# Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare

(2009/C 128/03)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to 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,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 sent to the EDPS on 2 July 2008,

HAS ADOPTED THE FOLLOWING OPINION:

## I. INTRODUCTION

*The proposal for a directive on the application of patients' rights in cross-border healthcare*

1. On 2 July 2008, the Commission adopted a proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare (hereinafter the proposal) [1]. The proposal was sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation (EC) No 45/2001.

2. The proposal aims at establishing a Community framework for the provision of cross-border healthcare within the EU, for those occasions where the care patients seek is provided in another Member State than in their home country. This is structured around three main areas:

   — the establishment of common principles in all EU health systems, defining clearly the Member States' responsibilities;

   — the development of a specific framework for cross-border healthcare, providing clarity on the patients' entitlements to have healthcare in another Member State;

   — the promotion of EU cooperation in healthcare, in areas like recognition of prescriptions issued in other countries, European reference networks, health technology assessment, data collection, quality and safety.

3. The objectives of this framework are twofold: to provide sufficient clarity about rights to be reimbursed for healthcare provided in other Member States, and ensure that the necessary requirements for high-quality, safe and efficient healthcare are ensured for cross-border care.

4. The implementation of a cross-border healthcare scheme requires the exchange of the relevant personal data relating to health (hereinafter health data) of the patients between the authorised organisations and healthcare professionals of the different Member States. These data are deemed as sensitive and fall under the stricter rules of data protection as laid down in Article 8 of Directive 95/46/EC on special categories of data.

*EDPS consultation*

5. The EDPS welcomes the fact that he is consulted on this issue and that reference to this consultation is made in the preamble of the proposal, in accordance with Article 28 of Regulation (EC) No 45/2001.

6. It is the first time that the EDPS has formally been consulted on a proposal for a Directive in the field of healthcare. In this Opinion, therefore, some of the remarks made are of a broader scope, addressing general issues of personal data protection in the healthcare sector, which could also be applicable for other relevant legal instruments (binding or not).

[1] COM(2008) 414 final. Please note that a complementary Communication on a Community framework on the application of patients' rights in cross-border healthcare (COM(2008) 415 final) was also adopted on the same date. However, since the Communication is only of rather general nature, the EDPS has chosen to focus on the proposed Directive.

7. Already at the outset, the EDPS would like to express his support to the initiatives of improving the conditions for cross-border healthcare. This proposal should in fact be seen in the context of the overall EC programme for improving the citizens' health in the information society. Other initiatives in this respect are the Commission's envisaged Directive and communication on human organs donation and transplantation ([1]), the recommendation on the interoperability of electronic health records ([2]), as well as the envisaged communication on telemedicine. ([3]) The EDPS is concerned, however, by the fact that all these related initiatives are not closely linked and/or interconnected in the area of privacy and data security, thus hampering the adoption of a uniform data protection approach in healthcare, especially with regard to the use of new ICT technologies. As an example, in the current proposal, although telemedicine is explicitly mentioned in recital 10 of the proposed directive, no reference to the relevant EC Communication's data protection dimension is made. Moreover, although electronic health records are a possible way of cross-border communication of health data, no link to the privacy issues addressed in the relevant Commission's recommendation is provided ([4]). This gives the impression that an overall healthcare privacy perspective is still not clearly defined and, in some cases, completely missing.

8. This is also evident in the current proposal, where the EDPS regrets to see that the data protection implications are not addressed in concrete terms. References to data protection can of course be found, but these are mainly of a general nature and do not adequately reflect the specific privacy-related needs and requirements of cross-border healthcare.

9. The EDPS wishes to emphasise that a uniform and sound data protection approach throughout the proposed healthcare instruments will not only ensure the citizens' fundamental right to protection of their data, but will also contribute to the further development of cross-border healthcare in the EU.

## II. **DATA PROTECTION IN CROSS-BORDER HEALTHCARE**

*General context*

10. The most prominent aim of the European Community has been to establish an internal market, an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured. Enabling citizens to move to and reside more easily in other Member States than where they originate from obviously led to issues relating to healthcare. For that reason, back in the 1990s, the Court of Justice was confronted within the context of the internal market with questions on the possible reimbursement of medical expenses incurred in another Member State. The Court of Justice recognised that the freedom to provide services, as laid down in Article 49 of the EC Treaty, includes the freedom for persons to move to another Member State in order to receive medical treatment ([5]). As a consequence, patients who wanted to receive cross-border healthcare could no longer be treated differently from nationals in their country of origin who received the same medical treatment without crossing the border.

11. These Court judgments are at the heart of the current proposal. Since the Court's case law is based on individual cases, the current proposal intends to improve clarity to ensure a more general and effective application of the freedoms to receive and provide health services. But, as already mentioned, the proposal is also part of a more ambitious programme with the purpose of improving the citizens' health in the information society, where the EU sees great possibilities for enhancing cross-border healthcare through the use of information technology.

12. For obvious reasons, setting rules for cross-border healthcare is a delicate issue. It touches upon a sensitive area in which Member States have established diverging national systems, for instance with regard to the insurance and reimbursement of costs or the organisation of the healthcare infrastructure, including healthcare information networks and applications. Although the Community legislator in the current proposal only concentrates on *cross-border* healthcare, the rules will at least influence the way in which national healthcare systems are organised.

13. Improving the conditions for cross-border healthcare will be to the benefit of the citizens. However, it will at the same time embody certain risks for the citizens as well. Many practical problems which are inherent to cross-border cooperation between people from different countries speaking different languages have to be solved. Since a good health is of the utmost importance for every citizen, any risk of miscommunication and subsequent inaccuracy should be excluded. It goes without saying that enhancing cross-border healthcare in combination

([1]) Announced in the Commission's work programme.
([2]) Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282), OJ L 190, 18.7.2008, p. 37.
([3]) Announced in the Commission's work programme.
([4]) Illustrative in this respect is the fact that no reference to privacy or data protection is included in the Communication mentioned in footnote 1, which is intended to set out a Community framework on the application of patients' rights in cross-border healthcare.
([5]) See Case 158/96, *Kohll*, [1998] ECR I-1931, para 34. See amongst others also Case C-147/99, *Smits and Peerbooms* [2001] ECR I-5473 and Case C-385/99, *Müller-Fauré and Van Riet* [2003] ECR I-12403.

with the use of information technological developments, has great implications for the protection of personal data. A more efficient and therefore increasing exchange of health data, the increasing distance between persons and instances concerned, the different national laws implementing the data protection rules, lead to questions on data security and legal certainty.

*Protection of health data*

14. It must be emphasised that health data is considered a special category of data which deserves higher protection. As the European Court of Human Rights in the context of Article 8 of the European Convention of Human Rights recently stated: 'The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention' ([1]). Before explaining the stricter rules for processing of health data which are laid down in Directive 95/46/EC, a few words will be devoted to the notion of 'health data'.

15. Directive 95/46/EC does not include an explicit definition of health data. Commonly, a wide interpretation is applied, often defining health data as 'personal data that have a clear and close link with the description of the health status of a person' ([2]). In this respect, health data normally includes medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs, etc.), as well as administrative and financial data relating to health (e.g. documents concerning hospital admissions, social security number, medical appointments scheduling, invoices for healthcare service provision, etc.). It should be noted that the term 'medical data' ([3]) is also sometimes used to refer to data relating to health, as well as the term 'healthcare data' ([4]). Throughout this Opinion the notion 'health data' will be used.

16. A useful definition of 'health data' is provided for by ISO 27799: 'any information which relates to the physical or mental health of an individual, or to the provision of health service to the individual, and which may include: (a) information about the registration of the individual for the provision of health services; (b) information about payments or eligibility for healthcare with respect to the individual; (c) a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; (d) any information about the individual collected in the course of the provision of health services to the individual; (e) information derived from the testing or examination of a body part or bodily substance; and (f) identification of a person (healthcare professional) as provider of healthcare to the individual'.

17. The EDPS is very much in favour of adopting a specific definition for the term 'health data' in the context of the current proposal, which could also be used in the future within other relevant EC legal texts (see Section III below).

18. Article 8 of Directive 95/46/EC sets out the rules on the processing of special categories of data. These rules are stricter than those for processing of other data as laid down in Article 7 of Directive 95/46/EC. This already shows where Article 8(1) explicitly states that the Member State *shall prohibit* the processing of, inter alia, data concerning health. In the subsequent paragraphs of the Article several exceptions to this prohibition are formulated, but these are narrower than the grounds for processing of normal data as set out in Article 7. For example, the prohibition does not apply if the data subject has given his or her *explicit* consent (Article 8(2)(a)), contrary to required *unambiguous* consent in Article 7 sub (a) of Directive 95/46/EC. Moreover, Member State law can determine that in certain cases even consent of the data subject cannot lift the prohibition. The third paragraph of Article 8 is solely dedicated to processing of data concerning health. According to this paragraph the prohibition of the first paragraph does not apply if the processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare 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.

19. Article 8 of Directive 95/46/EC lays much emphasis on the fact that the Member States should provide for suitable or adequate safeguards. Article 8(4) for instance allows Member States to lay down additional exceptions to the prohibition to process sensitive data for reasons of substantial public interest, but subject to the provision of suitable safeguards. This in general terms underlines the responsibility of Member States to attach special care to the processing of sensitive data, such as data concerning health.

*Protection of health data in cross-border situations*

Shared responsibilities between Member States

20. The Member States should be especially aware of the responsibility just mentioned once the issue of cross-border exchange of health data is at stake. As set out above, the cross-border exchange of health data increases the risk of inaccurate or illegitimate data processing.

([1]) See ECtHR 17 July 2008, *I v Finland* (appl. No 20511/03), para 38.
([2]) See Article 29 Working Party, working document on the processing of personal data relating to health in electronic health records (EHR), February 2007, WP 131, paragraph II.2. See also on the wide meaning of 'personal data': Article 29 Working Party, Opinion 4/2007 on the concept of personal data, WP 136.
([3]) Council of Europe, Recommendation No R(97)5 on the protection of medical data.
([4]) ISO 27799:2008 'Health informatics — Information security management in health using ISO/IEC 27002'.

Obviously this can have huge negative consequences for the data subject. Both the Member State of affiliation (where the patient is an insured person) and the Member State of treatment (where cross-border healthcare is actually provided) are involved in this process and therefore share this responsibility.

21. Security of health data is, in this context, an important issue. In the recent case cited above the European Court of Human Rights attached particular weight to the confidentiality of health data: 'Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general' ([1]).

22. The data protection rules, as laid down in Directive 95/46/EC, furthermore require that the Member State of affiliation should provide the patient with adequate, correct and up to date information about the transfer of his or her personal data to another Member State, together with ensuring the secure transfer of the data to this Member State. The Member State of treatment should also ensure secure receipt of this data and provide the appropriate level of protection when data is indeed processed, following its national data protection law.

23. The EDPS would like to make the Member States' shared responsibilities clear within the proposal, taking also into account the electronic data communication, especially in the context of new ICT applications, as this is discussed below.

Electronic health data communication

24. Improving cross-border exchange of health data is mainly established through the use of information technology. Although the exchange of data in a cross-border healthcare scheme may still be performed on paper (e.g. the patient moves to another Member State bringing all his/her relevant health data with him/her, like laboratory examinations, doctor referrals, etc.), it is clearly intended to use electronic means instead. Electronic communication of health data will be supported by healthcare information systems established (or to be established) in the Member States (in hospitals, clinics, etc.), as well as the use of new technologies, like the electronic healthcare record applications (operating possibly over the Internet), as well as other tools like patients and doctor health cards. Of course it is also possible that combined paper-based and electronic exchange forms are used, depending on the Member States healthcare systems.

25. E-health and telemedicine applications, which fall within the scope of the proposed Directive, will depend exclusively on the exchange of electronic health data (e.g. vital signs, images, etc.), usually in conjunction with other existing electronic healthcare information systems residing on the Member States of treatment and affiliation. This includes systems operating both at patient-to-doctor basis (e.g. remote monitoring and diagnosis), as well as at doctor-to-doctor basis (e.g. teleconsultation between healthcare professionals for expert advice on specific healthcare cases). Other more specific healthcare applications supporting the overall cross-border healthcare provision might also depend solely on electronic data exchange, e.g. electronic prescription (e-Prescription) or electronic referral (eReferral), which is already implemented at national level in some Member States ([2]).

*Areas of concern in cross-border health data exchange*

26. Taking into account the above mentioned considerations, together with the existing diversity of the Member States' health systems, as well as the growing development of e-health applications, the following two main areas of concern arise with regard to the protection of personal data in cross-border healthcare: (a) the different security levels which may be applied by the Member States for the protection of personal data (in terms of technical and organisational measures), and (b) privacy integration in e-health applications, especially in new developments. In addition, other aspects like secondary use of health data, especially in the area of statistics production, might also need special attention. These issues are further analysed in the remainder of this section.

Data security in the Member States

27. Despite the fact that Directives 95/46/EC and 2002/58/EC are uniformly applied in Europe, the interpretation and implementation of certain elements may differ between countries, especially in areas where the legal provisions are general and left up to the Member States. In this sense, main area of consideration is the security of the processing, i.e. the measures (technical and organisational) that the Member States take to safeguard the security of health data.

([1]) ECtHR 17 July 2008, *I v Finland* (appl. No 20511/03), para 38.

([2]) eHealth ERA Report, Towards the Establishment of a European eHealth Research Area, European Commission, Information Society and Media, March 2007, (http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf).

28. Although the strict protection of health data is a responsibility of all Member States, there is currently no commonly accepted definition of an 'appropriate' security level for healthcare within EU which could be applied in the case of cross-border healthcare. So, for example, a hospital in one Member State may be obliged by nationally imposed data protection regulations to adopt specific security measures (e.g. the definition of security policy and codes of conduct, specific rules for outsourcing and use of external contractors, auditing requirements, etc.) whereas in other Member States this might not be the case. This inconsistency may have impact on the cross-border data exchange, especially when in electronic form, since it cannot be guaranteed that data are secured (from a technical and organisational point of view) at the same level between different Member States.

29. There is, therefore, a need for further harmonisation in this field, in terms of defining a common set of security requirements for healthcare that should be commonly adopted by Member States' healthcare service providers. This need is definitely in line with the overall need for definition of common principles in the EU health systems, as set out in the proposal.

30. This should be done in a generic way, without imposing specific technical solutions to the Member States, but still setting a basis for mutual recognition and acceptance, e.g. in the fields of security policy definition, identification and authentication of patients and healthcare professionals, etc. Existing European and international standards (e.g. ISO and CEN) on healthcare and security, as well as well-accepted and legally based technical concepts (e.g. electronic signatures [1]) could be used as a road map in such an attempt.

31. The EDPS supports the idea of healthcare security harmonisation at EU level and is of the opinion that the Commission should undertake relevant initiatives, already in the framework of the current proposal (see Section III below).

Privacy in e-health applications

32. Privacy and security should be part of the design and implementation of any healthcare system, especially e-health applications as mentioned in this proposal (privacy-by-design). This undisputable requirement has already been supported in other relevant policy documents [2], both general, as well as healthcare specific [3].

33. In the framework of the e-health interoperability discussed within the proposal, the notion of 'privacy-by-design' should once more be stressed as a basis for all envisaged developments. This notion applies at several different layers: organisational, semantic, technical.

— At the organisational level, privacy should be considered in the definition of the necessary procedures for health data exchange between the Member States' healthcare organisations. This may have direct impact on the type of exchange and extend to which data are transferred (e.g. use of identification numbers instead of the patients' real names where this is possible).

— At the semantic level, privacy and security requirements should be incorporated within new standards and schemes, e.g. in the definition of the electronic prescription template as this is discussed within the proposal. This could build on existing technical standards in this field, e.g. standards on data confidentiality and digital signature, and address healthcare specific needs like role based authentication of qualified healthcare professionals.

— At the technical level, system architectures and user applications should adapt privacy enhancing technologies, implementing the aforementioned semantic definition.

34. The EDPS feels that the field of electronic prescriptions could serve as a start for the integration of privacy and security requirements at the very initial stage of development (see Section III below).

Other aspects

35. An additional aspect which could be considered in the framework of cross-border health data exchange is the secondary use of health data and in particular the use of data for statistical purposes, as already set out in the current proposal.

36. As mentioned earlier in point 18, Article 8(4) of Directive 95/46 foresees the possibility of secondary use of health data. However, this further processing should be done only for reasons of 'substantial public interest' and must be subject to 'suitable safeguards' laid down by national law or upon decision of the supervisory authority [4]. Moreover, in case of statistical data processing, as also mentioned in the EDPS opinion on the proposed regulation on

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13 , 19.1.2000, p. 12-20.

[2] The EDPS and EU Research and Technological Development, Policy Paper, EDPS, April 2008, (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf).

[3] Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282), OJ L 190, 18.7.2008, p. 37.

[4] See also recital 34 of Directive 95/46. See on this point also the WP 29 Opinion on EHR mentioned above in footnote 8, at p. 16.

Community statistics on public health and health and safety at work [1], an additional risk arises from the different meaning the notions 'confidentiality' and 'data protection' might have in the application of data protection legislation on the one hand and legislation on statistics on the other hand.

37. The EDPS wishes to underline the above elements in the context of the current proposal. More explicit references to the data protection requirements regarding the subsequent use of health data should be included (see Section III below).

## III. DETAILED ANALYSIS OF THE PROPOSAL

*The proposal's provisions on data protection*

38. The proposal includes a number of references to data protection and privacy in different parts of the document, more specifically:

— recital 3 states — among other things — that the Directive has to be implemented and applied with due respect for the rights to private life and protection of personal data;

— recital 11 refers to the fundamental right to privacy with respect to the processing of personal data, and confidentiality as two of the operating principles that are shared by health systems throughout the Community;

— recital 17 describes the right to the protection of personal data as fundamental right of the individuals that should be safeguarded, focusing especially on the individuals' right of access to health data — also in the context of cross-border healthcare — as this is established in Directive 95/46/EC;

— Article 3, which sets the relationship of the Directive with other Community provisions, refers in paragraph 1a to the Directives 95/46/EC and 2002/58/EC;

— Article 5 on the responsibilities of the Member State of treatment, sets in paragraph 1f the protection of the right to privacy as one of these responsibilities, in conformity with national measures implementing Directives 95/46/EC and 2002/58/EC;

— Article 6 on healthcare provided in another Member State, stresses in paragraph 5 the right of access for patients to their medical records when travelling to another Member State with the purpose of receiving healthcare there or seeking to receive healthcare provided in another Member State, again in conformity with national measures implementing Directives 95/46/EC and 2002/58/EC;

— Article 12 on the national contact point for cross-border healthcare, states in paragraph 2(a) that these contact points should be responsible — among other things — to provide and disseminate information to patients on the guarantees on the protection of personal data provided in another Member State;

— Article 16 on e-health, states that measures for achieving interoperability of information and communication technology systems should respect the fundamental right to the protection of personal data in accordance with the applicable law;

— lastly, in Article 18(1) it is mentioned — among other things — that the collection of data for statistical and monitoring purposes should be done in accordance with national and Community law on the protection of personal data.

39. The EDPS welcomes that data protection has been taken into account in the drafting of the proposal and that an attempt is made to show the overall need for privacy in the context of cross-border healthcare. However, the existing provisions of the proposal on data protection are either too general or refer to Member States' responsibilities in a rather selective and scattered way:

— in particular, recitals 3 and 11, together with Articles 3(1)(a), 16 and 18(1) are in fact addressing the general data protection legal framework (the last two in the context of e-health and statistics collection, but without setting specific privacy related requirements);

— as far as Member States' responsibilities are concerned, a general reference is made in Article 5(1)(f);

— recital 17 and Article 6(5) provide a more specific reference to the patients'right of access in the Member State of treatment;

— lastly, Article 12(2)(a) has a provision on the patients' right to information in the Member State of affiliation (through the operation of the national contact points).

In addition, as already mentioned in the Introduction of this Opinion, there is no link and/or reference to privacy aspects addressed in other EC legal instruments (binding or not binding) in the area of healthcare, especially with regard to the use of new ICT applications (like telemedicine or electronic health records).

[1] OJ C 295, 7.12.2007, p. 1.

40. In this way, although privacy is generally stated as a requirement of cross-border healthcare, the overall picture is still missing, both in terms of the Member States' obligations, as well as in terms of the particularities introduced through the cross-border nature of healthcare service provision (in contrast with national healthcare service provision). More specifically:

— Member States responsibilities are not presented in an integrated way, since some obligations (rights of access and information) are stressed — still in different parts of the proposal — whereas others are completely omitted, like security of processing;

— no reference is made to the concerns about Member States' inconsistencies on security measures and the need for health data security harmonisation at a European level, in the context of cross — border healthcare;

— no reference to privacy integration in e-health applications is made; this is also not adequately reflected in the e-Prescription case.

41. In addition, Article 18, which deals with data collection for statistical and monitoring purposes, raises some specific concerns. The first paragraph refers to 'statistical and *other additional data*'; it furthermore refers in plural to 'monitoring purposes' and subsequently lists the areas which are subject to these monitoring purposes, namely the provision of cross-border healthcare, the care provided, its providers and patients, the costs and outcomes. In this context, already quite unclear, a general reference to the data protection law is made, but no specific requirements relating to subsequent use of data concerning health as laid down in Article 8(4) of Directive 95/46/EC are set. Moreover, the second paragraph contains the unconditional obligation to transfer the large amount of data to the Commission at least on an annual basis. Since no explicit reference is made to an assessment of the necessity of this transfer, it seems that the Community legislator itself has already established the necessity of these transfers to the Commission.

*The EDPS recommendations*

42. In order to adequately address the aforementioned elements, the EDPS provides a number of recommendations, in terms of five basic steps for amendments, as described below.

Step 1 — Definition of health data

43. Article 4 defines the basic terms used within the proposal. The EDPS strongly recommends introducing in this article a definition of health data. A broad interpretation of health data should be applied, like the one described in Section II of this Opinion (points 14 and 15).

Step 2 — Introduction of a specific article on data protection

44. The EDPs also strongly recommends the introduction of a specific article on data protection within the proposal, which could set the overall privacy dimension in a clear and understandable way. This article should (a) describe the responsibilities of the Member States of affiliation and treatment, including — among other — the need for security of processing, and (b) identify the main areas for further development, i.e. security harmonisation and privacy integration in e-health. For these matters specific provisions can be made (within the proposed article), as presented in Steps 3 and 4 below.

Step 3 — Specific provision for security harmonisation

45. Following the amendment of Step 2, the EDPS recommends that the Commission adopts a mechanism for the definition of a commonly acceptable security level of the healthcare data at national level, taking into account existing technical standards in this field. This should be reflected in the proposal. A possible implementation could be through the use of comitology procedure, as this is already described in Article 19 and applies for other parts of the proposal. Moreover, additional instruments could be used for the production of relevant guidelines, including all concerned stakeholders, like the Article 29 Working Party and the EDPS.

Step 4 — Privacy integration in the e-Prescription template

46. Article 14 on the recognition of prescriptions issued in another Member State provides for the development of a Community prescription template, supporting interoperability of e-Prescriptions. This measure shall be adopted through a Comitology procedure, as this is defined in Article 19(2) of the proposal.

47. The EDPS recommends that the proposed e-Prescription template incorporates privacy and security, even at the very basic semantic definition of this template. This should be explicitly mentioned in Article 14(2)(a). Again the involvement of all relevant stakeholders is of major importance. In this respect, the EDPS wishes to be informed about and involved in further actions taken on this issue through the proposed Comitology procedure.

Step 5 — Subsequent use of health data for statistical and monitoring purposes

48. In order to prevent misunderstandings, the EDPS encourages clarifying the notion 'other additional data' in article 18(1). The Article should furthermore be amended in the sense that it refers more explicitly to the requirements for subsequent use of health data as laid down in Article 8(4) of Directive 95/46/EC. Moreover, the obligation to transmit all the data to the Commission, contained in the second paragraph, should be made subject to an assessment of the necessity of such transfers for legitimate purposes which are duly specified in advance.

## IV. **CONCLUSIONS**

49. The EDPS would like to express support to the initiatives of improving the conditions for cross-border healthcare. He expresses concerns, however, about the fact that EC healthcare related initiatives are not always well co-ordinated with regard to ICT use, privacy and security, thus hampering the adoption of a universal data protection approach towards healthcare.

50. The EDPS welcomes that reference to privacy is made within the current proposal. However, a number of amendments are needed, as explained in Section III of this Opinion, in order to provide clear requirements, both for the Member States of treatment and affiliation, as well to properly address the data protection dimension of cross-border healthcare.

— A definition of health data should be included in Article 4, covering any personal data that can have a clear and close link with the description of the health status of a person. This should in principle include medical data, as well as administrative and financial data relating to health.

— The introduction of a specific article on data protection is strongly recommended. This article should set clearly the overall picture, describing the responsibilities of the Member States of affiliation and treatment and identifying the main areas for further development, i.e. security harmonisation and privacy integration, especially in e-health applications.

— It is recommended that the Commission adopts a mechanism in the framework of this proposal for the definition of a commonly acceptable security level of the healthcare data at national level, taking into account existing technical standards in this field. Additional and/or complementary initiatives, including all concerned stakeholders, the Article 29 Working Party and the EDPS, should also be encouraged.

— It is recommended that the notion of 'privacy-by-design' is incorporated in the proposed Community template for e-Prescription (also at semantic level). This should be explicitly mentioned in Article 14(2)(a). The EDPS wishes to be informed about and involved in further actions taken on this issue through the proposed comitology procedure.

— It is recommended to specify the language of Article 18 and to include a more explicit reference to the specific requirements relating to subsequent use of data concerning health as laid down in Article 8(4) of Directive 95/46/EC.

Done in Brussels, 2 December 2008.

Peter HUSTINX

*European Data Protection Supervisor*