epSOS Local Data Providers

Fredrik Linden
Swedish Association of Local Authorities and Regions (SALAR), Stockholm, Sweden

SUMMARY: “epSOS local data providers” — is a local body that maintains registries and/or patient data on patients from some geographical area of the country. An epSOS data provider will have the legal status of data controller in country A. “epSOS Trusted Domain” should be perceived of as an extension beyond a certain national or regional territory where those national/regional eHealth services which are provided within epSOS can be delivered seamlessly to residents of these countries/regions travelling to destinations that are federated under this epSOS Trusted Domain. **Key words:** epSOS Patient data, patient summary, patient medication record

1. **EPSOS AS AN EU LARGE SCALE PILOT**

epSOS is a Large Scale Pilot that operates within a complex policy background and focuses on electronic patient record systems, with its initial focus on two cross border services, i.e., Patient Summary and e-Prescribing/e-dispensing. The aim of the pilot is to demonstrate that it is feasible for any Member State (MS) that already provides these eHealth services to insured persons, the epSOS pilots could work with minimal additional contractual documentation in a context which already provides an ideal opportunity to test the implementation and operation of the two cross-border interoperability pilot services which constitute the core of epSOS, Patient Summary and ePrescription. In the longer term, it will estimate and forecast the impact that epSOS may have on eHealth in Europe and provide recommendations for further development of cross-border eHealth, including recommendations on any legal and regulatory interventions which may be required for expanding to new cross border eHealth services and new countries.

Reimbursement of services is out of scope of epSOS. It appears however that the added value in epSOS would be mainly in the unplanned care scenario where results would in fact complement regulation 1408/71 and the European Health Insurance Card (EHIC) for reimbursement of health services to insured persons. Focusing on unplanned care will provide the greatest impact in terms of improvement of care; will allow a full exploration of a range of functionalities; and will minimize the constraints associated to the need to have prior established agreements for planned care delivery in another country.

The epSOS pilots will thus provide an ideal opportunity to test the extent to which the quality of unplanned care entitled to in accordance with the rules on citizen mobility in Regulation 1408/71, can be improved by timely access to summary patient data. Furthermore, given that Regulation 1408/71 and the EHIC already provide a basis for entitlement to unplanned care for insured persons, the epSOS pilots could work with minimal additional contractual documentation in a context which already provides a baseline before the use of epSOS services.

2. **ORGANISATIONAL AND LEGAL INTEROPERABILITY CHALLENGES IN epSOS**

The exchange of data which lies at the heart of the epSOS pilot requires that a sound framework of trust is
developed between all parties. The framework must ensure that healthcare professionals can rely upon the authenticity of the clinical data on which they will base decisions that suitable systems of security exist to ensure that data cannot be accessed by unauthorized parties and that patient rights of informed consent to data access are duly respected by all parties (authenticity, integrity and confidentiality).

In order to establish the framework of trust the project partners will agree a set of epSOS Framework contract and its related annexes which will govern the co-operative model of data exchange and form the documented basis for the trusted relationships between parties exchanging data. It will also serve as an aid to transparency, so that patients can be reassured that their legal rights to data privacy can be maintained in the cross border care setting. The core purpose of the framework contract and its related annexes will be to establish the epSOS Trusted Domain.

From a legal perspective, this means that MS, through their delegated national organisations, will enter into multi-lateral contractual arrangements based as closely as possible on the framework contract as local legislation allows. It is vital that such contractual agreements are comparable across the whole project (i.e. across all pilot sites) and that they all satisfy the local and EU level legal requirements on issues such as patient consent, data security, patient confidentiality, practitioner liability etc. Unlike other sectors, very little is regulated at EU level in terms of health systems and healthcare services as an EU issue is only now appearing on the European policy agenda. It must be remembered that according to the Treaty of the EU, healthcare is a matter of Member State regulation. The EU has legal competency on health matters is only insofar as they concern certain public health measures (art 152) and when they relate to matters of the fundamental freedoms of movement of people, goods and services. As a result, when a citizen receives health care services in another country, a number of issues lack legal certainty, such as: data exchange mechanisms, differing regulations on medicinal products and prescribing, variations in terms of HCPs duties and their roles, their work protocols and the national processes for accreditation, certification and audit of health care quality.

It is not for epSOS to confront this vast complexity but rather to establish a well delineated Trusted Domain within which it will establish and demonstrate conditions of organisational and legal interoperability based upon contractual agreements between existing systems, as an analogue to the technical interoperability which is another major objective of epSOS.

As highlighted above, building trust is central to all initiatives aiming to strengthen mobility and the internal market. A common element of such initiatives is to establish national nodes with particular legal and administrative duties focused on facilitating the cross border exchange. While MS normally have the responsibility for organising their internal process, within the epSOS pilots they are accountable to the other MS and they must demonstrate that they meet certain agreed essential requirements.

A certain level of legal certainty around Data Protection and Confidentiality exists at EU level because Data Protection and Confidentiality have been regulated at this level and the relevant directives have been transposed into national legislation. Although significant diversity still exists in the way transposition has been realized, there are sufficient pre-conditions and EU level interpretation guidance to allow optimism that these core issues of trust can be successfully addressed through well documented agreements which address the human processes of delivery of the epSOS services as well as the technical requirements of data protection. The main challenge of epSOS in this domain is to arrive at an EU level Information Governance, building on national high level policies of good information sharing practices and auditable processes. The concept of the NCPs and their role will be also critical in terms of federating different systems under a common Trusted Domain.

There is however insufficient legal certainty in terms of harmonisation in other aspects of the health service sector and building trust in epSOS will require – besides federating national systems and registers e.g. for identification and authorization of health professionals – an understanding of the processes at the level of the respective national authorities, so that appropriate standard terms and guidelines can be drawn up which will allow the epSOS partners to establish the Trusted Domain through which the epSOS services will function.

3. The epSOS Approach

In this landscape of existing uncertainties and on-going developments in several areas adjacent to epSOS, the project is challenged to adopt a strategy that will allow it to fully and successfully address its focus and scope; generate the maximum impact; and contain the complexity of its surrounding environment to a minimum.

The challenge is then to create conditions that will allow for health data exchange across as many of the epSOS MS as possible, whilst respecting all legal duties AND establishing a sense of trust in the system for all parties (authorities, providers and patients). Before this can become feasible all necessary privacy and quality and other legal requirements must be addressed in a mutually acceptable manner across all participating States.

The primary method for developing such a mutual acceptance will be by addressing as many as possible of these requirements in the design of the epSOS components. Building Trust by design in epSOS will guarantee a uniform application of tools to support trust and will ensure that traceability and audit of these elements lies at the heart of the system and are regulated within the system. However, it will not be possible address all legal and quality requirements in the system design and thus a number of them will need to be translated into auditable processes.
to be implemented alongside as con-
tactual and procedural elements of the epSOS services. In other words some human involvement is expect-
ed to be necessary. Therefore epSOS will not only deliver a technical spec-
fication but also an information gov-
ernance framework that will comprise policies, processes and audit mecha-
nisms that will be adopted by all ep-
SOS partners. Adherence to such requirements will need to be also contractually enforced and the con-
tactual documents that pilot sites will be required to sign will include provisions for applying and regularly auditing the epSOS information governance.

In the end there may still be some residual requirements that we will not be able to meet in this pilot. We will then need to consider either reducing the scope of the pilot trial or treat the issues on a case by case basis.

Hence the aforementioned framework contract will ensure that the NCPs have common legal duties and operate on the same rules, as far as local requirements allow. Health care systems are not to be influenced and the role of the project is rather to work with what is possible within currently existing legislation. In areas such as data protection where transposition of EU directives has already taken place this will be relatively straightforward. There are however fundamental legislative is-
tuats that are not regulated at EU lev-
el, e.g. the regulations on medicines in each country that will need to be dealt with on a case by case basis, apply-
ing the principles outlined below.

The epSOS National Contact Point as already set out in the Initial Scope, takes care of external and internal national communication in the epSOS project and the semantic mapping between information on either side. It is therefore at this level that the epSOS Trusted Domain may be established (upper horizontal circle in figure). The NCPs will be fur-
thermore responsible towards all MS partners in epSOS for securing that the needed processes are properly implemented at their own networks which will be typically points where care is delivered.

A Point of Care (PoC) maybe a hospital, an individual practice, a pharmacy, an emergency vehicle or any other point of the health care system, of country B, participating in the epSOS pilot, that the mobile citi-
zen will come in contact with. Ob-
viously a cycle of trust is also needed reaching down to this level (vertical circle in figure). Trusting the PoC depends upon local processes and procedures. Minimum requirements are expected to emerge from epSOS. This will most likely mean that re-
quirements for some new or amended processes may emerge, varying from country to country. Establishing this trust is a responsibility of the NCP and epSOS is expected to provide guidance on how local contract terms should be established, leaving it up to each MS to imple-
mant them (see expanded text, in Annex A).

Besides facilitating and controlling access to patient data from abroad, the NCPs will also provide the possi-
ibility for country A to update patient data with that generated in country B, if so decided by country A. The PoC will send a re-
cord of the care episode to its national NCP. The NCP forward that record to the NCP in the patient's home country. It is a matter of national procedures established if the record of 'foreign' care is in anyway integrated into the local record or the epSOS Summary.

It is envisaged that for the pur-
puses of running the pilot an audit-
ning mechanism within the network of NCPs will be established. How-
ever in the future a permanent mech-
nanism for maintaining and expand-
ing the epSOS trusted domain and elaborating further requirements for audits and auditing entities will be needed and will be addressed by ep-
SOS Recommendations.

In terms of the organisation-
als regulation of healthcare delivery, including issues of profes-
sional accreditations, the prin-
ciple to be applied is that, nation-
al regulations in the country of care delivery apply to the episode of care that is, the epSOS pilots must not require any changes to national health systems (Similar aspects are being explored in the context of the broader discus-
sion around the patient directive and the telemedicine initiatives, which is presently taking place at EU level). A citizen from coun-
try A, visiting country B will re-
cieve services as they are offered to the residents of country B, augmented only by the possibil-
ity to inform better medical decisions in country B through the epSOS services.

It should be also noted that the Country of Affiliation, is the country where a citizen pays taxes and health insurance, and in return he gets health (and eHealth) services. This is the only country with responsibility of maintenance of EHRs and patient summaries. Country B could maintain information collected on care episodes for a patient of country A for legal and reimbursement purposes. However, there is no obligation to maintain health records of any kind be opponent A's NCP. Transferring clinical information is out of scope. It is however understood that not returning to NCP(A) critical clinical findings may have safety implications for epSOS. The challenge will be addressed as part of the epSOS services workflows and service quality within Work package (WP) 3.8.

**Example 1:** if in Country B nurses may access HC information for the purposes of providing care, while in home country A where the record is generated a similar function is not permitted for nurses, then in the visited country a nurse may be given access to health care data for the purposes of providing care from the home country, even though a home country nurse would not have the same access to HC data.

**Example 2:** if a patient seeks to fill a prescription for a drug X issued in his home country, but drug X is a controlled drug in the visiting country and may not be dispensed, then the patient will not be able to obtain the drug.

**Example 3:** if a patient seeks to fill a nurse prescription from home country, but nurse prescriptions are not valid in visited country, the prescription will not be dispensed.

**Example 4:** If access to the medication summary is prohibited for a certain function in the health care system of country A e.g. “dispenser”, then such information will not be made available to the equivalent dispenser function in country B, even if such access is permitted in country B.

**Example 4B:** If however a patient from country A, was to have a medication summary created and maintained in country B, then the function “dispenser” in country B would have access to this information, unless otherwise decided by the patient through his/her free patient consent choice. Similarly, dispensers from other epSOS countries will be provided access to this information if not restricted by patient choice.

Given the potentially large variations in practice, and in order to secure wide acceptance, epSOS should foresee the elaboration of specific safeguards where needed in close collaboration also with EU level professional associations, and stakeholders.

**Patient Consent** may be requested for access to health data by any trusted entity, anywhere, anytime within the epSOS pilots trusted domains. In order to achieve at a high level of trust the system must be able to verify conditions for trust in every encounter by checking against a number of safeguards i.e., a licensed professional requesting the access, and the ID of the patient is matched to the ID of the electronic record and the access is requested in the context of care provision. (see Annex B on Patient Consent).

Patient Consent is not the only issue which requires some epSOS level consensus, we will also need to consider issues such as the different interpretations of professional roles and accreditation in different epSOS partner countries, as well as the complex issue of shared liability between co-operating partners. These issues will be addressed within the framework contract terms.

4. ESTABLISHING EPSOS TRUSTED DOMAINS

In the current phase of the project, all work packages of Project Domain 3 (technical) will be contributing to the establishment of the Trusted Domain by incorporating privacy into the design of the epSOS system. The following are examples of WPs that are expected to develop the Trusted Domain through policies and processes for delivery of the epSOS services.

**WP 3.6. Identity Management** will further explore technical solution for acquiring and verifying Patient consent that will maximize privacy by design and will propose optimized solutions that are realistic, practical and ensure free, specific and informed consent.

**WP 3.7. Security Services,** in effectively tackling the different security levels applied by the MS, may need to integrate realistic, efficient and auditable safeguards as part of the epSOS Security Policy, define roles and responsibilities for security at NCP and PoC level and make proposals for measures to ensure conformance to epSOS security policies. Furthermore, WP3.7. is expected to establish procedures for data anonymisation and code of practice when processing the system logs and user-provided content.

**WP3.8.Integration and customisation** will address issues of quality of the epSOS services, including provisions for patient safety in terms of potential risks associated with the provision of epSOS services.

**WP 3.1., WP3.2. Patient Summary and e-prescribing** in proposing functional specifications for services, may need to consider additional safeguards in terms of processes at the point of delivery of the service such as obtaining patient consent if not available or providing needed information to patients.

**WP3.8. Integration and Customisation,** in establishing guidance for pilots for connecting the local pilots to the international epSOS infrastructure, may consider establishing an guide for applying and auditing epSOS Information Governance.

**WP1.2. Evaluation** in evaluating the feasibility and applicability of these concepts.

REFERENCES


Corresponding author: Fredrik Linden. Swedish Association of Local Authorities and Regions (SALAR). E-mail: Fredrik.Linden@skl.se