eHealth Network of National Competent Authorities on eHealth

Conclusions on "eID EU Governance for eHealth Services"

The eHealth Network,

ACKNOWLEDGES:

that citizens expect core eHealth services to be available across geographical borders within the European Union and that reliable personal identification is a key enabler for the provision of safe, effective cross border eHealth services;

that within the specific domain of health, when providing health services by electronic means (known as eHealth), accurate and secure identification is the first step;

that given the increased mobility of citizens within the EU, Member States, supported by the European Commission are strengthening their cooperation to facilitate mutual recognition of safe electronic identification mechanisms;

given the need to build on the existing cooperation within Member States in this domain and to bring forward the objective of Directive 2011/24, (Art 14 2. c) *"to support Member States in developing common identification and authentication measures to facilitate transferability of data across border healthcare"*. This paper outlines the main principles to be addressed by individual Member States when developing their electronic identification mechanism, to enable interoperability for better care, as one of the key measures required to "*facilitate transferability of data across-border healthcare*";

Member States have met several times over the past years for High Level meetings and have unanimously agreed to focus one goal: to collaborate on cross border eID to enhance and improve European citizens' health treatment and care on a cross border level and by fostering healthcare cooperation among Member States:

That the EU has firmly set the pace towards cross border eHealth in general and cross border recognition of eIDs. In particular, through the following legal and strategic initiatives:

- the **Council Conclusions** of December 2009, provided a political mandate for EU eHealth cooperation in four specific areas and established an eHealth High Level Governance process in Europe;

- **Directive 2011/24/EU**[1] in particular Article 14 on eHealth proposing the EU's support to Member States in developing common identification and authentication measures in order to facilitate transferability of data in cross border healthcare through a voluntary network;

[1] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p45).

- **Conclusions of the High Level Group** meeting in Budapest in May 2011 establishing eID as a first priority for the focus of the EU eHealth High Level Governance work and adopting the Common CALLIOPE EU eHealth Roadmap[2] as its decision support instrument;

- Implementing **Decision 2011/890/EU**[3] **of the European Commission** of 22 December 2011 establishing an eHealth Network, as laid down by the Directive 2011/24/EU.

- **Directive 95/46/EC**[4] and the European Commission's proposal for a general Data Protection Regulation[5];

- The **Digital Agenda for Europe**[6] foreseeing relevant key actions, namely
  - **Key Action 3:** "The Commission will propose a revision of the eSignature Directive with a view to provide a legal framework for cross border recognition and interoperability of secure eAuthentication systems."
  - **Key Action 13:** "Undertake pilot actions to equip Europeans with secure online access to their medical health data."
  - **Key Action 16:** "The Commission will propose a Council and Parliament Decision to ensure mutual recognition of eID across the EU based on online 'authentication;"

- The **eHealth Action Plan 2004**[7] and the forthcoming one in 2012;

- The **eGovernment initiatives** in the area of eID including the 2010 **Action Plan**[8], the Signposts towards eGovernment 2010 Paper and the Common EU eID Management Roadmap;

- The Large Scale Pilots **epSOS** and **STORK.**

That for the scope of this paper, the meaning of the terms "Identification", "Authentication" and "Authorization" and their characteristics are those described in the Annex.

AGREES:

to work on an eID EU Governance eHealth services;

---

2 Calliope network – www.calliope-network.eu

3 2011/890/EU: Commission Implementing Decision of 22 December 2011 providing the rules for the establishment, the management and the functioning of the network of national responsible authorities on eHealth (OJ L 344, 28.12.2011, p.48).

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31).

5 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final.

6 Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 f/2

7 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - e-Health - making healthcare better for European citizens: an action plan for a European e-Health Area, COM/2004/0356 final

8 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM/2008/0798 final

that the eID EU Governance for eHealth services profits from the results of existing eHealth related projects and other on-going developments in the area of eGovernment.

to develop and establish appropriate governance principles to ensure trust and provide the basis for a consistent treatment of electronic identities throughout the EU, irrespective of the originating Member State;

that the overall vision for better health and citizen-centred health delivery requires that governments recognize every person's need for a personal electronic identification to enable the support of equity of access to healthcare services in the Information Society;

that a first step towards eID interoperability is to ensure a mutual recognition and acceptance of Identification and Authentication to enable interoperability for continuity of care and improve patient safety;

that the twin functionality of eID - **identification** (who you are) and **authentication** (proof that you are who you claim to be) mechanisms provides the basis for eHealth services for patients and health professional and authorisation processes that are critical to access health information and will build upon this proposed eID identification and authentication governance. Such Authorisation processes need to be addressed in the future;

that authentication has to provide the necessary level of assurance about the claim of the user who he pretends to be;

that electronic identities representing citizens inside as well as outside their country of residence are key for the cross-border use of eHealth services that privacy and data security are of utmost importance and that electronic identification processes must ensure that the identity of a person is genuine;

that eID process and services are the necessary foundation upon which access rights to personalized health information can be managed within a legal and ethical framework both within a Member State and when sharing information across borders;

to facilitate close co-operation between eID initiatives in the health and other relevant sectors to enable interoperability on eHealth systems in the best interests of patients, healthcare providers and society at large.

That the eID EU Governance framework for eHealth services shall be federated, multi-level, shall rely on authentic sources and shall enable private sector uptake. Appropriate conditions and definitions of each of these characteristics are described below:

Federated:

- respect and interconnect national infrastructures, which will enable mutual recognition of electronic identities for the purposes of eHealth services between countries;
- rely on mutual trust and recognition between administrations concerning identification and authentication methods, although these methods and sometimes principles may vary *between Member States;*
- will accommodate countries which use either a “health specific” or “cross sectoral” identification process.

Multilevel:

- shall rely on the definition of specific levels of assurance to support the authentication requirements of particular eHealth applications and services;
- Member States shall agree at which levels they choose to offer authentication services and define policies for the required level of assurance for each eHealth application and service;
- Member States shall accept as valid any authentication methods of the required level of assurance from other Member States based on an agreed set of criteria.

Relying on Authentic Sources:

- Each piece of data in a specific set of identity traits comes from a single authentic source;
- Accordingly, an Identifier should always be associated with an assigning competent and recognised authority which represents national or regional authorities, or any other legally trusted organization and is able to deliver a reliable identifier for individual citizens (patients, professionals) and organizations;
- It is desirable that assurance on the quality of source of eID Management data can be publicly available.

Enabling Private Sector Uptake:

- Member States may choose to rely on recognised and entrusted private sector partners (e.g. financial institutions) for the provision of eID Management-services – provided that these private sector partners are obliged to adhere to commonly agreed privacy and data security regulations.

THAT in the context of eID for Health services a number of open issues are still to be addressed:

- **Usability** - a health professional is expected to accommodate many different national and even regional eIDs and eID processes when offering care to citizens of other Member State. This level of complexity may be a barrier to integrating cross border eHealth services into the national clinical process;
- **Privacy** - there are different security levels and practices currently applied in Member States and a lack of harmonised national approaches to the transposition of the Data Protection Directive. It should be also noted that security needs are perceived differently by the different stakeholders under different circumstances (e.g. citizens' needs contrast with patients' needs). The rules, policies and processes that must be respected by each service provider, as well as competent sanction mechanisms for enforcing the system stability and appropriateness, need to be laid down by and between Member States. For eID it is a must to incorporate privacy enhancing technologies in solutions and to ensure testing and certification at appropriate levels;
- **Technical interoperability** - technical solutions are not convergent, making interoperability among existing systems complex. A common acceptable definition that specifies how the service providers may legitimately interact with each other needs to be agreed;
- **Legal certainty** - Directive 2011/24/EU, which will be transposed by 25 October 2013, provides a framework for legal certainty, but further specification within the mandate of Article 14 will be needed before all barriers to cross border eHealth may be removed. Hence, a competent forum for assessing and aligning the regulatory framework required for such a system should be established.;

- **Ethical issues** - A common approach to ethical issues related to eID (e.g., the recording and storage of, access to patient-identifiable information for immediate care by a defined team) needs to be developed between the appropriate competent regulatory bodies within a EU legal framework.

THAT specific EU level actions centred on the principles set out above shall be driven by Member States and serve as a an enabler for the cross border use of eHealth services. This includes full range of policies, financial aspects of implementations, processes and mechanisms for enforcement. Monitoring and follow up that need to be coordinated in the creation of an EU level Governance for eID Management.

In View of the above, to build the eID EU Governance for eHealth services **the eHealth Network, while** respecting the national strategies and building on ongoing initiatives[9] in this area,

RECOMMENDS that:

- the eHGI proposes a trust enhancing policy to the eHealth Network;

- the eHGI elaborates a proposal for "common identification and authentication measures to facilitate transferability of data across-border healthcare on the ground of mutual recognition" while assuring high data security and respecting patient privacy;

- the eHGI reports on the main cross border implications of a common European approach of eID for eHealth and a realistic timeframe for its implementation. This should include a reference glossary of common concepts and definitions to facilitate common understanding between Member States and across sectors,

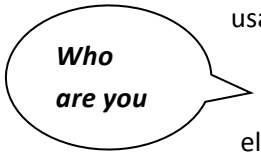
- the eHGI explores adequate models to enable interoperability between eID mechanisms in Health according to the principles, by taking into account the open issues to enable both an eHealth sector specific approach and a cross sectorial approach;

- the Member States, the eHealth Governance Initiative and all stakeholders take up an active role, within the appropriate institutional framework, in the decision making process leading to a major reform of EU legislation on data protection, as well as on eID and the eSignature package, with the aim of raising the specific needs and requirements of the health sector in such crucial domains.

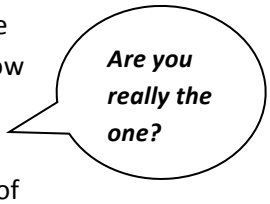
[9] epSOS, PEPPOL, SPOCS, eCodex, STORK, eEIF and National Implementations (eg. ELGA in Austria, etc.)

ANNEX

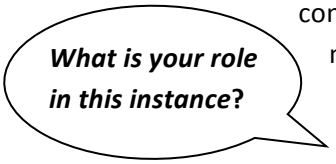
- **Identification.** This is the first level of the Identification process, independent of sector and usage. Establishing the *identity* a person or an entity may be done by means of a unique *identifier.* Identifiers are typically issued at national or regional level. Identification includes, on a generic level, appropriate processes to establish, describe and erase electronic identifiers.



- **Authentication**. Process for establishing through agreed credentials that the person is who they say they are. Such credentials can be something you know (e.g. PIN or password), something you hold (a physical or soft token) or something about your physical characteristics (e.g. biometrics). Any cross border eHealth service will need to ensure that the necessary combination of credentials and the tools for handling them are suitable for the specific level of assurance to support the authentication requirements and purpose.



- **Authorisation.** Beyond the assurance level of Authentication, access need to be regulated – in both electronic and conventional health and social care services – according to roles that consequently need to be recognized within digital systems and also across national borders.



By asserting attributes associated to an identity it is possible to differentiate the various roles of a citizen (a patient, a health professional, a person entitled to insurance, a tax payer, etc). Since such attributes are often linked to formal qualifications and positions they are important enablers for the process of *Authorisation*. In eHealth, additional authorisation mechanism of health professionals to access patient data is needed in order to protect the confidentiality of the data, based on patient's consent.

Authorisation in eHealth therefore creates trust, in so far that the Health Professional is identified as a person who is fully qualified, accredited and competent to offer appropriate the services. It also guarantees that health professionals maintain their right to access patient information and perform electronic transactions within the remit of their currently valid identified status/position.