



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.