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.