HEALTHeID

eIDAS – OpenNCP
Connector for eHealth

HEALTHeID Briefing Document

From Business to Use Case

Document Information:

Document status:	Draft
Document Version:	2.2
Date	September 06th, 2019
Authors:	Zoi Kolitsi , Legal and Policy Lead, AUTH Alberto Zanini, ARIA Diogo Martins, João Cunha, SPMS
Acknowledgements	The work in the Legal track of HEALTHeID has been supported by Petra Wilson, external expert; the Note on Patient Consent has been in addition supported by Klara Jirakova, HEALTHeID Transferability Lead. The work in the Business to the Use Case of HEALTHeID has been supported by Alberto Zanini and reviewed by Diogo Martins and João Cunha; All HEALTHeID partners have contributed to the discussion.

.

TABLE OF CONTENTS

1. Introduction to the document 3
2. Legal and Policy Context 3
3. Legal and Policy Requirements for HEALTHeID 5
(i) Alignment of Concepts and Definitions 5
(ii) Patient identification 6
(iii) Establishment of an on-line service context 7
(iv) Privacy and Data Protection by design 8
(v) Patient empowerment through eIDAS HEALTHeID 9
4. HEALTHeID reflections on patient oriented on-line services 9
4.1. On-line access to PIN 10
4.2. Patient Consent on-line service 11
4.2.1. Patient Consent Storage 12
4.2.2. Consent Data to be stored 13
4.3. Patient Identifier Service 13
5. HEALTHeID Vision 15
6. The need - ID for eHealth 17
7. The opportunity - eIDAS 18
8. The idea - eIDAS for eHEALTH 18
9. Exploiting HEALTHeID: a use case 18
ANNEX I. HEALTHeID Patient Information Notice 20
ANNEX II: PATIENT CONSENT services 22

1. Introduction to the document

This document has been created as part of the briefing package for -HEALTHeID participating Member States that wish to adopt and implement HEALTHeID solutions.

This document focuses on the legal aspects of the vision served by HEALTHeID.

HEALTHeID aims at developing, testing and delivering to the European Commission (EC) and the Member States (MS) a reference implementation of an HEALTHeID Connector (HeID Connector), at Technology Readiness Level (TRL) 7, linking the national OpenNCP-based National Contact Points for eHealth (NCPeH) to the eIDAS node and the relevant attribute providers in 4 core MS. The objective is to ensure that the implementation will be transferable to other national scenarios. Alignment, both technical and timewise with the deployment of the eIDAS nodes of the core countries will be maximized.

All the resulting HeID Connector solution components will be made available as Open Source Software to the eHDSI owner and the National Contact Points for eHealth. These, as well as additional modifications needed to the current OpenNCP implementation, will be described in a change proposal and will be submitted to the eHDSI owner. Early collaboration with DG SANTE, DG DIGIT and DG CONNECT and the eHDSI community is therefore sought.

The exploration on the topic of electronic identification and authentication is not new. It was first addressed in the epSOS Large Scale Pilot (LSP), with a view to providing a practical solution to running the LSP. The co-operation with STORK at that time through the STEPS initiative did not come to fruition of a realistic approach, mainly because the scenarios explored by STORK did not resonate with the on-site presence of the patient and the cross border transmission of patient identifiers submitted by the health care professional, on behalf of the patient. As a result, epSOS did not address the issue of electronic patient identification. This topic was explored in e-SENS, as part of its eHealth pilot, and the relevant contributions were invaluable in understanding the implications of eIDAS for cross boarder eHealth; this document builds further on that work.

2. Legal and Policy Context

The main legal foundation of the eIDAS specific framework for eHealth is anchored primarily on three legal instruments:

The eIDAS Regulation, consistent with cross cutting policies, promotes a paradigm where the citizens/patients may identify and authenticate themselves using their national eID credentials via a trustnetwork of national eIDAS nodes; once robustly identified and authenticated, the citizen may access cross border on-line services and manage and control access to their own personal documents and data, including health data. This will

be mediated by national legislation which may be in place to define the type of health data that patients may access electronically.

The Regulation enables the use of electronic identification means and trust services (i.e. electronic signatures, electronic seals, time stamping, registered electronic delivery and website authentication) by citizens, businesses and public administrations to access on-line services or manage electronic transactions. Importantly, it ensures that appropriate eID can have the same legal value as wet signature in cross border transactions and makes mutual recognition of electronic identities (eIDs) mandatory as of autumn -2018. The Regulation is a self-contained legal framework in its own right , in other words it contains all elements that are necessary to create the needed legal certainty for citizens and digital service providers in cross border encounters.

The GDPR is applicable to HEALTHeID, in as far as on-line services made available to the person/patient are concerned. It is not the intention of HEALTHeID to replace discussions taking place in the eHDSI community, beyond considering usability and technical implementation choices, when these become on-line services accessible directly by the patient and elaborate relevant proposals.

Directive 2011/24 in its Article 14 establishes the mechanisms for cooperation on and the exchange of information among Member States working within a voluntary network, i.e. the eHealth Network, connecting national authorities responsible for eHealth designated by the Member States. The topic of electronic identification and authentication has been extensively discussed within the **eHealth Network**, and features strongly in eHealth Network's MWP 2018- 2021.

Single Digital Gateway Regulation 2018/1724 which establisheds a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services is also applicable. It will require that infromation about the Health eID solutions is available to Euopean citizens and also that Member States collect data about use of the solution to report to the Commission

In addition to these 3 main legal foundations the EC "**Communication on enabling the digital transformation of health and care in the Digital Single Market**; empowering citizens and building a healthier society" lays out three priorities to be followed in the coming years:

Citizens' secure access to electronic health records and the possibility to share their records across borders, and the use of e-prescriptions. (Priority 1)

- Supporting data infrastructure, to advance research, disease prevention and personalised health and care in key areas included rare, infectious and complex diseases. (Priority 2)

- Facilitating feedback and interaction between patients and healthcare providers, to support prevention and citizen empowerment as well as quality and patient-centred care, focussing on chronic diseases and on a better understanding of the outcomes of healthcare systems. (Priority 3)

The Multi-Annual Work Plan (MWP) is also focused on topics relevant to the above DTHC DSM priorities, including patient access, use of data and digital health literacy of patients, mHealth apps, telehealth and patient-generated data; innovating use of health data; enhancing the continuity of care (e.g. stimulating and supporting the adoption of eHDSI services) and overcoming implementation challenges (e.g. interoperability & standards, skills, trust, security and privacy).

All 3 priorities would require robust citizen/patient identification and authentication and eIDAS solutions for cross border access and management of citizen own health data. Citizen empowerment, enabled through eIDAS, should be therefore viewed within a broader consideration, beyond the current limited scope of cross border exchange for emergency situations and needs to inform the design of the HeID Connector in what concerns the ability of the citizens to act upon sharing their health data.

3. Legal and Policy Requirements for HEALTHeID

These have been grouped under the following headings:

(i) Alignment of Concepts and Definitions

The definitions provided in the eIDAS Regulation differ in their articulation from those of the eHDSI Identity Management Specification, however they are not in effect misaligned. It is important, however, to clarify that patient identifiers serve primarily to locate the person in the national eHealth system, while electronic identification of the person aims at identifying and authenticating an individual. Both aspects are necessary for realizing patient enabled on-line cross border eHealth use cases.

nFR 01: The HEALTHeID Connector implementation process must adopt definitions and concepts as described in the eIDAS Regulation and translate them appropriately to the cross border eHealth context.
nFR 02: In addition to the eIDAS workflow, the HEALTHeID Connector must provide for completing the patient identification through capturing or mapping the identification data to the patient identifier.
nFR 03: Any additional step in the eIDAS workflow should be carefully designed and verified as to its ability to preserve the LoA enabled by the eID scheme.

(ii) Patient identification

The three situations identified in the relevant Deloitte study (see section 3) will impact HEALTHeID in different ways:

- Where a notified, nationally issued eID scheme with unique identifier that is used as the patient ID number for eHealth use cases will be employed by country A, citizen and patient identification may collapse into one single step.
- The same applies in situations where a notified, nationally issued sector specific eHealth eID scheme with sector specific patient ID number for eHealth use cases will be employed.
- In all other cases, patient identification and authentication in cross border eHealth may be generally described as a two step process: in the first step, the citizen involved in a cross border eHealth encounter must be authenticated under eIDAS; subsequently, the citizen must be further identified *as a patient*, by means of his/her patient identifier which links the person unequivocally to his/her electronic health documents and entitlements in the national health care system.

HEALTHeID should adopt and provide solutions for the third general scenario. e-SENS explored the option of "injecting" patient identifiers as additional attributes into the eIDAS SAML profile; the approach was however presented significant organizational and legal constraints which were not overcome at that time.

HEALTHeID should therefore seek alternatives of equal legal strength to collecting and sharing this important identification attribute. For example:

- Where a Country A is in the position to technically and legally map the person identifiers to the patient identifiers, this mapping will become a national level action,
- Where such mapping is not possible or the preferred approach, the authenticated citizen may be prompted to submit his/her own patient identifier, electronically on-line, replacing the respective action performed by the health professional.

In both cases above, trust is established by the trust framework within the network of NCPeHs. In the case of patient provided information, all checks and controls applied today for HP enabled entries are relevant. In addition this on-line service is provided by the Service provider (SP) to the patient, following eIDAS authentication of the individual it can therefore enjoy the legal effects of the eIDAS.

nFR 04: the HEALTHeID Connector should be designed and implemented in a way to cover all possible national situations; the default settings should therefore allow for a MS with a non health specific notified eID scheme and no possibility

to map person to patient identifiers to employ the HEALTHeID HeID Connector.

(iii) Establishment of an on-line service context

Recital 12 describes the aim of the eIDAS Regulation as being "to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible". Recital 14 further explains that "the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation."

In the present eHDSI use cases, there are no direct on-line services provided to the patient e.g. in the form of accessing data, providing consent, donating data for research etc. eIDAS, on the other hand, assumes interaction between three parties: a **Citizen** wishing to access a cross border service and therefore interacting with a ***Service Provider*** operating in a country other than his/her country of affiliation, the latter being a relying party for identifying and authenticating this citizen to his respective **national eIDAS node**.

In the eIDAS realm, it is therefore essential to recognize and map three roles: the citizen/consumer in country A seeking to receive a service from a Service Provider in country B, who is "the relying party" i.e. relies upon its national eIDAS node (of country B) for identifying and authenticating the individual requesting the service. In the current cross border eHealth services of unplanned care, we can map these roles as follows:

- the patient from country A, is seeking to receive
- **an (on-line) service** i.e., enable access to PS or ePrescription to a HP in country B
- from the healthcare portal **in country B**, who is then "**the relying party**" i.e. relies upon the
- **national eIDAS node** of country B for identifying and authenticating the individual.

It should be however noted that in the current eHDSI use cases, the patient does not receive an on-line service. While it is recognized that the design and implementation of such services is out of scope of HEALTHeID, the HEALTHeID Connector would be void without an on-line service directed by the Service Provider to the patient.

nFR 05: the HEALTHeID Connector should be designed and implemented with the aim to enable patient access to an on line service. At least one such service should be identified and linked to the HEALTHeID use case.

(iv) Privacy and Data Protection by design

These requirements relate primarily to the demo on-line services developed by HEALTHeID. Where relevant, this discussion should be aligned with relevant work under the eHDSI.

Patient Information Notice (PIN) on-line service: The patient driven approach to identification and triggering of the service will require an information notice the same content as the eHDSI model PIN, supplemented with information on identification data, but with different usability considerations (e.g. text presentation, display and verification of having been informed).

HEALTHeID recommends a layered information approach, providing the full necessary content but, through links to the respective sections of the model PIN. This should be in addition to and is not meant to replace the current MS approaches to PIN.

On-line consent service: Additional requirements below relate to situations where such a service is relevant (see also section 3.2). We may distinguish between two groups of MS – those relying nationally on patient consent and those relying on a different legal bases provided for in GDPR In a cross-border exchange, we may therefore encounter 4 different situations:

- Both involved MS rely on Patient consent
- None of the involved MS relies on Patient Consent
- MS A relies on Patient Consent, MS B does not rely on Patient Consent
- MS A does not rely on Patient Consent, MS B relies om Patient Consent

In addition, we must differentiate between two elements of consent:

a. *CONSENT to Patient Summary (PS)/ePrescription (eP) being accessed and viewed by the healthcare professional in country B according to country B provisions*
b. *CONSENT to a record of the care received in country being created and stored in that country and according to country B provisions. This stored record will be able to be accessed by the patient in country A.*

nFR 06: A specific health care encounter context must be established; the patient must provide informed consent in relation to this specific context. This context should be also articulated into text information made available to the patient in advance to providing consent.
nFR 07: The strong patient identification process should be extended to also include specific patient consent for disclosure to the health care encounter and for a specified period of time

nFR 08: The HEALTHeID Connector should provide also for linked eIDs as in the case of children linked to a guardian, or adults over whom a power of attorney exists.

(v) Patient empowerment through eIDAS HEALTHeID

The scope and mandate of HEALTHeID is to implement, test and validate an appropriate solution for electronic patient identification, suitable for immediate deployment in the eHDSI, by the parties involved, which are the national NCPeH, without an obligation to address situations beyond this scope. Nevertheless, in selecting the proper implementation choice, scalabilty to use cases that will be supported as part of the eHealth Network MWP should be also considered.

nFR 09: Technology under the patient's control (such as an eHealth App on a smart phone) must be considered for the implementation of the above workflows.

nFR 10: HEALTHeID should address citizen empowerment enabled through eIDAS, within a broader consideration, beyond the current limited scope of cross border exchange for emergency situations.

nFR 11: The design of the HEALTHeID Connector should address, as a minimum, the requirements of the first priority of the Digital Transformation of Health and Care (DTHC) for enabling the citizens to act upon sharing of their records and be extendable to all three priorities in the future.

4. HEALTHeID reflections on patient oriented on-line services

Why is HEALTHeD dealing with on line patient oriented services? Simply because eIDAS electronic identification becomes meaningful only if the person being electronically identified towards a SP to receive an on-line service by this SP.

It is not the objective of HEALTHeID to deliver such on-line services, beyond what is necessary for demonstrating the HEALTHeID Connector and its functionality. In doing so, HEALTHeID is entering in a space of policy discussions taking place in the CEF projects and the eHMSEG and its subgroups. A process for alignment of concepts and frameworks is needed.

How should HEALTHeID proceed in creating patient oriented on-line services for demonstration purposes? HEALTHeID has explored how the concept of eIDAS based electronic identification may be transferred to the current cross border context of Patient Summary and ePrescription services and has reached the following preliminary conclusions.

1. Irrespective of chosen legal basis for access to patient data in a MS, the patient must be informed on the purpose of the processing (Article 5, 13, 14 of the GDPR) through a Patient/Privacy Information Notice (PIN). Providing an on-line PIN service is therefore a potential on-line service relevant to all MS;
2. Identification attributes provided by Country of Affiliation (Country A) may or may not include a patient identifier. In the latter case the patient identifier must be uniquely associated to the person identified and authenticated. Providing a functionality for patient entering own patient identifier on-line (a function today performed by the Health Professional) could be a second on-line service that would be relevant to certain MS;
3. Patient providing on-line consent in country B is an additional service identified; this service would be relevant to certain MS.

In summary:

HEALTHeID should as a minimum provide an on-line PIN service. This PIN itself will include also information on the purpose and use of identification data and as such represent an extension of the scope as considered today in the model eHMSEG adopted PIN. This will be the **HEALTHeID baseline on-line service**. It will be piloted by HEALTHeID MS and will be proposed for adoption by all MS.

Additional services to be implemented, piloted within HEALTHeID and demonstrated for adoption by MS beyond HEALTHeID will be:

- On-line patient identifier service
- On-line patient consent service proof of concept

The questions that need be resolved for these services are addressed in the following sections:

4.1. On-line access to PIN

This service entails display of the PIN as it has been localized by each country B and an indication by the patient that she/he has read and agreed to the conditions described in the PIN e.g. through selecting between “cancel” and “continue” with the provision of the services.

The ***appropriate place in the workflow*** for displaying the PIN is after or at the same time as patient authentication.

The ***appropriate content*** of the PIN, should not diverge from that of the model PIN, in what concerns its substance. It should be however noted that the needs addressed by the HEALTHeID PIN are different, hence the approach in the design is different in the following ways:

- The model PIN is 5 pages long (even if experience from Luxembourg shows that it may be reduced when localized e.g. to 4 pages). It is meant to be made public through the eHDSI and national NCPeH websites and may be read by the traveling citizens at any time before or during their cross border encounter; the HEALTHeID PIN is short and it provides a link for further information and it is meant to be read by the person agreeing to the terms of the requested service on site and in the middle of an on-line process.
- The model PIN states "*After being presented with the PIN by the health professional, the patient acknowledges that he/she is confirming the lawful processing of data by clicking on an appropriate confirmation button (see above information on consent and other legal basis for the processing of personal data*)". In practice, this cannot be recorded today as a patient enabled action but rather as a HP action. In HEALTHeID, it will be indeed the patient clicking the box "continue" or similar indicating agreement with the terms under which the service is offered.
- The model PIN does not include information on identification attributes.
- The HEALTHeID PIN should be understood as an on-line service that will become relevant once the HEALTHeID approach is adopted and - if so decided- in future waves of the CEF implementation.
- The model PIN makes the suggestion that as a minimum an English version of the PIN should be available in Country B. HEALTHeID has adopted this recommendation.

The patient driven approach to identification and triggering of the service will require a PIN of the same content as the model PIN, supplemented with information on identification data, but with different usability considerations in terms of length of the text, display and verification of having been informed.

The ***appropriate presentation of the PIN*** is therefore a layered information approach, providing the minimum necessary content but, through links to the respective sections of the model PIN, as this has been localized by each MS, make available the whole set of information (see more, see less options). Please refer to **ANNEX I for the HEALTHeID PIN** and its links to sections of the model PIN.

4.2. Patient Consent on-line service

We may globally distinguish between two groups of MS – those relying nationally on patient consent and those relying on a different legal bases. In a cross-border exchange, we may therefore encounter 4 different situations:

- Both involved MS rely on Patient consent

- None of the involved MS relies on Patient Consent
- MS A relies on Patient Consent, MS B does not rely on Patient Consent
- MS A does not rely on Patient Consent, MS B relies on Patient Consent

In addition, we must differentiate between two elements of consent:

a. CONSENT to Patient Summary/ePrescription being accessed and viewed by the healthcare professional in country B
b. CONSENT to a record of the care received in country being created and stored in that country and according to country B provisions

The ***appropriate place in the workflow*** for obtaining consent where appropriate is immediately after displaying the PIN.

Please refer to **ANNEX II for the patient consent PIN and form**.

4.2.1. Patient Consent Storage

HEALTHeID Solutions should cater to all possible situations and should not clash with national guidance on the appropriate legal basis for data processing in the health care sector.

Variation in national guidance on the appropriate legal basis for data processing in the health sector in different MS is not expected to be a problem for transferability of HEALTHeID to different national legal environments. Further consolidating the accompanying model PIN with HEALTHeID will make the solution coherent by design.

On the basis of the above, we may describe Patient Consent Storage for each combination of these situations:

TABLE I: Patient Consent Storage

Country A	**Country B**	**HEALTHeID Consent (a)**	**HEALTHeID Consent (b)**
Patient Consent as a Legal Basis		**Patient Consent to access data**	**Patient consent to process data in country B**
YES	YES	This part of consent (a) should be collected and stored in country B. Storage of consent is necessary for audit purposes. Country B should be able to prove if requested that consent was obtained.	This part of consent (b) is collected in country B and stored in country B. Country B collects this consent as a data provider for foreign citizens.
NO	NO	Consent (a) is not collected	Consent (b) is not collected
YES	NO	Country B collects and stores consent (a) on behalf of country A	Consent (b) is not collected

		and for Audit purposes; it may be made available to country A if requested.	
NO	YES	Country B collects consent (a) and stores locally for audit purposes.	Thiis part of consent (b) is collected in country B and stored in country B. Country B collects this consent as a data provider for foreign citizens.

4.2.2. Consent Data to be stored

Where the legal basis for processing data is consent, then the data processor/controller must be able to show that the requisite consent was actually obtained, accordingly the consent must be stored. It should be noted that the processor/controller relying on consent should also be able to demonstrate that the consent was informed, accordingly the patient information notice should also be stored. The record of consent stored should include:

- Evidence that consent has been provided
- The encounter ID for which consent was provided
- A time stamp of when the action took place

A reference to uniquely identified version of the information document (PIN) used for informing the patient on the purpose of the processing.

4.3. Patient Identifier Service

This service will in principle replace today's health professional action of inserting the partient identifier by the patient him/herself. It will also replace today's manual inspection and verification of patient identifier against patient identification details by an automatic process performed by the HEALTHeID solution.

The assumption currently employed in the eHDSI is that there is suffient overlap between the attributes in the patient identification document and the attributes returned by country A, associated to the patient identifier to allow for such a verification, for all MS. HEALTHeID is also operating on the assumption, while the mapping of attributes for the core MS as follows:

	CZECH REPUBLIC	GREECE (AMKA)	ITALY	PORTUGAL
eIDAS MDS	Patient Identifier			
Current Family Name(s)	present	present	present	present
Family name **Current First Name(s)**	present	present	present	present
Date of Birth	present	present	present	present
Uniqueness Identifier	different from Patient Identifier	different from Patient Identifier	different from Patient Identifier	different from Patient Identifier

The HEALTHeID Connector will provide the functionality for comparing the eIDAS data set and patient identifier data sets received and issue a recommendation on the matching of attributes. It is however the ultimate responsibility of country A to ensure that the clinical document forwarded to country B corresponds to the patient that has been identified.

5. HEALTHeID Vision

Cross border eHealth can benefit greatly from the adoption of eIDAS based electronic identification and authentication of patients, leveraging on the high level of legal certainty and robust liability framework introduced by eIDAS and also the GDPR. The operation of the ERNs is also paving the way for networked, patient centered cross border healthcare, while enabling technologies will further contribute to the vision of European citizens that are enabled to decide upon and manage access to their own data.

At the same time MS and the European Commission have been investing in the sustainable deployment of cross border eHealth services, starting from the successfully piloted CBeHIS involving the cross border access of Patient Summaries and ePrescription.

The HEALTHeID vision carefully balances the need to safeguard and avoid disruption of the current CEF eHDSI infrastructure and services, against the need to migrate towards better integrated cross border eHealth in the DSM realm. The HEALTHeID Vision builds on the following universal principles underlining both the present and the projected future of cross border eHealth.

I. Citizens - Patients

Our electronic identities, mutually recognized under the eIDAS Regulation, are our passport to enjoying access to digital services in all sectors, offered anywhere to citizens living and working anywhere in the EU. The potential impact for health care is immense, as this enables a multitude of services, not least those involving sharing of health data across borders and, as envisioned in the EC Communication, can further shape the future of health and care provision.

Strong electronic identification and authentication for the citizen is necessary for enjoying the potential benefits, it may however not be enough. The citizens must be also identifiable in their national eHealth infrastructures, via their patient identifiers, which may differ from their citizen identifiers. While the situation regarding general vs specific patient identifiers varies amongst MS, it is important to consider that, for health care purposes, electronic identification involves the identification and authentication of a citizen as well as identification of the patient, irrespective of whether these need be two seperate steps or a single step, i.e., where general purpose identifiers are used for health care purposes or where health specific eID schemes have been notified.

HEALTHeID is about patient identification, in compliance with but going beyond the strict eIDAS scope.

II. Patient empowerment

We may identify three main process components, leading to lawful data sharing:

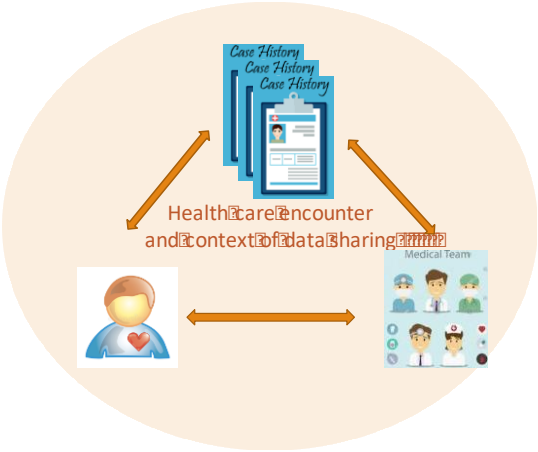
(i) Identification and Authentication of the *patient* towards the SP

(ii) Establishment, by the SP, of the context of the data sharing, i.e., correlation of the patient, involved HP(s) and health data to be shared in a uniquely identified health care encounter

(iii) Enabling HP access to the document through context specific and, where necessary, informed patient consent

The first component involves a generic eIDAS information flow, supplemented as needed by health specific patient identification.

The second component is not eIDAS driven, but is necessary to establish the specific situation and context of data sharing to which consent of the identified patient will be provided to. For establishing such a context, it is necessary to link the patient (eID), the patient identifier (if different) in the country where the health data is, the health professional and the data to be shared and associate it to the specific health care encounter.



The third component closely couples the eIDAS identification of the individual to the patient agreement on the conditions of the on-line service offering. This step then establishes the legal pre-requisites for lawful data sharing.

This interaction described above is not a scenario in itself but a universal, flexible foundation to integrate and operate strong eID within and aside from the eIDAS eID framework and its associated trust services.

HEALTHeID solutions will leverage on the potential to match the strong AAL, made transparent and secured by the eIDAS workflow to conclude a fully regulated-by-design process leading to lawful access to health data.

III. Interaction Patterns

In our current approach employed by CBeHIS, the two collaborating NCPeHs in country B and country A, assume roles of Data Consumer (DC) and Data Provider (DP), respectively. In future generalized scenarios, the DP can be any entity that stores and manages health data in any country, whereas the role of DC can be with one or more entities that consume health data in one or more other countries. This case, is already today the real life situation within the members of the ERNs, where DPs from one or more countries share

data with DCs in one or more countries, on the basis of patient consent, specific to the context of the ERN function and processes.

The authorization for access to medical information of a particular patient by a specified health professional or in a more general case a specified care team, enables a variety of future exchange patterns with the SPs as trusted anchor points, for example,

- Patient pushing medical information to a particular HP or care team, based on an **HP/team locator** (i.e. patient needs to "locate" the HP/care team-SP enables the process of locating the DC);
- Enabling a specific HP to pull medical information for a particular patient based on an **information locator** (i.e. the HP need to "locate" the electronic clinical document they need to access-SP enables the process of locating the DP who will then locate the requested clinical document)
- Enabling the integration of further, potentially patient-controlled, **data sharing scenarios** (e.g. a rare disease patient enabling access to his records by a multinational care team defined within an ERN, or rare disease patient enabling access to parts or the whole of his data for research purposes by the members of the scientific ERN community).

A HEALTHeID patient driven approach could augment the current eHDSI services, but could also be deployable in other scenarios, beyond the scope of the current CBeHIS.

The HEALTHeID vision is not constrained by the limitations of our current uses cases. Although the implementation will focus on serving the current CBeHIS use cases, the design and technical implementation choices will lay the foundations for patient enabled future scenarios of lawful sharing of health data, between DPs and DCs in the EU.

6. The need - ID for eHealth

Identification of patients is an important need for the delivery of efficient health services and public health management. Health professionals (HPs) need to know a patient's identity to access relevant medical and treatment histories and ensure that they are giving appropriate and consistent care. Patients are also interested: recent responses to the public consultation on the Communication on transformation of health and care in the Digital Single Market (2017) clearly state that there is a positive response to engage in personal health information management, with more than 80% of people interviewed which agrees to the idea that sharing health data can be beneficial to improve diagnosis,

treatment, and prevention of disease across the EU[1]. Furthermore, patients could need documentation to prove enrollment in insurance programs or other instruments that cover medical expenses. An inclusive, secure, and viable method of uniquely authenticate and identify healthcare users over time and across countries is paramount for each of these needs and the overall goal of achieving universal healthcare.

7. The opportunity - eIDAS

The eIDAS Regulation (EU Regulation no. 910/2014), and especially its part on electronic identification, entered into force in September 2018, "*ensures that people and businesses can use their national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available*". This means that, if a patient comes from a Country where eIDs are available, she/he has the right to access public services abroad, with the same eID used to perform online access to domestic "service provider". The online access will be performed with a high level of security, which is still a key concern among the citizens.

8. The idea - eIDAS for eHEALTH

The EU-funded project HEALTHeID (Grant Agreement INEA/CEF/ICT/A2017/1444644) aims to bridge the gap between the need and the opportunity, developing evolution of IT solutions already in place and created to assure interoperability between the different electronic health infrastructures deployed across the European countries. Patients will be no longer required to show a paper document to the health professionals or allow any other form of "weak" identification performed by the HP: the usage of their electronic ID will guarantee a secure identification. A familiar user experience, implemented by the issuer of such eID in their respective Country of origin, will help in the process of empowerment and engagement of the patients.

9. Exploiting HEALTHeID: a use case

Alice is a patient belonging to Country A, and is traveling abroad. During her journey in Country B, Alice needs medical treatment. A local health professional, Bob, have to identify Alice in order to access her medical data and deliver the appropriate care. Instead of seeking Alice's person identifier in a paper document, or asking her to provide such a data, Bob asks Alice to perform a cross-border authentication using her eID, released by her Country of usual residence and where she is insured (Country A) - the same she used online some weeks ago to book her flights and accommodations, or to pay local taxes in Country A. Performing this process, Bob avoids any risk of wrong typing, and Alice is sure

[1] Source: https://ec.europa.eu/digital-single-market/en/policies/ehealth

her medical data are properly accessed, in a secure process, and only if her consent has been given in an initial stage.

ANNEX I. HEALTHeID Patient Information Notice

BACKGROUND - WHAT IS EUROPEAN eHEALTH

As a European citizen you are entitled to seek the help of a healthcare professional in another EU country for planned or unplanned (emergency) care. In most cases you will be able to claim reimbursement for such care (further advice from your National Contact Point)

The healthcare professionals in the country you are visiting will be able to treat you much better if they can see the main parts of your healthcare records – **known as your Patient Summary** and your prescription history and active prescriptions - **known as your ePrescriptions**.

The European Union has established a safe and secure system for allowing a healthcare professional in the country you are visiting to access and view your Patient Summary or to dispense your ePrecriptions.

IDENTIFYING YOURSELF

The healthcare professional or a member of their staff in the country you are visiting will ask you to identify yourself using the electronic identification system. They will explain how to use the local identification application.

You will not be asked to share any PIN code or other confidential identification tool.

Your identification information will be kept in the healthcare system as long as is necessary for the care and treatment you will receive.

A record of the fact that you have been identified as well as your name and contact details will be kept by the healthcare system in the country you are visiting for as long as the administrative rules in the country you are visiting require.

YOUR RIGHTS

You have the right to accept or deny electronic access to your Patient Summary or e-Prescriptions by a healthcare professional in a country you are visiting.

This does not mean you will be refused care, but your care may be impacted if the healthcare professional cannot access your Patient Summary.

You are entitled to receive further information about the purposes for which your data will be used and who will have access to it.

You have a right to a portable copy of the record the healthcare professional in the country you are visiting has created, but this duty may be fulfilled some weeks after your visit.

If you find any errors in the record created in the country you visited, you have right to have such errors corrected.

Further information on your rights may be found at www.xxx.yy

ANNEX II: PATIENT CONSENT services

BACKGROUND - WHAT IS EUROPEAN eHEALTH

As a European citizen you are entitled to seek the help of a healthcare professional in another EU country for planned or unplanned (emergency) care. In most cases you will be able to claim reimbursement for such care (further advice from your National Contact Point)

The healthcare professionals in the country you are visiting will be able to treat you much better if they can see the main parts of your healthcare records – **known as your Patient Summary** and your prescription history and active prescriptions - **known as your ePrescriptions**.

The European Union has established a safe and secure system for allowing a healthcare professional in the country you are visiting to access and view your Patient Summary or to dispense your ePrecriptions.

In order to be able to use that system the health care professional must have:

Your consent to accessing and viewing your Patient Summary and ePrecriptions

Your consent to creating a record of the care you receive or the medication you have been dispensed in the country you are visiting.

This form concerns only the two consents above.

Even if you provide these consents, you may still refuse any treatment or care offered to you in the country you are visiting.

IDENTIFYING YOURSELF

The healthcare professional or a member of their staff in the country you are visiting will ask you to identify yourself using the electronic identification system. They will explain how to use the local identification application.

You will not be asked to share any PIN code or other confidential identification tool.

Your identification information will be kept in the healthcare system as long as is necessary for the care and treatment you will receive.

A record of the fact that you have been identified as well as your name and contact details will be kept by the healthcare system in the country you are visiting for as long as the administrative rules in the country you are visiting require.

ACCESSING YOUR PATIENT SUMMARY and ePRESCRIPTIONS and CREATINGA NEW RECORD

Once you have been securely identified the healthcare professional will use the European eHealth secure infrastructure to contact your home country and request to retrieve your Patient Summary.

The healthcare professional will be able to see major illness you have had, medication you are taking and other key information.

Anything you have asked your home doctor not to include in your Patient Summary will not be visible to the healthcare professional in the country you are visiting.

If you are provided with a medication, a dispensation report will be returned to your home country.

A record of the care and treatment you receive in the country you are visiting will be stored there for as long as is required by local law.

YOUR RIGHTS

You have the right to give or withhold your consent to access to your Patient Summary or e-Prescriptions by a healthcare professional or to have your data stored in a country you are visiting.

This does not mean you will be refused care, but your care may be impacted if the healthcare professional cannot access your Patient Summary.

You are entitled to receive further information about the purposes for which your data will be used and who will have access to it.

You have a right to a portable copy of the record the healthcare professional in the country you are visiting has created, but this duty may be fulfilled some weeks after your visit.

If you find any errors in the record created in the country you visited, you have right to have such errors corrected.

Further information on your rights may be found at: www.xxx.yy

PATEINT IDENTIFICATION DETAILS (automatically filled in)

First Name: ..... **Surname:** .....

Date of Birth: ☐☐ ☐☐ ☐☐☐☐ **ID number:** ☐☐☐☐☐☐☐☐☐

If Required

PARENT/GUARDIAN IDENTIFICATION DETAILS (automatically filled in)

First Name: ..... **Surname:** .....

Date of Birth: ☐☐ ☐☐ ☐☐☐☐ **ID number:** ☐☐☐☐☐☐☐☐☐

☑

I CONSENT to my Patient Summary* being accessed and viewed by the healthcare professional in [name of country]

I understand that my Patient Summary/e-Prescriptions will be used only for my care /dispensation of medication and for administrative purposes linked to my care, for the purposes of this healthcare encounter

Signature **Date**

....

☑

I CONSENT to a record of the care* I have received in [name of country] being created and stored in that country

I understand that this record will be used only for my care and for administrative purposes linked to my care.

Signature **Date**

*To be modified accordingly to each situation i.e. individual or proxy, Patient Summary or ePrescription.