



00145/12/EN
WP 189

Working Document 01/2012 on epSOS

Adopted on 25 January 2012

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

1. Introduction

The objective of this Working Document of the Article 29 Working Party is to provide guidance on data protection issues in relation with the epSOS (European Patients Smart Open Services) project. It is not the intention of this paper to present a comprehensive view on all specific aspects of the epSOS project. The paper intends to clarify the most important principles of the EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995/46/EC). The paper also deals with how the analysis of the Directive provided in the Working Document on the processing of personal data relating to health in electronic health records (WP 131), should be interpreted in the case of the epSOS project.

This paper does not, however, touch on the duty of all the organizations involved in the epSOS project to comply with the rules on personal data established by the national laws transposing the Directive 1995/46/EC. Therefore, further guidance, assistance and supervision may be provided by the data protection authorities in the Member States.

EpSOS is a pilot¹ that offers cross-border e-Health Services to European citizens. It focuses on developing a practical [e-Health](#) framework and ICT (information and communication technology) infrastructure that enables access to patient health information from different European healthcare systems. It aims at improving the quality of healthcare for citizens when travelling to another European country. EpSOS is being tested in two pilot phases. Different Member States are participating in these pilots. The pilot of the first phase of epSOS is about to start and the technical, legal and organizational concepts for the second phase are being established.

There are two uses for epSOS:

- a Patient Summary containing medical data and accessed by healthcare providers for patient treatment and
- the cross-border use of electronic prescriptions ("ePrescription" - or "eMedication" systems).

As the epSOS project is still developing, its technical, legal and organizational concepts have not yet been fixed. Therefore the Working Party cannot make a final assessment at this stage.

The EU Directive on the application of patients' rights in cross-border healthcare (2011/24/EU) aims to establish rules for facilitating access to safe and high-quality cross-border healthcare in the Union, to ensure patient mobility and to promote cooperation on healthcare between Member States. It applies to patients who decide to seek healthcare in a Member State other than the Member State of affiliation. It respects the responsibilities of the Member States for the organization and delivery of healthcare and medical care. Similarly, this paper respects the responsibilities of the Member States for the organization and delivery of healthcare and medical care and does not wish to address national health or e-Health systems.

¹ Preliminary project involving real data.

However, the Working Party is well aware that there is a huge variation in circumstances between Member States with regard to the legal, technical and organizational preconditions as well as with the status and planning of respective national e-Health frameworks and ICT infrastructure. It also realizes that there is variation in the interpretation of the EC Directive 1995/46/EC in the health sector and that these variations may play a role in the field of supranational data processing.

Given this complex and disparate landscape and the preliminary character of the epSOS project, the task of producing recommendations is potentially challenging. At this stage it seems that the recommendations can only be general rather than specific.

Even if the scope of this paper is not exhaustive, the issues raised need to be understood and discussed with regard to future cooperation between Member States. In particular, the Working Party intends to clarify some of the major challenges and data protection issues that may arise and will have to be addressed in the context of cross-border projects involving health data. Future cooperation in this area might be jointly supervised by the competent national data protection authorities (see below for further details).

The paper seeks to address the following issues;

- the legal basis of the data processing in the project including the principle of proportionality and purpose limitation,
- organizational questions,
- transparency and,
- data security.

As this document deals mainly with data processing in electronic health records, it should be read as a complementary document to WP 131 on the processing of personal data relating to health in electronic health records (EHR).

2. Description of the epSOS Project

EpSOS is a Large Scale Pilot that focuses on electronic patient record systems, with an initial focus on two cross-border services, i.e., Patient Summary and ePrescription. In the short term, the epSOS project will examine the design, development, implementation and operation of those two cross-border interoperability pilot services which constitute the core of the system. In the longer term, epSOS will also estimate the impact that the project may have on e-Health in Europe and provide recommendations for further development of cross-border e-Health, including recommendations on any legal and regulatory interventions which may be required for expanding to new cross-border e-Health services and new countries.

It is in the context of the preparation and development of the two core services (Patient Summary and ePrescription) that the present paper should be considered.

For both services a Member State can take up the role of "country A" and/or "country B". "Country A" is the Member State of affiliation, i.e. the state where personal health data of an epSOS patient is stored and where he or she is insured. "Country B" is where the cross-border healthcare is provided when the patient seeks care or dispensation abroad. This is a different country, where information about a patient is needed to support the provision of healthcare².

Participating Member States (as country A and/or country B) must each designate a "national contact point" (NCP). This legal entity assumes all legal duties nationally and is contractually bound to safeguard the "epSOS trusted domain" in terms of all national matters.³

Data exchanges will take place directly between these NCPs. But the epSOS project does not have a central network facility. The data processing operations at NCP level are, however, regulated by common security and communications standards and supported by central services and directories.

epSOS itself describes the general workflow as follows:

- a patient seeks treatment from a health care professional (HCP) in country B;
- the HCP issues a patient identification and confirms patient consent for access to data for the purposes of the specific care encounter. If affirmative the HCP confirms to NCP in country B and issues a subsequent request;
- the NCP in country B relays the request and patient consent confirmation to the NCP in country A for further processing;
- NCP in country A satisfies its local and the epSOS security policy and answers the request accordingly;
- NCP in country B processes the received information and relays to the requesting HCP;
- HCP in country B indicates dispensation information. The information is relayed by NCP in country B to the NCP in country A.

Between participating Member States (as country A and/or as country B) the "epSOS trusted domain" is established. This is defined as:

*"The epSOS trusted domain is comprised of epSOS NCPs and their national contractual partners which collectively fulfill all technical, legal and organizational requirements, for safe delivery of epSOS services and secure and confidential transfer or storage of data resulting from healthcare encounters as appropriate, within the epSOS Trusted Domain, according to this framework agreement."*⁴

² See the following document published by epSOS: "D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites", p. 7
(http://www.epsos.eu/uploads/tx_epsosfileshare/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf).

³ The concept of a "trusted domain" will be explained later on in this chapter.

⁴ See the following document published by epSOS: "D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites", p. 8
(http://www.epsos.eu/uploads/tx_epsosfileshare/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf)

As can be deduced from the description of the "epSOS trusted domain", the pilot project is supposed to be carried out using contracts or ordinances⁵ between participating Member States and the epSOS project, between Member States and their respective NCP, as well as between NCPs and Health Care Professionals. epSOS will draw up a standard contract that can subsequently be adapted by NCPs to suit their national needs. The final contract nevertheless has to be approved by the epSOS project steering board (in order to avoid that contracts would be too divergent in the various Member States and to ensure that the contracts respect a number of minimum principles).

An important element here is that the epSOS project itself points out that this use of contracts can only be maintained for the duration of the pilot project: *"This mechanism is however, not sustainable after the end of the project and will need to migrate to a permanent mechanism if the services are to be widely deployed and offered on a routine basis"*.⁶

3. Legal Basis & Proportionality

- **General remarks on the legal basis**

The right of data protection is a fundamental right stated in Article 8 of the EU Charter of fundamental rights. According to this provision, everyone has the right to the protection of their own personal data. Such data must be processed fairly for specified purposes and either on the basis of the consent of the person concerned or some other legitimate basis laid down by national law. Everyone has the right of access to data which has been collected about them and the right (if incorrect) to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

Under certain conditions data protection rights can be restricted. However such a restriction must be regulated and carried out in line with the principle of proportionality (see below chapter 5).

Furthermore, the wider general legal basis for the processing of health data from health records as well as for electronic prescription can be gleaned from the detailed comments laid down in WP 131 which elaborates the relevant provisions of Directive 95/46/EC.

The **general principles** laid down in Article 6 of the Directive must also be taken into account. These include, in particular, the purpose limitation principle, the proportionality principle, the data quality principle and the principle which requires personal data to be kept for no longer than is necessary for the purposes for which the data were collected or further processed. Furthermore other general principles such as the information requirements, the data subject's right of access, rectification and deletion and security related obligations have to be observed.

⁵ Ordinances could be used to regulate the relationship between the government/state and an NCP.

⁶ See the following document published by epSOS: "D.2.1.2. Legal and Regulatory Constraints on epSOS Design-Participating Member States. Standard contract terms for MS Document for Engagement of Pilot Sites", p. 19 (http://www.epsos.eu/uploads/tx_epsosfileshare/D2.1.2_Standard_Contract_Terms_for_MS_Document_for_engagement_of_pilot_sites_01.pdf)

In addition, and as set out in WP 131, all data contained in medical documentation, in electronic health records and in EHR systems should be considered to be “**sensitive personal data**”. Therefore, they are not only subject to all the general rules on the protection of personal data in the Directive, but also subject to the special data protection rules on the processing of sensitive information contained in **Article 8** of the Directive.

- **Applicability of Article 8 of the Directive**

Article 8

Article 8 (1) of the Data Protection Directive 95/46/EC prohibits the processing of personal data concerning health in general. Article 6 of the Council of Europe Convention No 108 prohibits automatic processing of such data “unless domestic law provides appropriate safeguards”. However, considering the importance of using information about a patient in order to provide appropriate medical treatment, there are exemptions to the general prohibition of processing medical data. The Directive provides for mandatory derogations laid down in Article 8 (2) and (3) plus an optional exemption in Article 8 (4). All these derogations are limited and have to be construed in a narrow fashion.

Article 8 (3)

According to Art. 8 (3) of the Data Protection Directive 95/46/EC, the prohibition to process personal health data shall not apply where the processing of the health data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

In WP 131 Article 8 (3) is construed in the following way (page 10):

*This derogation only covers processing of personal data for the **specific purpose** of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature and for the purpose of the management of these healthcare services, e.g. invoicing, accounting or statistics.*

Not covered by this derogation is further processing which is not required for the direct provision of such services, such as medical research, the subsequent reimbursement of costs by a sickness insurance scheme or the pursuit of pecuniary claims. Equally outside the scope of application of Article 8 (3) are some other processing operations in areas such as public health and social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, as these are mentioned in recital 34 of the Directive as examples for invoking Article 8 (4).

In the epSOS case it seems that processing probably will take place outside the specific purposes mentioned in Art. 8 (3) of the Data Protection Directive as interpreted by the WP 131.

No general guarantees can be upheld against further processing in country B for other purposes than to provide and manage health-care. For example some countries have national legislation which obliges health care providers to give away data in electronic health care records to research institutes without the consent of the patients, no matter if the data originates from epSOS or from a national health care provider only.

The same is also valid for the NCPs; depending on national legislation and the legal basis for each NCP, there are no guarantees that NCPs, in either country A and B, will not have to use or give away the sensitive data that they process for other purposes than for epSOS .

In addition to this, no solution has been presented which would guarantee that only staff bound by professional secrecy will be able to access data within epSOS.

As a consequence of the aforementioned circumstances, in the future it would require limitation and specification of the epSOS purposes and usages if Article 8 (3) could be taken into consideration as a legal basis for epSOS. EpSOS in its current shape does not appear to fulfil these requirements.⁷

Article 8 (4)

Referring to substantial public interest exemptions laid down in Article 8 (4) of the Directive, some of the Member States might have an explicit legal basis for the transfer of health data to other health care providers within the EU. However, this is not the case in all Member States. In addition such a legal basis on national level could only regulate the transfer of health data to other health care providers (who are located in another Member State, country B), but not the use of the data by these health care providers in country B.

Conclusions

Therefore the Working Party is of the opinion that the **explicit consent** [(Article 8 (2) (a)] and the **vital interest of the data subject** [Article 8 (2) (c)] can serve as an appropriate legal basis for the processing of personal data in the framework of the epSOS project, in its current shape.

- **Explicit consent and information**

Article 8 (2) (a) of the Directive reads as follows:

“Paragraph 1 shall not apply where: (a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent;”

The necessary elements of consent are elaborated in the opinion on consent (WP 187). WP 131 deals specifically with health data. The following elements are contained in both WPs:

⁷ As the epSOS project has not clarified its purposes in a way complying with Article 8 (3) so far, it could also be considered uncertain whether the processing of health data is “required” for the purposes mentioned in Article 8 (3).

“Consent must be a “freely given, specific and informed indication of the data subject’s wishes”, as defined in Article 2(h) of the Directive.

‘Free’ consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as ‘free’. Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a fait accompli cannot be considered to be valid. The individual data subject has a genuine free choice and must be subsequently able to withdraw the consent without detriment.

‘Specific’ consent must relate to a well-defined, concrete situation in which the processing of medical data is envisaged. Therefore only a ‘general agreement’ of the data subject e.g. to the collection of his medical data for an EHR and to subsequent transfers of these medical data of the past and of the future to health professionals involved in treatment would not constitute consent in the terms of Article 2 (h) of the Directive.

‘Informed’ consent means consent by the data subject, based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question.

*In contrast to the provisions of Article 7 of the Directive, consent in the case of sensitive personal data and therefore in an EHR must be **explicit**. Opt-out solutions will not meet the requirement of being ‘explicit’. In accordance with the general definition that consent presupposes a declaration of intent, explicitness must relate, in particular, to the **sensitivity of the data**. The data subject must be aware that he is renouncing special protection. Written consent is, however, not required.*

*Again in contrast to Article 7, Article 8 (2) (a) acknowledges that there may be cases of processing of sensitive data in which **not even explicit consent** of the data subject should lift the prohibition of processing: Member States are free if, and how to regulate such cases in detail.”*

- **Two-steps-consent**

The Working Party recommends that a **two-steps-consent** by the data subject to the transfer and processing of health data should be envisaged. Firstly an explicit consent should be given to the participation of the data subject in the epSOS project or parts of it (for example in the form of modular access rights for health care providers, see below). This first consent in country A would allow the health care providers to prepare specific data with the intention to make them available in future to other health care providers in the framework of epSOS. The first consent would be required only once at the point where (actually before) the data subject’s data are prepared or made available to the system. Therefore it follows, that the first consent necessarily has to be given before the second consent. If there, following the first consent, are any major changes in the processing of data within epSOS, a new consent will be required.

The need of a first consent could also provide the side benefit of limiting the number of data subjects available within the system to the strictly necessary and thereby also limiting the potential damage in case of unlawful access to this sensitive data.

In order to facilitate making the benefits of epSOS available to data subjects who need treatment in country B but have not previously given consent in country A, the epSOS project could investigate the possibility of allowing patients to give also their first consent for instance in a secure way over the Internet in country B.

The second consent shall be given explicitly for the processing of health data in the case of actual treatment in country B.

As mentioned above, one of the preconditions for a valid consent is that the data subject has received **information** (from the controller or his representative) which satisfies the requirements of the Articles 10 and 11 of the Directive.

The information regarding the **first consent** should contain a comprehensive, clear and understandable description of the epSOS project, mentioning at least the categories of data that would be transferred by which health care providers to which other health care providers and other institutions. This includes the institutions involved in the further processing of the data in country B for other purposes than to provide and manage health care. Information must also be provided about the purpose of the transfer and how long the data would be stored. Finally it must be made clear that there is the option of withdrawing consent at any time. The data subject should also be informed about the right of access and rectification of data concerning him/her.

The information given before the **second consent** must at least contain the explanation which health care provider and other institution will process which categories of data and for which purpose.

The patient should also have the possibility to give his/her consent only to the transfer and processing of certain categories of health data (**modular** access rights for health care providers in another country). Finally it must also be made clear that there is the option of withdrawing consent at any time. The data subject should also be informed about the right of access and rectification of data concerning him/her.

- **Vital interests of the data subject**

Article 8 (2) (c) of the Directive 95/46/EC sets out that the processing of sensitive personal data can be justified if it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent. The processing must relate to essential individual interests of the data subject or of another person and it must – in the medical context – be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions (emergency case). Accordingly, this exception could be applied only to a small number of cases of treatment and only where the first consent of the two-steps-model has been given. It is of great importance that the scope of this exception should be narrowly defined as to when and how it can be applied. Also, technical measures should be employed in order to prevent misuse of the emergency case.

With regards to the exchange of data in such cases in the epSOS project, the data subject should be informed about it in the general information concerning the epSOS project

In this situation it is especially important that the patient is given access to information about the transmissions that have taken place(see further in the chapter on transparency).

- **Proportionality and purpose limitation**

The “principle of proportionality” is one of the general principles of European Union law. It requires that any measure affecting individuals’ rights is appropriate for attaining the objective pursued and does not go beyond what is necessary to achieve it. Article 6 of the Directive incorporates this principle, by stating that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. In addition, it also establishes that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

As mentioned above, all data contained in medical documentation, in electronic health records and otherwise in EHR systems should be considered to be “sensitive personal data”. As it has been already stated, a consequence of this is the general prohibition of processing such data, except in some specific cases. Simultaneously, any derogation to be applied to this general rule should be interpreted as limited and has to be construed in a narrow fashion. This applies to data included in the electronic Patient Summary and ePrescription.

As it has been explained above the explicit consent of data subjects, or an action to protect their vital interest, could serve as an appropriate legal basis for the processing of health-related personal data in the framework of the epSOS project. However the processing of such data must be **strictly limited to the minimum necessary to the fulfilment of the epSOS purposes**. Only relevant information in relation to the epSOS purposes should be recorded into the Patient Summary and ePrescription.

Moreover, information should not be retained in these services for longer than necessary, as set out in article 6.1(e) of the Directive.

Each query for personal data available through the epSOS system should be based on the existence of a real need to access specific data related to the care or treatment to be provided or the medicine to be prescribed or dispensed.

As stated in WP 131, only those healthcare professionals/authorized personnel who are involved in the patient’s treatment may access medical records, and therefore the epSOS Patient Summary and ePrescription information. From the wording of the documentation provided to the Working Party, there does not seem to be a requirement for the NCPs to store medical information for the fulfilment of the epSOS purposes, so the retention of such data by the NCPs should be avoided.

However, in case personal data has to be stored, for example at the NCP, the epSOS project should decide on a maximum retention period and also on a common procedure as to what shall happen to the data at the end of the retention period.

Accessing data through the epSOS system for purposes other than the provision of care or treatment to patients and the prescription and dispensation of medicines should be prohibited.

Nevertheless, the principle of proportionality cannot be tackled in an isolated way, due to its clear link with the principle of purpose limitation. Therefore in order to properly assess how those requirements should be put into place in practice it is necessary to clearly identify the legitimate purpose or purposes for which the epSOS project intends to process personal data. As stated in the Directive, such purposes must be specific and explicit, that is, determined in a precise and well-defined manner, so generic approaches could not be sufficient. The "provision of care or treatment" and "the prescription and dispensation of medicines" are, of course, legitimate purposes, but the Working Party wonders whether they are sufficiently and precisely describing the aims and activities of epSOS. Moreover, any other envisaged purposes must be defined prior to any processing, in order to warrant that no more personal data than is necessary will be processed, and therefore to properly comply with the requirements of Community law.

- **Legal instrument as basis for the system**

Thought could be given to developing a legal instrument on the EU level which would regulate the epSOS-system and the data protection roles of the different "players" (health care providers, national contact points etc.). Under the precondition that the epSOS project will be developed into an "EU-project", it should be explored whether the European Commission could issue a Commission Decision in order to further regulate the system.⁸

Moreover, the EU Directive on the application of patients' rights in cross-border healthcare (2011/24/EU) will be transposed by 25 October 2013. It would be reasonable to assume that national provisions will be adopted to comply with it. The requirements for the exchange of information among Member States are subject to discussions of the eHealth network according to Art.14 of the directive 2011/24/EU .

4. The epSOS project: organizational issues

This chapter is limited to the supranational epSOS processing which will be developed on top of the existing national eHealth systems. This section does not deal with the national systems since they are – as such – not affected by the epSOS project.

- **Background**

The epSOS system is a communication system between all participating NCPs without a central network facility.

It works as follows: a HCP - Health Care Professional - (country B) requests for information about patient X who resides in country A. NCP (country B) then requests for information

⁸ Such a decision could be comparable to the Commission Decision 2008/49/EC of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data.

about patient X at NCP (country A). If any information about patient X is found in country A it is transmitted from NCP (country A) to NCP (country B). NCP (country B) transmits the information about patient X to HCP (country B).

So, the epSOS system essentially consists of a multitude of point-to-point connections, however these are regulated by common security and communications standards and supported by central services and directories:

*"The epSOS NCP interfaces regard to services provided and consumed by other NCPs of the epSOS infrastructure. epSOS interfaces are "normative" for an epSOS NCP. An NCP is a "participant" of epSOS world if and only if it is compliant to normative epSOS interfaces in terms of structure, behavior and security policy. The main part of this service is related to NCP to NCP exchange, but some common utility services can be centralized now or in the future."*⁹

*"There are a number of information sources which are relevant for every NCP and must be in the same state for every NCP. Examples for this are common taxonomies, schemas, and WSE addresses of NCPs. This shared data is centrally managed in order to avoid inconsistencies and version conflicts in a generalization process of epSOS."*¹⁰

- **The processing**

In terms of Article 2 (b) of Directive 95/46/EC country B retrieves the patient data disclosed (by transmission) by country A.

The exchange of patient data between country A and country B can be considered as a *set of* (these two) *operations*.

- **Who is the controller?**
- *The NCP*

Article 2 (d) of the Directive reads as follows:

"'Controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations the controller or the specific criteria for his nomination may be designated by national or Community law.

Further definition is provided in the Opinion on the concepts of "controller" and "processor"¹¹.

Some crucial elements of the definition of "controller" are pointed out below.

⁹ D3.3.2 Final epSOS System Technical Specification, version 1.4 (april 2010), p. 64.

¹⁰ D3.3.2 Final epSOS System Technical Specification, version 1.4 (april 2010), p. 71.

¹¹ Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

- "determines"

(1) "[O]ne should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions "why is this processing taking place? Who initiated it?"." (p. 8 of the Opinion on the concepts of "controller" and "processor")

(2) "The concept of controller [...] should be interpreted mainly according to Community data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis." (p. 9 of the Opinion on the concepts of "controller" and "processor")

- "purposes and means"

(3) "[M]eans" does not only refer to the technical ways of processing personal data, but also to the "how" of processing, which includes questions like "which data shall be processed", "which third parties shall have access to this data", "when data shall be deleted", etc." (p. 14 of the Opinion on the concepts of "controller" and "processor")

The epSOS project paper sets out the following:

"A "country" in epSOS is represented by one single legal entity, which then assumes all legal duties and is contractually bound to safeguard the epSOS trusted domain in terms of all national matters. This legal entity is referred to as the National Contact Point (NCP). [...] The NCP in each country will also assume the responsibility of ensuring that patient rights according to their national legislation are appropriately handled [...]."¹²

This epSOS view is aligned with the earlier analysis of Article 2 (d) of the Directive.

Therefore, starting from the definition of "controller" in WP169 on the one hand and from the epSOS project's own description of the facts on the other, it appears that the NCP in country A is controller for the *disclosure* of the patient data, and the NCP in country B is controller for the *retrieval* of the patient data.

However, the results of the questionnaire reveal there might be a different national reality.¹³

There is also a certain regulatory role at an EU level because of the delivery of central services by the epSOS project and the security and communication standards; however this is not an EU role of direct involvement in the data processing. Other issues are the acceptance of new participants and the provision of information to data subjects (e.g. www.epsos.eu). If this pilot system becomes a permanent set-up, there might be reason to designate a separate body being the controller - alone or jointly with the participating NCPs.

¹² D2.1.2 Legal and Regulatory Constraints on epSOS Design- Participating Member States, January 31,2010, Final version, p. 14

¹³ For example in decentralized systems. See the answers to question 8e) in the Questionnaire concerning the EPSOS project; patient summary and electronic prescriptions (Aug 2011), p. 27-28 (annexed).

- *The health care providers*

Firstly, the health care providers are controllers for the *creation* of the medical records from which the epSOS datasets are derived and sent abroad.

In certain EU Member States all participating healthcare providers are also supposed to be jointly controlling the NCP processing, the NCP acting as a processor.¹⁴

The concept of *joint control* has been analysed in WP 169. The background is the *function* of the concept of "controller":

"[T]he provisions on the rights of the data subject, to information, access, rectification, erasure and blocking, and to object to the processing of personal data (Articles 10-12 and 14), have been framed in such a way as to create obligations for the controller. The controller is also central in the provisions on notification and prior checking (Articles 18-21). Finally, it should be no surprise that the controller is also held liable, in principle, for any damage resulting from unlawful processing (Article 23).

This means that the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to allocate responsibility." (p. 4)

This function (co-)determines the extent to which joint control is acceptable:

"[Th]e assessment of joint control should take into account on the one hand the necessity to ensure full compliance with data protection rules, and on the other hand that the multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing." (p. 24)

Accordingly, if all participating healthcare providers in a country are supposed to be jointly controlling the NCP processing¹⁵, such a scattered control can raise serious doubts.¹⁶ These doubts might be mitigated by appropriate measures to safeguard patients'¹⁷ rights and to guarantee transparency.

- **Concluding remark with regard to epSOS regulation**

Where the purposes and means of the epSOS processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law (Article 2 (d) of the Directive).

¹⁴ In some countries, each health care provider is supposed to be joint controller – together with the NCP – of the NCP processing.

¹⁵ Or if each health care provider is supposed to be joint controller together with the NCP.

¹⁶ See also Example No. 15 in WP 169, p. 24.

¹⁷ See p. 17, par. 3 for an example of such a measure.

- **Supervision, prior checking and notification**

Following this analysis and pursuant Articles 4 and 28 of the Directive, there is currently no data protection supervisor for the whole epSOS processing. Each data protection authority supervises his own NCP. Because of the trans-border character of the epSOS processing, co-operation between national DPAs in supervising the epSOS project is strongly recommended (see Article 28 (6), second sentence of the Directive).

Every controller must, if it is provided for by the applicable national law, notify the data protection authority in his own Member State before carrying out any processing operations (Article 18 (1) of the Directive).

Dependent on national law a check will be carried out prior to the start of the processing (Article 20 of the Directive).

5. Transparency

- **Access & Rectification, Erasure and Blocking**

Data which are inaccurate or incomplete must be erased, rectified or blocked. The assessment of whether data are accurate must consider the purposes for which the data were collected or for which they are further processed. As a result the accuracy of a medical diagnosis can normally be disputed with the support of data protection principles only if there has been an error concerning the identity of a patient or if a similar major mistake has been made.

In order to make it possible for data subjects to safeguard their rights, a common epSOS website should be constructed which specifies the rights of the data subjects according to the different legislations of all the participating states. The information on the website should in a clear way specify the rights, conditions and practicalities according to each national legislation. The information should be understandable and easily available on the Internet in the languages of the participating states.

A data subject should be able to ask questions about access and the possibility of rectification/erasure/blocking to any of the controllers as well as to any other body involved in the exchange of information within the epSOS project. A request for access or for the rectification/erasure/blocking of data which is given in to an epSOS partner who does not handle the requestor's data, should be forwarded to the correct data controller within the epSOS system even if they are situated in another Member State.

The epSOS project should investigate the possibility of giving to data subjects direct (electronic) reading access to their own data. The data protection right of access e.g. under Article 12 of Directive 95/46/EC need not necessarily always mean *direct* access. Direct access might, however, contribute considerably to trust in the epSOS system. From a data protection point of view a precondition for granting direct access would be secure electronic identification and authentication in order to prevent access by unauthorized persons. (see WP 131 page 15)

All data controllers who handle epSOS data, no matter on what level or in which role (e.g. as health care provider, dispenser of e-prescriptions, National Contact Point, and so forth) must give data subjects the *right to access to and the right to the rectification/erasure/blocking of his or her own data*, regardless of whether the data subject is a national or resident of another Member State and regardless of whether the relevant data derives from data controllers in other Member States.

The right to access and rectification/erasure/blocking must be applied in accordance with the national law to which the data controller is subject. In exceptional cases, restrictions or limitations to data subjects' rights of access and rectification/erasure/blocking of data may be applicable under national data protection laws transposing Directive 95/46/EC.

No data controller who processes data in the epSOS project can refuse access or the rectification/erasure/blocking solely on the ground that the data controller itself did not introduce the data to epSOS.

Relevant law: According to Article 12 of the Directive, Member States shall guarantee every data subject the right to rectification, erasure or blocking and to obtain certain information from the controller. According to Article 13.1 of the Directive, Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Article 12 when such a restriction constitutes a necessary measure to safeguard certain specified interests.

- **Notification**

All data controllers who handle epSOS data, no matter on what level or in which role (eg. as health care provider, dispenser of e-prescriptions, national contact point, etc) *must notify* their national supervisory authority in accordance with relevant national legislation, regardless of whether the data subjects are nationals or residents of another Member State and regardless of whether the data which is handled derives from data controllers in other Member States.

Relevant law: Article 18 of Directive 95/46/EC sets out an obligation to notify the supervisory authority before carrying out any automatic processing operation, and also specifies the situations which may be exempted from this obligation.

6. Data Security

Because of the way epSOS operates and given the highly sensitive nature of the data processed it is necessary to take specific technical and organizational measures to prevent the destruction, accidental loss, alteration, dissemination of and/or unauthorized access to the personal data. In addition such measures should prevent any further unlawful processing of the data (see Article 17 of Directive 95/46/EC).

These measures should take account of the highly sensitive nature of the data to be processed, the central role of ICT within the framework of the project, and the cross-border dimension of the data transfers through the epSOS project. As a result, it is appropriate to implement a high level of personal data protection that should be adequate to the risks arising from the epSOS system.

This protection needs to be effective throughout the processing. To achieve this, common minimum standards should be adopted and all involved should follow them.

As a result appropriate measures and arrangements are required to ensure the following among the epSOS partners:

- (a) Confidentiality - information is protected against unauthorized access or unintended disclosure – only authorized users have access to the information and other system resources,
- (b) Integrity - information is protected against unauthorized modification;
- c) Traceability- each communication and each data transaction can be tracked back to a certain originator in a way that can easily be audited.

Especially, the following measures and arrangements are necessary in order to take full account of security principles and the specific risks related to the processing of personal data in the epSOS system:

- Firstly, all staff implementing the project should be provided with clear-cut, written instructions on how to appropriately use the epSOS system in order to prevent security risks and breaches. Such instructions should take account of the roles/functions of individual staff members (medical staff, pharmaceutical staff, staff at the point of care – POC). The separate functions and competences applying to the each category should be made clear in order to determine their responsibilities in terms of data processing.
- Secondly, suitable arrangements should be made in using the Patient Summary and e-prescription storage and archiving systems to protect the data against unauthorized access, theft and/or partial/total loss of storage media and portable/fixed processing systems – Encryption technologies should¹⁸ be applied.
- Similarly, for data exchanges, secure communication protocols and end-to-end-encryption must be adopted based on encryption standards for securing electronic communications. This has to be done in order to prevent acquisition/disclosure of the information in the presence of any intermediaries not controlled by the patient or the authorized healthcare organizations. Endpoints of the encryption must be located within environments either controlled by the patient directly or by the professional healthcare organizations authorized by the patient for processing his/her medical data. Where communications of health data take place by way of applications that rely on publicly available networks (e.g. the Internet) for data exchanges, the system should envisage the use of reliable digital certificates for both the server systems delivering the service and the client devices accessing the data. An unbroken chain of digital evidence must be preserved to safeguard the integrity and authenticity of the health data in an end-to-end manner.

¹⁸ Encryption of sensitive personal data is compulsory in several Member States.

- Special attention must be paid to adopting a reliable and effective electronic identification system that provides strong authentication. This applies equally to both participating staff members and patients.

Additionally, procedures should be put in place to regularly verify the authentication credentials and the authorization profiles allocated to the staff. The data controller should devise specific procedures to prevent online access and consultation by data subjects where there are possible data confidentiality threats – whether detected directly by the data controller or reported by the data subjects (e.g. in case of theft/loss of authentication credentials, unauthorized access to the system and other data breaches, etc.).

- Appropriateness of the security level also depends on the system's capability to correctly record and track in an auditable way the individual operations that makeup the overall data processing ; this applies, in particular, to data access requests and any handling of the data. The system should also include regular internal checks and controls on authenticity of authorizations. Accordingly, appropriate internal and external controls should be used in the way of audit log systems to verify database accesses, whilst there should be specific alerts where risky and/or non-standard behavior is identified. To ensure that this all works the system should be audited on a regular basis.
- Unauthorized data access and/or changes should be prevented when the back-up data are transferred and/or stored (e.g. by means of encryption).It should be ensured that all epSOS operators must be subject to professional secrecy or similar rules of practice – as is the case in respect of health care practitioners.
- Specifically with regards to the e-Prescription system, the requirements mentioned above should go hand in hand with the deployment of additional measures to ensure that pharmaceutical operators can only access digital prescriptions for providing the medicines prescribed and they should prevent any kind of epSOS related prescription database from being set up at the pharmacy.
- In emergency situations, if it proves necessary to access any information without the required authorizations, that and any subsequent access (including any data processing operations) should be logged and subject to audit; records should also be kept concerning the reasons for the particular data access.

7. Conclusions and recommendations

- All data contained in medical documentation, in electronic health records and in EHR systems are “sensitive personal data” and therefore subject to Article 8 of the Directive.
- The processing of healthcare data must have a clear legal basis. In the absence of other legitimate grounds, this can be the data subject's two- step explicit consent (first for participation in general and then in the case of the concrete treatment/dispensation). The epSOS project could investigate the possibility of allowing patients to give also their first consent in country B, for instance in a secure way over the Internet.

- Processing of personal and sensitive data can be justified without second consent in country B if it is necessary to protect the vital interests of a data subject or of another person if in the emergency case the data subject is physically or legally incapable of giving his consent.
- One of the basic preconditions for a valid consent is that the information given to the data subject satisfies the requirements of Articles 10 and 11 of the Directive.
- The processing of personal data must be strictly limited to the minimum which is necessary for the fulfilment of the epSOS purposes which must be specified, explicit and legitimate.
- In order to safeguard that data are not kept longer than is necessary in the epSOS system, a maximum retention period should be decided as well as a common procedure as to what shall happen to the data at the end of the retention period.
- Each query about the personal data available through epSOS should be for a real need of access to specific information related to the care or treatment to be provided or the medicine to be prescribed or dispensed in a particular case.
- Because of the cross-border character of the epSOS processing, co-operation between DPAs in supervising epSOS is strongly recommended.
- All data controllers handling epSOS data must notify the competent supervisory authority in accordance with the national legislation, regardless of whether the data subjects are nationals or residents of another Member State and irrespective of whether the data handled originate from data controllers in other Member States.
- A high level of IT-security is necessary for epSOS. Especially the following measures and arrangements are necessary in order to take full account of security principles which follow from the Directive and the specific risks related to the processing of personal data in the epSOS system:
 - All staff implementing the project should be provided with clear-cut, written instructions on how to appropriately use the epSOS system in order to prevent security risks and breaches.
 - Suitable arrangements should be made in using the Patient Summary and e-prescription storage and archiving systems to protect the data against unauthorized access, theft and/or partial/total loss of storage media.
 - For data exchanges, secure communication protocols and end-to-end-encryption must be adopted based on encryption standards for securing electronic communications.
 - Special attention must be paid to adopting a reliable and effective electronic identification system that provides strong authentication (of both participating staff and patients).
 - The system must be capable to correctly record and track in an auditable way the individual operations that make-up the overall data processing.
 - Unauthorized data access and/or changes should be prevented when the back-up data are transferred and/or stored (e.g. by means of encryption).
 - With regards to the e-prescription system, additional measures should be deployed in order to ensure that pharmaceutical operators can only access digital prescriptions for providing the medicines prescribed.
 - In emergency situations, any access should be logged and subject to audit.
- All data controllers who handle epSOS data must provide data subjects with the right of access to and rectification/erasure/blocking of their own data.
- A data subject should be able to address questions about access and demands for rectification/erasure/blocking to any of the controllers as well as to any other body

involved in the exchange of information within epSOS. A demand to access or for the rectification/erasure/blocking of data which is given to an epSOS partner who does not handle data about the data subject, should be forwarded to the data controller in charge within the epSOS system even if this relevant controller is established in another Member State.

- epSOS should investigate the possibility of granting the data subject direct (electronic) reading access to his/her own data.
- A common epSOS website should be constructed to inform on the specific rights of data subjects according to the different legislations of all the participating states. The information on the website should clearly specify the rights, conditions and practicalities according to the national legislation of each Member State.

Done at Brussels, on 25 January 2012

*For the Working Party
The Chairman
Jacob KOHNSTAMM*