations for efficient and rational governance of patient registries"[10]
- CPME document
  - "Ensuring the secure use of telemedicine and e-health applications in an integrated Europe – Towards a Common Policy Agreement on Electronic ID Systems for Physicians" [11]
- Technical Delta Analysis on eID and related topics V0.6

8. Annex (Informational)

8.1 Excerpt from the IHE Health Professional Directory Profile

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
hpdProviderStatus	1.3.6.1.4.1.1937 6.1.2.4.1.1	Maintain status of provider in directory Values are defined in Table 3.58.4.1.2.3-1	Directory String	Case Ignore Match	S

[10] see http://patientregistries.eu/ and http://parent-wiki.nijz.si/

[11] see http://www.cpme.eu/cpme-policy-ensuring-the-secure-use-of-telemedicine-and-e-health-applications-in-an-integrated-europe-towards-a-common-policy-agreement-on-electronic-id-systems-for-physicians/

hpdProviderLanguageSupported	1.3.6.1.4.1.19376.1.2.4.1.2	Languages that the provider supports Recommended best practice is to use RFC 5646 [RFC 5646] which, in conjunction with ISO 639 [ISO639], defines two- and three- letter primary language tags with optional subtags. Examples include "en" or "eng" for English, "akk" for Akkadian, and "en-GB" for English used in the United Kingdom."	Directory String	Case Ignore Match, Case Ignore Substrings Match	M
hpdProviderBillingAddress	1.3.6.1.4.1.19376.1.2.4.1.3	The provider billing address field. It shall be represented in the format described in Section 3.58.4.1.2.4.	Postal Address	Case Ignore Match, Case Ignore Substrings Match	M
hpdProviderMailingAddress	1.3.6.1.4.1.19376.1.2.4.1.7	The provider mailing address field. It shall be represented in the format described in Section 3.58.4.1.2.4.	Postal Address	Case Ignore Match, Case Ignore Substrings Match	M
hpdProviderPracticeAddress	1.3.6.1.4.1.19376.1.2.4.1.4	The provider practice address field. It shall be represented in the format described in Section 3.58.4.1.2.4.	Postal Address	Case Ignore Match, Case Ignore Substrings Match	M
hpdMedicalRecordsDeliveryEmailAddress	1.3.6.1.4.1.19376.1.2.4.1.5	Electronic mailing address of provider where medical records can be sent	String	Case Ignore Match	S
memberOf	1.3.6.1.4.1.19376.1.2.4.1.6	Group to which provider is a member of. A provider can be a member of zero, one or many groups. The Provider Information Directory shall reuse existing LDAP functionality that offers memberOf as an operational attribute. See 3.58.4.1.2.2.4 for details.	DN	Case Ignore Match	M
hpdCredential	1.3.6.1.4.1.19376.1.2.4.1.8	Detailed Health related credentials earned by provider; DN to one or more credential entries in the HPDCredential object class	DN	Case Ignore Match	M
hpdProviderLegalAddress	1.3.6.1.4.1.19376.1.2.4.1.10	Provider Legal address (e.g., the address where the provider has registered the business, receives legal correspondence, other based on local convention) It shall be represented in the format described in Section 3.58.4.1.2.4.	Postal Address	Case Ignore Match, Case Ignore Substrings Match	S
hpdHasAServic e	1.3.6.1.4.1.19376.1.2.4.1.11	Reference to descriptions of electronic services supported by the Provider, See HPDElectronicServices.	DN	Case Ignore Match	M

Table 1- Table 3.58.4.1.2.2.1-1: HPDProvider Optional Attributes

-

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
credentialType	1.3.6.1.4.1.19 376.1.2.4.2.1	Type of Credential<degree, certificate, credential> Degree is not a valid type for Organizational Provider's credential	Directory String	Case Ignore Match	S
credentialName	1.3.6.1.4.1.19 376.1.2.4.2.2	Name of Credential, degree, or certification that belongs to provider. Follows the ISO21091 naming format as that of the HCStandardRole: credentialName@organization_domain_name where credentialName is the standard name of the credential, and organization_domain_name is the domain name of the organization for those credentials local to the organization, or credential@Locality where credential is the standard name of the structural role if applicable to the Locality (i.e., state).	Directory String	Case Ignore Match	S
credentialNumber	1.3.6.1.4.1.19 376.1.2.4.2.3	Credential Identifier Follows the ISO 21091 UID format: (Issuing Authority OID: ID) The issuing authority OID could be used to identify the issuing agency, state and country. ID is the national/regional identifier assigned to the provider's credential. E.g., a certificate number.	Directory String	Case Ignore Match	S

Table 2- Table 3.58.4.1.2.2.1-2: HPDProviderCredential Mandatory Attributes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
credentialDescription	1.3.6.1.4.1.19 376.1.2.4.2.4	Additional information on the credential	Directory String	Case Ignore Match	S
credentialIssueDate	1.3.6.1.4.1.19 376.1.2.4.2.5	Date when credential was issued to the provider	Date	Case Ignore Match	S
credentialRenewalDate	1.3.6.1.4.1.19 376.1.2.4.2.6	Date when credential is due renewal	Date	Case Ignore Match	S
credentialStatus	1.3.6.1.4.1.19 376.1.2.4.2.7	Values are defined in Table 3.58.4.1.2.3-1	Directory String	Case Ignore Match	S

Table 3 - Table 3.58.4.1.2.2.1-3: HPDProviderCredential Optional Attributes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
hpdMemberId	1.3.6.1.4.1.19 376.1.2.4.3.1	Unique Identifier for this Membership relationship	String	Case Ignore Match	S
hpdHasAProvider	1.3.6.1.4.1.19 376.1.2.4.3.2	Reference to Individual Provider	DN	Case Ignore Match	S
hpdHasAnOrg	1.3.6.1.4.1.19 376.1.2.4.3.3	Reference to Organizational Provider	DN	Case Ignore Match	S

Table 4 - Table 3.58.4.1.2.2.1-4: HPDProviderMembership Mandatory Attributes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
hpdHasAService	1.3.6.1.4.1.19 376.1.2.4.1.11	Only present if this electronic service information is specific to the Individual-Organization relationship	DN	Case Ignore Match	M
telephoneNumber	2.5.4.20	Only present when this telephone number is specific to the Individual-Organization relationship	TelephoneNumber	telephoneNumberMatch	M
facsimileTelephoneNumber	2.5.4.23	Only present when this facsimile number is specific to the Individual-Organization relationship	TelephoneNumber	telephoneNumberMatch	M
mobile	0.9.2342.1920 0300.100.1.41	Only present when this mobile number is specific to the Individual-Organization relationship	TelephoneNumber	telephoneNumberMatch	M
pager	0.9.2342.1920 0300.100.1.42	Only present when this pager number is specific to the Individual-Organization relationship	TelephoneNumber	telephoneNumberMatch	M
mail	0.9.2342.1920 0300.100.1.3	Used for general purpose email communication. Only present when this general purpose email is specific to the Individual- Organization relationship.	String	Case Ignore Match	M

Table 5 - Table 3.58.4.1.2.2.1-5: HPDProviderMembership Optional Attributes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
hpdServiceId	1.3.6.1.4.1.19 376.1.2.4.4.1	An identifier assigned by the provider directory whose purpose is to uniquely identify a unique Electronic Service Object.	String	Case Ignore Match	S
hpdServiceAddre ss	1.3.6.1.4.1.19 376.1.2.4.4.2	The electronic service address possibly in URI or email address form	String	Case Ignore Match	S

Table 6 - Table 3.58.4.1.2.2.1-6: HPDElectronicService Mandatory Attributes

Attribute	OID	Description	Syntax	Matching rules	Multi-Valued
hpdIntegration Pr ofile	1.3.6.1.4.1.19 376.1.2.4.4.3	A string which describes the integration profile. Values are defined through local configuration.	String	Case Ignore Match	M
hpdContentProf il e	1.3.6.1.4.1.19 376.1.2.4.4.4	A string which describes the content profile preferred in situations when content is being pushed to the service. Content not conforming to one of the specified content profiles may result in unpredictable results. When IHE content profiles are used, this is the formatCode. Values are defined through local configuration.	String	Case Ignore Match	M
hpdCertificate	1.3.6.1.4.1.19 376.1.2.4.4.5	Public Digital Certificate for this service	Binary	Not Applicable	M

Table 7- HPDElectronicService Optional Attributes

HPD Concept	LDAP Syntax	Object Class	Attribute within Object Class	Single/ Multi Valued	Optio nality	Comments
Unique Entry Identifier	String	inetOrgPerson	uid	S	R	RDN Format as defined by ISO 21091 Section 9.2 (Issuing
Provider “Identifiers”	String	HCProfessional	hcIdentifier	M	R	Format as defined by ISO 21091 (Issuing Authority:Type:I D:Status) Type values will be defined by national or regional organizations. Status is defined in Section 3.58.4.1.2.3

Provider Type	String	HCProfessional	hcProfession	M	R	The values will be defined by national or regional organizations. An example of possible types is the list of Individuals or Groups Values from the Healthcare Provider Taxonomy Published by the American Medical Association twice a year. An example of this document can be found at the following reference URL: http://www.adldata.com/Downloads/Glossaries/taxono my_80.pdf.
Provider Type description	String	inetOrgPerson	description	M	R	The definitions will be defined by national or regional organizations. See Provider Type for more information.
Provider Status	String	HPDProvider	hpdProviderStatus	S	O	Values found in Table 3.58.4.1.2.3-1
Provider Primary Name	String	inetOrgPerson	displayName	S	R	Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1
Provider Title	String	inetOrgPerson	title	S	O	Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1
Provider First name	String	inetOrgPerson	givenName	M	R2	Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1
Provider Middle Name	String	inetOrgPerson	initials	M	O	Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1
Provider Last Name	String	inetOrgPerson	sn	M	R	Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1
Provider Known names	String	inetOrgPerson	cn	M	R	Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a 3.24.5.2.3.1
Provider Language Supported	String	HPDProvider	hpdProviderLanguageSupported	M	O	Supported written or spoken language for a person. Values for this attribute type MUST conform to the definition of the Accept- Language header field defined in [RFC2068] with one exception: the sequence "Accept- Language" ":" should be omitted. The following example indicates that this person supports French, supports British English 80%, and general English 70%. (e.g., fr, en- gb;q=0.8, en;q=0.7)
Provider Gender	String	Natural Person	gender	S	O	Using Natural Person auxiliary class as defined in RFC 2985

Provider medical records deliver email address	String	HPDProvider	hpdMedicalRecordsDeliveryEmailAddress	S	O	Intended for sending medical records via email
Provider e-mail address	String	inetOrgPerson	mail	M	O	Intended for general purpose email communication
S-MIME Certificate	Binary	inetOrgPerson	userSMIMECertificate	M	O	RFC2798: PKCS#7 SignedData used to support S/MIME; typically used for encrypting MIME messages over an email. Other purposes and constraints can be found by looking inside the certificates.
Signing Certificate	Binary	HCProfessional	hcSigningCertificat e	M	O	Public key and certificate for the user's non- repudiation signing certificate used for health transactions
User Certificate	Binary	inetOrgPerson	userCertificate	M	O	RFC2256: X.509 user certificate for general purpose use; purposes and constraints can be found by looking inside the certificates
Electronic Service URI	String	groupofURLs	labeledURI	M	O	Points to a service entry in a systems directory or to a webservices definition page defining the end points of services.
Creation Date	Date	N/A	createTimestamp	S	R	This is an operation attribute that LDAP directory server maintains to capture the time when an entry was created.
Last Update Date	Date	N/A	modifyTimestamp	S	R	This is an operation attribute that that LDAP directory server maintains to capture the time when an entry was modified.
Provider Facility Name	String	inetOrgPerson	physicalDeliveryOfficeName	M	R2	This attribute contains the facility name that a postal service uses to identify a provider's facility.
Provider Mailing Address	Postal Address	HPDProvider	hpdProviderMailingAddress	M	R2	Mailing address
Provider Billing Address	Postal Address	HPDProvider	hpdProviderBillingAddress	M	O	Business billing or legal address
Provider Practice Address	Postal Address	HPDProvider	hpdProviderPracticeAddress	M	R2	Practice or Service address
Provider Practice Organization	DN	HCProfessional	HcPracticeLocation	M	O	DN of organization the provider practices
Provider Business Phone	Telephone Number	inetOrgPerson	telephoneNumber	M	R2	As per ITI TF-2a:3.24

Provider Mobile Phone	Telephone Number	inetOrgPerson	mobile	M	R2	As per ITI TF-2a:3.24 Business Mobile
Provider Pager	Telephone Number	inetOrgPerson	pager	M	R2	As per ITI TF-2a:3.24
Provider Fax	Facsimile Telephone Number	inetOrgPerson	facsimileTelephone Number	M	R2	
Provider "Credential"	DN	HPDProvider	hpdCredential	M	O	Detailed Health related credentials earned by provider
Provider Specialty	String	HCProfessional	hcSpecialisation	M	O	A major Grouping i.e., Dermatology, Oncology, Dental, Internal Med. (Issuing Authority: Code System: Code: CodeDisplayNam e) Populate with ISO 21298 defined medical specialties. May also be populated with other specialties specified by jurisdiction or organization
Provider Relationship	DN	HPDProvider	memberOf	M	O	Groups to which this provider belongs; In search scenarios, it is desirable for a Provider Information Consumer to be able to determine which organizations this individual provider is a member of.
Legal Address	Postal Address	HPDProvider	hpdProviderLegalA ddress	S	O	
Electronic Service	DN	HPDProvider	hpdHasAService	M	O	

Table 8 - Table 3.58.4.1.2.2.2-1: Individual Provider Mapping

HPD Concept	LDAP Syntax	Object Class	Attribute within Object Class	Single/ Multi Valued	Optio nality	Comments
Unique Entity Identifier	String	uidObject	uid	S	R	RDN Format as defined by ISO 21091 Section 9.2 (Issuing Authority Name:ID)
Org Identifiers	String	HCRegulatedOrganization	hcIdentifier	M	R	Format as defined by ISO 21091 (Issuing Authority:Type:ID: Status) Type values will be defined by national or regional organizations. Status is defined in Section 3.58.4.1.2.3
Organization known names	String	Organization	O	M	R2	Organization known name. Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1
Organization Name	String	HCRegulatedOrganization	HcRegistere dName	M	R	The legal name of the entity as registered with the health care regulating authority. Use of language tag and HL7 Name Data Type (XCN) as per ITI TF-2a: 3.24.5.2.3.1

Org Type	String	Organization	businessCategory	M	O	The values will be defined by national or regional organizations. An example is the list of Non Individual Values from the Healthcare Provider Taxonomy Published by the American Medical Association twice a year. An example of this document can be found at the following reference URL: http://www.adldata.com/Downloads/Glossaries/taxonomy_80.pdf.
Org Type Description	String	Organization	description	M	O	The description shall be defined by national or regional organizations. See Org Type for more information.
Org Status	String	HPDProvider	hpdProviderStatus	S	O	Values found in Table 3.58.4.1.2.3-1
Org Contact	DN	HCRegulatedOrganization	ClinicalInformationCon	M	O	Clinical contacts; DN to HCProfessional entry
Org Practice Address	Postal Address	HPDProvider	hpdProviderPracticeAddress	M	R2	Practice or Service address
Org Billing Address	Postal Address	HPDProvider	hpdProviderBillingAddress	M	O	Business billing or legal address
Org Mailing Address	Postal Address	HPDProvider	hpdProviderMailingAddress	M	R2	Mailing address
Org Credentials	DN	HPDProvider	hpdCredential	M	O	Detailed Health related credentials earned by provider; Degree is not a valid type for Organizational Provider
Provider Language Supported	String	HPDProvider	hpdProviderLanguageSupported	M	O	Language that the organization supports. Values for this attribute type MUST conform to the definition of the Accept-Language header field defined in [RFC2068] with one exception: the sequence "Accept- Language" ":" should be omitted. The following example indicates that this person supports French, supports British English 80%, and general English 70%. (e.g., fr, en- gb;q=0.8, en;q=0.7)
Org Specialty	String	HCRegulatedOrganization	HcSpecialisation	M	O	(Issuing Authority: Code System: Code: CodeDisplayName) Populate with ISO

Electronic Service URI	String	groupofURLs	labeledURI	M	O	Points to a service entry in a systems directory or to a webservices definition page defining the end points of services.
Signing Certificate	Binary	HCRegulatedOrganization	HcSigningCertificate	M	O	Public key and certificate for the user's non- repudiation signing certificate used for health transactions
Organization Certificate	Binary	HCRegulatedOrganization	HcOrganizationCertificates	M	O	Used for storing health care organization certificates; Certificate purposes and constraints can be found by looking inside the certificates.
Org Business Phone	Telephone Number	Organization	telephoneNumber	M	R2	
Org Fax	Facsimile Telephon	Organization	facsimileTelephoneNum	M	R2	
Provider Relationship	DN	HPDProvider	memberOf	M	O	Groups to which this provider belongs; In search scenarios, it is desirable for a Provider Information Consumer to be able to determine which organizations this organization provider is a member of.
Creation Date	Date	N/A	createTimestamp	S	R	This is an operation attribute that LDAP directory server maintains to capture the time when an entry was created.
Last Update Date	Date	N/A	modifyTimestamp	S	R	This is an operation attribute that that LDAP directory server maintains to capture the time when an entry was modified.
Electronic Service	DN	HPDProvider	hpdHasAService	M	O	
Legal Address	Postal Address	HPDProvider	hpdProviderLegalAddress	S	O	

Table 9 - Table 3.58.4.1.2.2.3-1: Organizational Provider Mapping

HPD Concept	LDAP Syntax	Object Class	Attribute within Object Class	Single/ Multi Valued	Option ality	Comments
Relationship Name	String	groupOfNames	cn	S	R	Name of the relationship group. The name value is not defined, but it makes sense to derive it from the owning organization entry.

Owning organization	DN	groupOfNames	owner	S	R2	Reference to the organizational provider that owns this group, i.e., superior to the members of this group. Note that the groupOfNames object class defines this attribute as being optional
Member providers	DN	groupOfNames	member	M	O	References to organizational or individual providers that are members of this group, i.e., subordinate to the group owner

Table 10 - Table 3.58.4.1.2.2.4-1: Relationship Mapping

9. Appendices

9.1 Definitions

CONCEPT	DEFINITION
CBeHIS	The generic services are the necessary implementation of data exchange at country level (generic services), plus the core services at EU level. These together enable the provision of Cross Border eHealth Information Services (CBeHIS).
CEF eHealth DSI	is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF). eHDSI sets up and starts deploying the core and generic services, as defined in the CEF, for Patient Summary and ePrescription.
Communication Gateway	MS system that manages CBeHIS transactions with other MS and which connects to the NI. It is an entry/exit point from the MS, acting on behalf of a HP and citizen (at a Point of Care) that assures the exchange of patient's medical data in a controlled environment.
Compliance Establishment Process	A well-defined set of activities and evidences 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 univocally identified and his data may be accessed.
Country-B	The country of treatment i.e. where cross-border health care is provided when the patient is seeking care abroad.
Framework	Is 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 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[12] identification and health care records in MS
NCP	National Contact Point as referred in Article 6 of the 2011/24/EU

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

	Directive
NCPeH	National Contact Point for eHealth, that may act as an organization and technical gateway for the provision of eHealth Cross-Border Information Services
NCPeH Deployment	Set of activities aiming to evidence the 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 the service to the citizens and health professionals
NCPeH Preparation	Set of activities aiming to set up an NCPeH
Organisational Framework	Define core characteristics, duties and responsibilities of an NCPeH
PoC	A Point of Contact is a location where an EU citizen may seek healthcare services. It can be a hospital, a pharmacy or any other point of the healthcare system of Country B.
Requirement	Definition of relevant needs (business, functional, non-functional, technical and technological) for system specification and implementation