EUROPEAN COMMISSION
DG HEALTH AND CONSUMERS
DG COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY

eHealth-units

5TH EHEALTH NETWORK 13 MAY 2014
COVER NOTE BY SECRETARIAT

Topic 7: Information points

Issue at stake
The eHGI and the Secretariat would like to inform you about several items which will either be place on the agenda of the eHealth Network in November, or will be valuable to the new Joint Action on eHealth (which will start end 2014).

Summary of document
Report on use of SNOMED CT The secretariat will report back on the progress made on the discussion for using SNOMED CT in cross-border context. No document is needed. *Guidelines on patient registries and supporting tools* The PARENT Joint Action prepared an information paper containing the most relevant information about the Joint Action, and a first look into the guidelines on interoperability of patient registries that are under preparation. *Recommendations on health records & patient access to health data* The eHGI drafted a document describing the need for patient access to electronic health records. The paper proposes a few next steps to be taken by the eHealth Network with regard to patient access. *Authorisation to access data* Authorisation is the final and key step in the process the get access to electronic health records. The eHGI has drafted a briefing note key explaining the objective based on eIdentification and authentication. *Horizontal legal aspects* The deployment of cross-border eHealth services entails a number of legal challenges which are a prerequisite to the deployment of cross-border eHealth services in general. This information paper prepared by the eHGI describes these challenges.

Format of procedure in the eHN
The Co-Chairs will introduce the topic, and will request the different authors to inform the eHeath Network shortly about the information points. No discussion/decision necessary at this point. Please note that the time per information point is limited.

INFORMATION PAPER

for eHealth Network[1]

Guidelines on patient registries and supporting tools

Introduction

Article 14(2)b of the Directive on patients' rights in cross-border healthcare states that among the objectives of the eHealth Network will be to ***draw up guidelines on effective methods for enabling the use of medical information for public health and research***.

Due to their sheer number and large volume of collected medical information, patient registries[2] present significant potential for research and public health improvements in EU. Patient registries are of increased importance due to public health needs (e.g. monitoring of patients' treatments, safety assessment) and the trends of translational medicine (e.g. registry-based clinical trials, personalized medicine).

The quality and structure of data currently held in patient registries is however inconsistent and – due to lack of use of common methodology – in most cases cannot be directly used for secondary purposes[3]. Processes and legal agreements for data sharing across registries and Member States are seldom established. Time-consuming search and identification constitutes another important barrier. Although there are some best practices in particular areas such as Rare Disease, the need for a generalised methodology across diseases and medical cases is of paramount importance.

As a consequence this large and growing amount of medical data in the EU remains unavailable for broad research and public health purposes. To improve long term use of this data it is necessary to agree on EU-wide guidelines and tools for making patient registries interoperable across the EU, addressing the needs of data sharing for secondary use. Patient registry holders and a number of EU stakeholders have already expressed a need for EU level sharing of registry-related knowledge and best practices, as well as for tools and services improving quality of data and data availability for secondary use.

What is PARENT doing?

PARENT is a joint effort by Member States and the European Commission as a direct response to the objective set in Article 14(2)b of the Directive. PARENT aims to improve secondary use of data from patient registries in a cross-border setting for both public health and research needs. Based on

[1] Drafted by the Patient Registries iNiTiative Joint Action (PARENT), www.patientregistries.eu

[2] A patient registry is an organized system that uses observational study methods to collect uniform data (clinical and other) to evaluate specified outcomes for a population defined by a particular disease, condition, or exposure, and that serves one or more predetermined scientific, clinical, or policy purposes. Three general categories with multiple subcategories and combinations account for the majority of registries that are developed for evaluating patient outcomes. These categories include observational studies in which the patient has had an exposure to (1) a product or (2) service, has a particular (3) disease or condition, or various combinations thereof.' (Gliklich RE, Dreyer NA, eds: Registries for Evaluating Patient Outcomes: A User's Guide. 2nd ed., 2010).

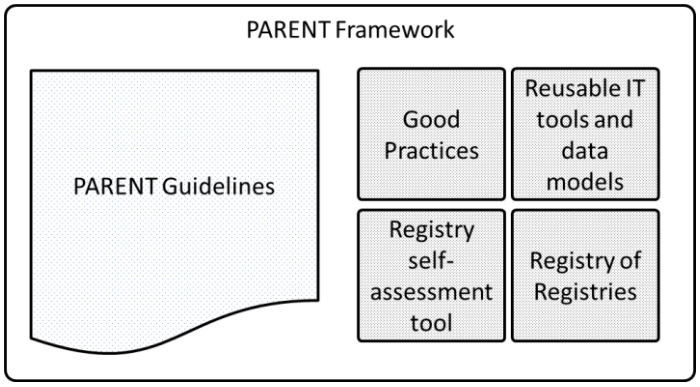
[3] Including areas such as Quality of Care, Pharmacovigilance, Safety, Health Technology Assessment, Public Health Policy and others

analyses performed, these objectives can only be achieved by:

(1) improving use of primary data sources for feeding data into patient registries[4];
(2) improving data quality and interoperability of new and existing patient registries;
(3) mapping of patient registries in the EU with the purpose of supporting search and identification of available data sources; and exchanging information about national best practices and lessons learnt on patient registries;
(4) supporting data sharing between and across registries; and data reporting to authorities and relevant bodies;
(5) providing support services for registry holders at EU level.

Therefore PARENT is developing methodological guidelines and recommendations for efficient and rational governance of interoperable patient registries (the *Guidelines*) and additional implementation tools and services to be available in Autumn 2014.

Fig. 1: PARENT Guidelines and supporting tools



PARENT partners: 22 MS
PARENT Associated Projects Group: EAR EFORT, EPIRARE (&RD-CONNECT), EUReMS, EUCERD JA, EUBIROD, EUROCISS, EPAAC, EuraHS, eHGI, epSOS, EUnetHTA, SHN, EHR4CR (&EMIF)
Additional partners and stakeholders: NICE UK, CPME, ESIP, EFPIA, EBE, EUREGHA, HIQA Ireland and many others

The Guidelines on patient registries (to be released in autumn 2014) cover the entire registry lifecycle, including a guide and good practices on registry design, set-up, governance and management, as well as secondary use of data. The structure of the guidelines is provided in Appendix 1 and is based on extensive ongoing consultation process with key EU stakeholders (PARENT Stakeholder Forum, relevant EU Joint Actions and eHealth projects). They represent a key resource to be used by registry holders and stakeholders (i.e. European Reference Network, Joint Research Centre). There is a clear need for common adoption and further implementation of Guidelines on EU level in order to create value of data from patient registries.

A pilot **Registry of Registries (www.parent-ror.eu)** has been released in November 2013, in order to facilitate the mapping of patient registries across EU. It currently holds descriptions of approximately 140 national or regional registries across the EU and is increasingly being used by stakeholders (such as the European Society for Cardiology) to map registries relevant to them.

A **self-assessment functionality** will be added by autumn 2014, to support clear added value to registry holders and support its sustainability by providing assessment and tailored improvement guidance (based on *Guidelines*) to registry holders, as well as an indication of registry ability to share data – to be used by regulators, medical knowledge researchers, funders, etc. EU and Member

[4] Where PARENT recognizes the results and ongoing work of several projects focusing on improving interoperability of Electronic Health Records (EHR) as primary sources of data (i.e. SemanticHealthNet, EHR4CR, TRANSFoRM, EMIF, SALUS);

States' authorities will be able to use the Registry of Registries and assessment tool to monitor improvement of registries' interoperability capacity for providing **data for secondary use** and to assess the level of the implementation of the guidelines on patient registries, and the resulting positive outcomes.

As collaborative effort is a prerequisite for **common data models in registries**, PARENT is establishing an online collaborative environment where registry experts contribute towards development of generic and field specific registry datasets. A number of existing proposals for a common/minimum data set are being analysed and made available in a semantically interoperable format based on the approach used in SemanticHealthNet.

The eHealth Network and Patient Registries

As the leading body in EU eHealth policy, the eHealth Network will be requested to adopt the guidelines on patient registries and promote the use of the Registry of Registries. PARENT therefore also proposes that the supporting interoperability assets (Registry of Registries, Assessment tool etc.) are taken into account for the Connecting Europe Facility. In November 2014 the eHealth Network will be presented with the main outcomes of PARENT and will be asked to discuss and adopt the necessary documentation. PARENT is expected to run until 1st May 2015, and will be able to take on request by the eHealth Network for further dissemination. Below is the draft roadmap leading towards validation by the eHealth Network (eHN):

- Information paper presentation at eHN meeting (May 2014)
- PARENT Seminar on Sustainability; Draft Guidelines Workshop (June 2014; MS representatives invited to provide feedback)
- Launch of PARENT Guidelines and Framework (Oct 2014)
- Discussion paper presentation at eHN meeting (Nov 2014)
- Guidelines Adoption paper presentation at eHN meeting (May 2015)

For information

APPENDIX 1: DRAFT index of "*Methodological guidelines for efficient and rational governance of interoperable patient registries*":

INFORMATION PAPER

eHealth Governance Initiative:

Joint Action JA-EHGov & Thematic Network SEHGovIA

DELIVERABLE

D6.3 Recommendations on patient health records, including patient access to health data

WP6 Trust and Acceptability

Version:	V4
Date:	22-04-2014

Project co-funded by the European Commission within the ICT Policy Support Programme and the Health Framework Programme

COVER PAGE	
Project acronym	**eHGI Joint Action**
Grant agreement number	**20102302**
Status*	**FINAL**
Dissemination level**	**PU**
Author(s) & organisation(s)	**Luc Nicolas (PFS PH), Diane Whitehouse (EHTEL), Leif Littkens and Benny Eklund (Uppsala County Council, Sweden), Laine Mokrik (Tervis-Estonia), Michael Wilks (CPME), Stephan Schug (EHTEL) and WP6 members**
Contact	**luc.nicolas@sante.belgique.be**

* Status: Draft / In Progress / Final

** Dissemination level: PU = Public or

CO = Confidential, only for members of the consortium and the Commission Services

ABSTRACT

The paper documents the evidence collected after deployment of the “patient access to data” service in Sweden (Uppsala) and Estonia and lists the key issues that need to be appropriately addressed at national and European levels.

Change History					
Version	**Date**	**Status**	**Author**	**Details**	**Review**
V1	20.02.2014	Draft	Luc Nicolas		WP6+ externals
V2	05.04.2014	Draft	Diane Whitehouse		WP6+ externals
V3	07.04.2014	Draft	Luc Nicolas		PSC
V4	22.04.2014	Final	VITA	Grammar review and formatting	

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

ABBREVIATIONS

EHR	Electronic Health Record
NHS	National Health Service
GP	General Practitioner

TABLE OF CONTENTS

1. Introduction and scope of the paper

This briefing paper covers several elements: it describes the national and international background to the need for patient access to electronic health records; it examines the existing evidence, drawing on two cases – those of Uppsala county in Sweden and of Estonia – and uses them to identify the benefits, lessons learned and functionalities relating to patient access; it then uses the same two cases to identify a range of seven open issues which still need consideration. The paper ends by identifying a set of proposed next steps to be taken by the eHealth Network with regard to patient access as a result of these open issues. This will involve the organisation of a formal workshop that brings together key projects and Member States. The workshop outcomes should provide the input for a formal recommendation to be submitted to the eHealth Network at an appropriate date.

Items that are outside the scope of the paper: First, apart from the question of access *per se*, the question of the modalities of control of access by the patient himself or herself, and the subsequent need for supplementary rules, are highly dependent on national public "culture"; this issue is not explored here. Second, questions related to topics such as consent, modulated access[1] and exclusions are related to the issue of authorisation and are therefore not dealt with specifically in this document. Third, while aspects of patient access associated with security, data protection, safe identification and the authentication of actors are considered to be essential prerequisites to patient access, they are also not discussed here.

[1] Capacity to limit access to specific information and/or HCP

2. National and international background to patient access

With the majority of Member States currently entering the phase of deploying wide-scale eHealth applications, two challenges arise: the question of access to data by the patient himself or herself sometimes remains unaddressed at national level, while the upcoming deployment of cross-border use cases requires consensus at the European level. There is now growing experience of wider-scale deployment.

The evidence accumulated, e.g. in the Swedish context, shows that resolving the question of patient access to electronic health records is not a side issue: it is an important prerequisite in order to support patient empowerment, citizen engagement and innovative approaches to health care.

Patient access to electronic health records is an important driver for the use of key eHealth applications. Recent experience in Member States demonstrates that the absence of provision for an active role for citizens/patients in the implementation of national eHealth roadmaps has often led to significant hurdles and delays.

Key Action 13 of the European Commission's 2020 *A Digital Agenda for Europe* aims at undertaking pilot actions to "**equip Europeans with secure online access to their medical health data by 2015"**. To support this objective, the European Commission funded two pilot projects entitled "SUSTAINS"[2] and "PALANTE"[3]. These projects were designed to equip Europeans with secure online access to their medical health data and, together, have involved over 20 regions in 12 Member States.[4]

With the financial support of the European Commission, pilot projects in integrated care are also being implemented in a growing number of European regions (see, for example, United4health, Smartcare, Carewell, Beyond Silos and Integrate).[5] The use cases on which all of these projects are based assume some kind of access by the patient to his or her data.

[2] http://www.sustainsproject.eu/
[3] http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=297260
[4] Austria, Czech Republic, Denmark, Finland, Greece, Ireland, Italy, Norway, Slovenia, Spain, Turkey and UK (Scotland)
[5] http://www.integratedcarefoundation.org/project/project-integrate
http://pilotsmartcare.eu/home/
http://www.united4health.eu/
http://www.beyond-silos.eu/home/

The wide-scale deployment of cross-border services, such as those piloted by epSOS[6], furthermore requires a minimum consensus at the level of the European Union on the scope and modalities of patient access.

Overall: Access to patient data should be about making access to data meaningful and understood. It is about moving patient access from paper to the digital world. Creating convergence at the national level can also enhance and support access to patient data across borders or despite borders. Patient access needs to be complemented by the ability to access data across borders, and the associated value that benefits both the person (the patient as an individual) and the health system. These two outcomes are vital and complementary.

3. Existing evidence

The existing evidence has been tested, and documented, in the Swedish county of Uppsala via the SUSTAINS project. The results of the Uppsala initiative have proved to be sufficiently valid for Sweden as a whole to extend this service to the entire country. Estonia has been offering a patient access to data service since 2008. Meanwhile, the National Health Service (NHS) in England has been planning a roll-out of patient access to data from 2013 onwards.

This sub-section aims at summarising the main findings from two sources: the SUSTAINS project in Sweden, and the Estonian context (the English example is not documented here).

These two examples are used to provide the Member States with a list of the key open issues that surround patients' access to their own data.

The two examples also show that there are various commonalities among doctors' opinions in Member States as well as dissimilarities. The question of electronic access by the patient to his or her medical data is often considered to be a sensitive issue by public authorities.[7] Numerous *a priori* legitimate questions are raised about this issue by health care professionals. However, the evidence to date in this limited number of countries shows that most of

[6] http://www.epsos.eu/

[7] This position was taken by associations of medical doctors in Sweden but can certainly be extrapolated to associations of medical doctors in other countries.

these assumptions and fears are not justified. In Sweden, for example, doctors' anxieties that patients might be confused by the various sets of data have been shown to be unfounded. In fact, patients have been happy with the patient access service provided and they appreciate the degree of patient empowerment it enables. Opening up the electronic health record to the patient improves: the quality of the data available; the quality of communication between health care professionals and the patient; and long-term patient safety. In Estonia, there was also some initial resistance on the part of the hospital sector; it is now the treatment relationship between the health care professional and the patient that guides the degree of appropriate access to patient data; and, ultimately, it is the patients themselves who monitor/vet to what extent inappropriate access has taken place (which they are then able to report to Estonia's Data Protection Inspectorate).

3.1 Uppsala, Sweden

After nine years as a pilot at a general practitioner (GP)'s surgery, the "Read your EHR via the net" service was made available to the public on 8 November 2012. With a few exceptions, the service includes all the medical information from GP surgeries, open care and all hospital care in the county of Uppsala.

The patient/citizen chooses whether to see his/her information as soon as the information is entered in the electronic health record (EHR) or within 14 days.

After one year of operation:

- 50,000 unique patients/citizens have used the service.
- Each patient has logged in five times on average, and in total there have been 250,000 logins.
- 98% of patients have chosen to read the information immediately.
- Females used the service slightly more than males: the share of those who had an EHR was 7.37% for females and 5.54% for males (after nine months of the service being operational).
- After one year, 9% of patients/citizens with an EHR in the county of Uppsala had used the service.
- Users were aged between 23 and 72 years of age.
- The typical user had a current medical problem and was a major consumer of health care.

At first, the doctors' union opposed the introduction of the service, mainly for the reasons given below. The union argued that:

- There will be a rush of patient questions that prevents work.
- Patients will not understand the information.
- Patients will be concerned about the information.
- There is a risk that health care workers will be threatened when patients read the log list of who has access to the data.

However, evidence collected from the Uppsala initiative shows that doctors' fears were unfounded. There was no rush of questions on the part of the patients, who did not experience any real problems in understanding the notes of the clinicians. Overall, the service has drawn extraordinarily wide media attention (more than 150 articles have appeared in newspapers and it has featured on TV and radio over 30 times).

On the whole, the "Read your EHR via the net" service has proved to be the most successful eHealth service introduced so far.

The Uppsala evidence from the SUSTAINS project indicates that the service has led to the following benefits:

- Improvement in quality of the information produced.
- Improvement of communication between the health care professional and the patient.
- Patient empowerment and a more balanced relationship between the health care professional and patient.
- Time gain for the health care professional through the reduction of administrative constraints.
- Better access to the services. The "read the EHR" service opens doors to other eHealth services.
- Potential benefits in terms of patient safety and adherence to treatment.

3.2 Estonia

A new version of the Estonian National Patient Portal was launched on 1 July 2013 (it was first introduced in the country at the end of 2008). It allows patients to log in using their ID card and/or Mobile ID. The services available to patients in the new portal include: electronic health records, links to medical images, electronic referrals, compilation and electronic signature of different types of "expression of will"[8], access to health insurance validity, viewing and updating of personal data and contact details of a close relative, time-critical data, viewing of ePrescriptions, tracking usage of personal data, delegating

[8] Regarding, for example, blood transfusion, usage of post-mortal body for scientific and education purposes, and post-mortal transplantation of organs and tissues

access to a trustee of personal medical data, and masking data or masking single medical documents to health care professionals/trustees.

The following functionalities have been considered as important drivers to foster a citizen's/patient's use and acceptability of the patient access to data service. They relate to the patient's capacity to:

- Consult his or her data.
- Mask certain data.
- Have access to all access logins.
- Book (or rebook) appointments.
- Direct a question to a specific health care professional.
- Fill in forms online.
- Request an e-Prescription.

By March 2014:

- More than 1.2 million persons had seen the medical documents stored in the central health information system via the National Patient Portal.
- The Estonian National Patient Portal had more than 66,000 unique users; the number has grown over the four years since it was first launched and the number of unique users is increasing.
- More than 1,000 delegations of access had been compiled in the National Patient Portal and sent to the central information system.
- More than 1,500 expressions of will had been compiled in the National Patient Portal and sent to the central information system.

Evidence collected in Estonia shows that the launch of its patient access to data service has not caused any major problems other than some initial resistance from the hospital sector. Use of the service is directly related to the amount of information available and the availability of services, with added value for the citizen/patient. The service is mainly used by young females (aged 21-40 years), while its use by the male population remains marginal. During the first three years of the health information service deployment, most efforts were dedicated to the involvement of health care providers and physicians as they were considered "the source of health care data". Although patients have been involved from the first day of the health information service, it can be concluded that during the first years of its deployment not enough data was produced to attract a majority of patients to use the service. While, overall, the lessons learned are quite positive, additional incentives are needed to achieve a more complete digital documentation in the national health information system, and hence for more data and possible applications to be available to patients.

4. List of key open issues and currently proposed solutions

Seven key open issues are listed below. Where proposed solutions to the specific issues are available, they are mentioned.

4.1 Direct or health care professional-mediated access

In the case of health care professional-mediated access, it is the health care professional who decides for each individual patient whether to provide him or her with access to his/her data. Optionally, the health care professional can also decide to provide partial access to the patient. The principle of mediated access is in contradiction with the principles of patients' rights legislation in most Member States, but it can be seen as an intermediary step in countries where there is cultural sensitivity to patient access. Mediated access, however, seems to remain necessary for certain categories of people (e.g. teenagers) or activity (e.g. "clinical thoughts"; see Section 4.5).

4.2 Delayed or immediate access

The assumption is that it might be better to give patients (bad) news about their medical results before they have access to the data themselves. Evidence shows, however, that when given the choice, patients usually opt for immediate access to the data. Providing the patient with the option to choose is important.

4.3 Default rules for access by children and teenagers

Parents (or official guardians) are by default allowed to have access to the data of their children (up to 12 years old). Teenagers (up to 18 years old) have no default access to their own data except when they are affected by a chronic disease (and this access occurs only if the doctor in charge assesses the individual teenage patient's maturity and the need is very strong). Thus, access is decided on a case-by-case basis when maturity is assessed as sufficient and indication is very high.

4.4 Vulnerable patients or patients under influence

These patients are to be provided with the option of voluntarily suspending their access to data. Only a formalised procedure would allow them to regain access.

4.5 Health care professionals' personal notes

These notes are by default not accessible to the patient. The situation requires that these notes are specifically "tagged" in the electronic health record as the personal notes of the health care professional. "Clinical assumptions and thought" are considered to be information which should be shared between health care professionals, but should not be directly accessible to patients. Evidence collected from the Open Notes[9] project in the USA tends to demonstrate that – when shared – such specific pieces of information are highly valued by the patients, and have a demonstrated impact on use of the service and patients' adherence. Evidence from Uppsala, Sweden shows that the use of "personal notes" by doctors is very rare (i.e. in less than 0.01% of all notes).

4.6 Issues relating to trust and acceptability

A number of other critical issues that directly affect trust and acceptability need to be further considered. Below is a non-exhaustive list:

- Give the patient the option of providing data (both "objective and subjective" data, and both structured and unstructured) as input for the health care professional.
- Provide guidance to avoid uncontrolled proliferation of patients' portals.
- Develop and/or select appropriate technical and semantic standards to improve data readability and understanding by the patient.
- Invest in mass and targeted information and education campaigns about patient access to electronic health records for the citizen/patient.
- Include mobility aspects for the patients.

4.7 Mandates management service

The availability of a secure "mandates management service" guaranteed by the public authorities is seen as an important complementary service which should add the necessary flexibility to the system.

[9] http://www.nejm.org/doi/full/10.1056/NEJMp1310132

5. Next steps (towards a mandate to be adopted by the eHealth Network)

In view of the strategic importance of this issue, and the availability in the coming months of supplementary evidence emerging through projects such as SUSTAINS and PALANTE, it is proposed that a formal workshop on the issue of patient access to data should be organised. The workshop should bring together key projects and Member States, with the results providing the **input for a formal recommendation** to be submitted to the eHealth network at an appropriate date.

INFORMATION PAPER

eHealth Governance Initiative

Authorisation to access data

- Outline

1. Accessing health information: a key objective based on e-Identification and authentication
2. Conditions for the authorisation process
   2.1. Patients' fundamental right to control who accesses shared personal data: consent and management of authorisation
   2.2. Who has access: HP's role and therapeutic link with the patient
   2.3. Cross-border minimum interoperability requirement – necessity of National Contact Points (NCP)
3. Recommendations
   3.1. Objective and general principle
   3.2. Actions to be taken at EU level – by the EC, by a group of Member States or by stakeholders
   3.3. Actions to be taken at national or regional level (according to country organisation)
   3.4. Priorities and authorisation: next steps

1. Accessing health information: a key objective based on e-Identification and authentication

To guarantee European citizens their rights in cross-border healthcare, as mandated by the 2011/24/EU Directive, when it comes to eHealth it is necessary to authorise access to health data for online requests from another Member State.

In contrast to other sectors, the main situation in healthcare is what has been defined as "on site" as opposed to online. Indeed, in this situation, the request to access data is made by a healthcare professional during an encounter with a foreign patient. Authorisation is the final and key step in the process that starts with patient identification, identity authentication, health professional identification and identity authentication.

This is an especially difficult step because health data is protected under privacy and confidentiality laws and by strong technical means that prevent unauthorised access. The systems vary between Member States due to different technical solutions but in particular because of legal and cultural differences.

It is of utmost importance to build a circle of trust between Member States, while it is also necessary to ensure that the solutions will be consistent with the ongoing prepared Regulation on electronic identification and trust services for electronic transactions in the internal market (EIDAS) – and/or that special measures are taken to conform to specific constraints for eHealth. In addition, future processes will need to comply with the Data Protection Regulation currently under discussion or will entail specific measures for personal health data.

2. Conditions for the authorisation process

As management and control of health data depends on legal regulations strongly linked to national and regional cultures, it is necessary to consider the present situation in Member States. As a result, a special workshop was organised by the eHGI in March 2014.

In most countries, citizens cannot currently access their medical records and very few professionals are able to do so either. The situation is changing, but unfortunately the legal and practical basis sometimes differs significantly. Moreover, the domain involved may vary: access can be limited to specific hosts or specific documents.

Online access by citizens themselves, which is currently rare, is a trend that should not be overlooked. In countries or regions where a central host or centrally defined rules have been enforced, such as Austria, Estonia, France, Greece, Italy (various regions) and the UK (not a complete list), online access is possible or is being implemented, or discussions are underway to define its form (as in Belgium, for example).

Another common trend relates to emergency situations: all countries converge towards a "breaking glass" mechanism that allows HPs direct access to data when patients' lives are at risk, with a posteriori control.

2.1. Patients' fundamental right to control who accesses shared personal data: consent and management of authorisation

This is a key aspect when it comes to sharing data between HPs or hospitals that treat or have treated the citizen involved. A common position for shared repositories is that the patient should be in control:

- of the creation of any shared record
- of the HPs allowed to access it

There is a critical difference between "opt-in" and "opt-out" schemes. Solutions are and will be closely related to national choices. Due to the growing concern for privacy, opt-in systems tend to be adopted and are more or less binding. However, some countries – such as Denmark and Estonia, where the population is widely familiar with electronic procedures and trusts the public management of the system – are strongly in favour of an opt-out system.

A key component of any process is patient consent. In any on-site access by a healthcare professional not yet authorised by his or her position in the system and towards the patient, the patient has to be informed. In any event, consent validation depends on the signature of a document or on an e-signature. However, the e-signature may be that of the Health Professional in combination with an authenticated ID of the patient that proves his or her presence and acknowledgement, e.g. for the creation of a National Health Record in France.

2.2. Who has access: HP's role and therapeutic link with the patient

In Europe, cross-border access will first involve the five regulated health professions listed in the revised 2005/36/EC Directive (doctor, nurse, dentist, midwife, pharmacist). In all countries, HPs' access to patient data depends on their role and permission, the definition of which is based on their profession but differs between countries. Key aspects are the HP's effective position in the healthcare system, his or her therapeutic link with the patient and his or her participation in a care team, such as a hospital unit.

Secure authorisation procedures are currently very time-consuming, which is a serious obstacle for professionals with time constraints. This would be all the more so for cross-border access if procedures differ between countries. Accordingly, procedures will need to conform to local interfaces, techniques and practices. Otherwise, no system will be used.

2.3. Cross-border minimum interoperability requirement – necessity of National Contact Points (NCP)

Constraints have already been identified for identification and authentication. A significant difficulty is that the patient ID must be able to be validated at any location (and moreover in a foreign country).

It is also necessary to be able to access data with no knowledge of its location, and independently of the patient's country organisation, as the data may be in a central repository (to which access is limited) or in a variety of local repositories. A National Contact Point or a network of regional control points (depending on the institutional framework of the health system in the relevant Member State) must exist in the patient country in order to translate the request and locate the data to which access is to be allowed, as was demonstrated during the epSOS project.

3. Recommendations

3.1. Objective and general principle

In conformance not only with the proposed EIDAS Regulation but also with eHealth Network eID (electronic Identification) policy, the cross-border authorisation process will not modify the national system but will enable interoperability between countries who choose to participate.

Interoperability has to be ensured at a legal, organisational and semantic, and technical level.

The system must be technically neutral, while being able to be adapted to the different resources and systems available in particular countries. It should be noted that many solutions are now based on smart cards (at least for the HP) and that all countries that have developed health record systems are now working on means that allow patients to have mobile access. As already stated for other domains, it should be recommended that countries which are currently developing systems try as far as possible to use solutions developed by countries that are at a more advanced stage, thus sharing costs and reducing the difficulties of cross-border access.

The solutions have to adapt to national constraints, particularly for eID. As already stated by the eHealth Network, the process must support systems with specific health IDs as well as those with general public eIDs.

Accordingly, the key principle is "When in Rome, do as the Romans do"[1]. It is impossible to conform simultaneously to diverse complex authorisation rules in different countries. If the requesting HP is authorised in his or her country to access given information, a positive agreement should be transmitted to the patient's country, along with validated IDs of the HP and patient. However, in this case patient consent in written form should be necessary. The country of treatment should be responsible for giving this agreement.

Many steps are required to achieve this situation, but above all a strong circle of trust has to be built among all parties involved.

[1] as designed and demonstrated in the epSOS project

3.2. Actions to be taken at EU level – by the EC, by a group of Member States or by stakeholders

■ *More analysis needed*

A survey among Member States should provide specific information about legal and technical barriers. In particular, rules for consent have to be monitored – how it is granted, for how long, for which information, how it could operate when a patient travels abroad, etc.

■ *Commonly agreed scope and perimeter (semantic clarification)*

• A common dictionary and definition of terms is necessary, as many terms are fuzzy, e.g. consent (related to data access, data sharing and even treatment), care team, therapeutic link, etc.

• The perimeter of the data and documents subject to authorisation has to be defined and known (for example, a social condition may be included in medical records in some cases; it should be borne in mind that such documents that are not confidential per se may help identify a person within a database, depending on security measures).

■ *Minimum constraints*

• For HP identity authentication, a prerequisite is the availability of online HP directories, as seen in previous documents. The content is dependent on the level of information needed for the authorisation process. Accordingly, a common structure and minimum content of these directories are necessary inside the circle of trust, particularly with regard to the HP's current position in the healthcare system (e.g. working in a hospital unit).

• It is necessary to define a common consent document structure and creation/dissemination process, including use of e-signature or another agreed secure replacement mechanism.

• With regard to EIDAS, assurance levels have to be defined (consistent with EIDAS levels) – related to use cases for authorisation.

• In all countries, an audit trail is mandatory for all access to personal data. An agreement should define the information to be stored and exchanged when necessary in order to ensure at least the traceability of cross-border access. This agreement should define who is allowed to access the audit trail and who can review/check the audit trail mechanism.

■ *Special attention to coherence with EIDAS, the Data Protection Regulation and CEF*

Under an agreed governance process/mechanism, coherence must be ensured, and specific health domain needs have to be taken into account and articulated with EIDAS and the Data Protection Regulation.

- *Online citizen access*

Such access could be determined and organised by each country in accordance with eIDAS and with specific amendments if these are deemed necessary. However, multilateral agreements should be useful, as it is the case for other sectors starting to conform to eIDAS before 2018.

- *Emergency situations*

Ultimately, a simple "breaking glass procedure" should allow normal rules to be disregarded, providing that minimum conditions and a posteriori control are in place (i.e. secure identification of healthcare professionals, tracing and specific notification).

3.3. Actions to be taken at national or regional level (according to country organisation)

- *Publication of schemes*

The proposal for eID and signature regulation (EIDAS) includes mandatory notification of eID schemes by national authorities. For the eHealth authorisation process, it is also necessary to notify authorisation schemes at EU level: definition of available documents for cross-border access (based on national priorities and available documents, constraints, technical means, agreements with other Member States).

- *Prerequisite: HP directory and National Contact Point*

As seen above, participating Member States will need to create and update an online directory of professionals and health organisations, based on an agreed minimum common structure and data set, which is accessible to the country's HPs. A National Contact Point (or a network of regional contact points) is also necessary in order to authenticate HPs, validate their requests and relay them.

- *Legal interoperability*

In terms of the various documents and services that are requested to be produced on the legal aspects of eHealth (e.g. on authorisation and access), it is important to examine not just Member State-specific contexts but also to cover any cross-border implications.

3.4. Priorities and authorisation: next steps

- *A progressive approach*

As is the case for EIDAS, it will be useful to start developments inside a reduced voluntary group of Member States who are ready to do so.

In practical terms, authorisation to access data means authorisation to access datasets and more probably – at least in the next few years – documents. The progressive approach should be restricted to specific documents that are accessible through the National Contact Point (whether this is in central, regional or local repositories) in the countries involved. Experiments or developments could also be based on commonly defined documents: Patient Summaries and e-Prescriptions. Experiments could quickly start among countries that are already working together or that participated in projects as epSOS. To avoid duplicating bilateral agreements and compromising coherence, it should be proposed that developments will be based on a commonly agreed minimum framework.

However, to encourage development, specific documents or information could also be considered – such as biological analysis results – as could specific domains, such as rare diseases.

This progressive approach involves provisional solutions, which are legally possible, being adopted and planned for each experiment or development. This is especially true of consent, as it is not currently possible to use a common validated system (the EIDAS Regulation being a proposal that has not yet been formally adopted and will not become mandatory until 2018), even for e-signature by the HP, who would then shoulder the responsibility of guaranteeing patient consent (if this can be made compatible with regulations currently in force in the country – legal interoperability will have to be addressed).

First developments could start as pilots as soon as 2015.

- *First infostructure steps and tasks*

At EU level, it is necessary to set up a specific group to monitor the tasks listed above.

A study should be conducted as soon as possible (to try and prevent more divergences from occurring).

An expert group should produce a common dictionary and propose to Member States the various repositories and document structures and content (HP directories, consent, assurance levels, audit trail). Ths group should also analyse online access possibilities and difficulties. It would also propose mechanisms for emergency situations. This set of studies and proposals could be produced in 2015 and 2016, since it is necessary to consult with ministries and stakeholders.

The group should monitor coherence with regulations and with CEF. It will draw on the support of a special team of legal experts.

The first priority is to reach an agreement on definitions, content and the process for publishing eID and authorisation schemes so that Member States can start doing so.

The second priority is to define a common structure and minimum data set for HP directories, which defines specific roles and responsibilities. It should be available by the end of 2016.

At country or regional level, the first task is to publish authorisation policy and precise constraints.

The second priority is to develop HP directories in coordination with the EU expert group.

INFORMATION PAPER

DISCUSSING PRIORITIES TO BE ADDRESSED BY THE EHEALTH NETWORK CONCERNING HORIZONTAL LEGAL ASPECTS

Proposed by the eHealth Governance Initiative

Date: 13th May 2014

Preamble

The eHealth Network has adopted the first release of the "*Guidelines on minimum/non-exhaustive patient summary dataset for electronic exchange in accordance with the cross-border directive 2011/24/EU*" and is presently discussing guidelines for the interoperability of ePrescription.

The deployment of these cross-border services entails a number of legal challenges which are not specific to a particular cross-border service, but which are a prerequisite to the deployment of such cross-border services in general. Such prerequisites have already been outlined in Article 12 of the Patient Summary guidelines and it is expected that they will be addressed by the eHealth Network under priority 3 of its Multiannual Work Programme, *"Addressing legal barriers to interoperability, including data protection issues*", by the end of 2014.

This discussion paper proposes a two-step approach: Firstly, the eHealth Network will agree on the list of topics considered relevant for discussion under this priority and their prioritisation, which is consistent with the prioritisation for Patient Summary and e-Prescription services. In a second phase, the eHealth Network will agree on actions to deal with the challenges within each of these topics.

This discussion paper focuses on the first step and formulates proposals, building upon the CALLIOPE and epSOS recommendations as well as input from the relevant studies commissioned by the EC.

Challenges and risks

With respect to privacy and data protection, Directive 95/46/EC aims to remove barriers to the free flow of information in the EU. While the Member States (MS) have all recognised data contained in medical documentation as "sensitive personal data" that is subject to a higher level of protection, there is great national diversity in the way the Data Protection Directive has been implemented in national provisions, which in some cases creates barriers to the free movement of data. In order to overcome such barriers, the participating MS in epSOS reached agreements on common policies and measures concerning privacy and security to be applied in each country that participates in the exchange of data, which were then applied, monitored and reported upon for the purposes of the pilot.

As steps towards common identification and authentication measures for eHealth, the EC legislative proposals for data protection and electronic identification and trust services and the eHealth Network are expected to create convergence and therefore may diminish the need for such agreements; however, they are not expected to be implemented and enforced for the next few years. On the other hand, the epSOS pilot services have involved national investments to establish operational pilot services in several MS, thus creating an obligation to maintain a legally sound operational framework.

A number of countries have implemented nationwide pilots and are already running them on the basis of bilateral or regional agreements. The scenario of different groups of MS identifying and deploying cross-border eHealth business cases of common interest is in fact the most likely situation, with epSOS ending in June 2014 as an EU-wide, multi-million large-scale pilot. There is an obvious risk that – in the absence of a valid legal framework addressing the key elements of the epSOS Framework Agreement, and a mechanism to support and monitor their implementation – regional and bilateral solutions will soon replace the convergence achieved through this.

Intermediate measures are therefore necessary in the intermittent period for maintaining the convergence needed to enable the deployment of eHealth cross-border services.

Relevant issues to be addressed by the eHealth Network

(i) NCPs for eHealth

MS piloting epSOS have agreed that they need to appoint National Contact Points for eHealth for cross-border eHealth services. These are appointed by the appropriate authority in each country to act as a communication gateway and also as a mediator for delivering the services. As such, an NCP for eHealth is identifiable in both the EU domain and in its national domain and remains an active part of the cross-border eHealth environment if it complies with normative epSOS interfaces in terms of structure, behaviour and security policy compliance. An NCP, where appropriate in a

MS, may also act as an interface between the existing different national functions and infrastructures.

This NCP profile is quite different from the NCP described in Article 6 of Directive 2011/24/EC.

It is however noted that it is a requirement of Directive 95/46/EC to provide patients with adequate information concerning the processing of their personal data. Such information may be provided by the NCP set up under Article 6.

It is recommended that

1. The eHealth Network adopts common criteria for National Contact Points for eHealth and considers their possible interrelations with the NCPs under Article 6 regarding the provision of eHealth services across borders.
    - Agreement on such criteria of NCPs is a prerequisite for the adoption of ePrescription guidelines, which could be actionable by MS for the purposes of implementing cross-border ePrescription services.

(ii) Common privacy, security and quality of service policies

In addition to setting up the NCPs for eHealth, MS must reach agreements on a number of common policies which must be implemented in each MS as part of its participation in a Circle of Trust for the purposes of information flow for health and public health purposes.

While bilateral initiatives or initiatives of specific interest to different groups of MS may include specific provisions to best execute their objectives, their EU interoperability will be secured by

- Including the common agreements referred to above in their contractual arrangements
- Ensuring that any additional requirements do not create conflicts with these agreements
- Raising any new issues identified in the process of their specific interest collaboration for consideration and policy update at EU level
- Maintaining transparency within the framework of EU co-operation on interoperability

It is recommended that

2. The eHealth Network adopts common eID and authentication measures – including agreements on appropriate security levels for cross-border eHealth;
3. The eHealth Network commits to enabling a high level of assurance regarding authorisations of health professionals to access and process health data, including through the availability of authentic sources and online national health professional registries;
4. The eHealth Network adopts common measures for data protection, including a policy on patient consent for re-use of data for public health and research purposes at EU level;
5. The eHealth Network agrees on an appropriate duration of storage of data in the log files for audit purposes;
6. The eHealth Network agrees on appropriate SLAs for national services necessary for operation of cross-border eHealth services;
7. Such common policies and measures must be reflected in any cross-border eHealth agreements signed by MS for the purposes of providing eHealth services;
8. In order to create conditions for EU level legal and organisational interoperability, such MS agreements or acts may be modified during transposition into bilateral or multilateral contacts only in so far as it is necessary to do so in order to comply with local/regional law or customs.

(iii) Co-ordination mechanisms

Member State co-operation mechanisms are provided for in EU legislation, such as the regulation on eID and trust services. The eHealth Network on the other hand is a co-operation mechanism for cross-border eHealth and has the broad mandate to *"work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare".*

While the consolidation of these roles is expected to be the subject of EU and national organisational interventions, it is expected that the eHealth Network will have a central role in co-ordinating eHealth-specific policy aspects within the more general governance of interoperability at EU level.