Alþingi
Erindi nr. Þ 135/289
komudagur 21.11.2007

Persónuvernd

Rauðarárstíg 10 105 Reykjavík
sími: 510 9600 bréfasími: 510 9606
netfang: postur@personuvernd.is
veffang: personuvernd.is

Nefndasvið Alþingis
Austurstræti 8-10
150 Reykjavík

Reykjavík, 16. nóvember 2007
Tilvísun: 2007110803 SMG/--

Efni: Umsögn um tillögu til þingsályktunar um eflingu rafrænnar sjúkraskrár

Persónuvernd vísar til bréfs heilbrigðisnefndar Alþingis, dags. 13. nóvember sl., þar sem óskað er umsagnar stofnunarinnar um tillögu til þingsályktunar um eflingu rafrænnar sjúkraskrár (þskj. 29, 29. mál, 135. löggjafarþing).

Tillagan hljóðar svo:

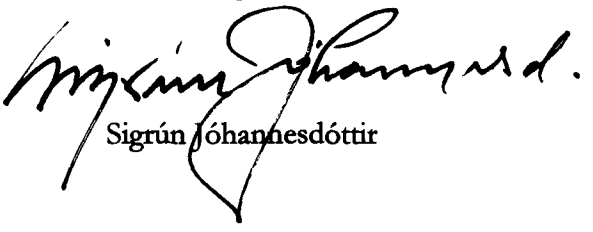
> „Alþingi ályktar að fela heilbrigðisráðherra að sjá til þess að á kjörtímabilinu verði lokið við innleiðingu rafrænnar sjúkraskrár fyrir alla heilbrigðisþjónustu, jafnt á sjúkrastofnunum sem á heilsugæslustöðvum og hjá sjálfstætt starfandi heilbrigðisstarfsmönnum."

Ef átt er við rafræna sjúkraskrá á landsvísu telur Persónuvernd það vera forsendu fyrir starfrækslu slíkrar skráar að kveðið sé skýrlega á um hana í lögum. Þá er afar brýnt að tryggja öryggi persónuupplýsinga í slíkri landsskrá með fullnægjandi hætti.

Til upplýsingar má geta þess að hinn 6. nóvember sl. fór Persónuvernd á fund nefndar sem heilbrigðisráðherra hefur skipað til að endurskoða ákvæði laga og reglugerða um sjúkraskrár, einkum með tilliti til rafrænna sjúkraskráa. Á fundinum kynnti Persónuvernd vinnuskjal sem starfshópur á vegum Evrópusambandsins hefur tekið saman um rafrænar sjúkraskrár á landsvísu. Starfshópur þessi sinnir ráðgjafarhlutverki um persónuverndarmálefni í Evrópusambandinu og hefur m.a. það hlutverk að stuðla að samræmingu í framkvæmd persónuverndarlöggjafar í Evrópu. Hann er skipaður fulltrúum persónuverndarstofnana í aðildarríkjum Evrópusambandsins, fulltrúum Evrópsku persónuverndarstofnunarinnar og fulltrúum framkvæmdastjórnar Evrópusambandsins. Persónuvernd situr fundi hópsins sem áheyrnarfulltrúi.

Til upplýsingar fylgir vinnuskjalið hjálagt, en í því eru tilgreind atriði sem starfshópurinn telur forsendur fyrir rekstri rafrænnar sjúkraskrár á landsvísu.

Virðingarfyllst



Sigrún Jóhannesdóttir

Hjál. Vinnuskjal 29. gr. starfshópsins um rafrænar sjúkraskrár á landsvísu

ARTICLE 29 Data Protection Working Party

00323/07/EN
WP 131

Working Document on the processing of personal data relating to health in electronic health records (EHR)

Adopted on 15 February 2007

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 (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43.

Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

EXECUTIVE SUMMARY

In this Working Document on **the processing of personal data relating to health in electronic health records (EHR),** the Article 29 Working Party provides guidance on the interpretation of the applicable data protection legal framework for EHR systems and explains some of the general principles. The Working Document also gives indications on the data protection requirements for setting up EHR systems, as well as the applicable safeguards.

The Article 29 Working Party first examines the **general legal data protection framework** for EHR systems. The Article 29 Working Party recalls the general prohibition of the processing of personal data concerning health of Article 8 (1) of the Data Protection Directive 95/46/EC, and then discusses the possible application of the derogations in Article 8 (2), (3) and (4) of the Directive in the context of EHR systems by stressing the need for interpreting such derogations in a narrow fashion.

The Article 29 Working Party also reflects on a **suitable legal framework for EHR systems** and provides **recommendations on eleven topics** where special safeguards within EHR systems seem particularly necessary in order to guarantee the data protection rights of patients and individuals. These topics are:

1. Respecting self determination
2. Identification and authentication of patients and health care professionals
3. Authorization for accessing EHR in order to read and write in EHR
4. Use of EHR for other purposes
5. Organisational structure of an EHR system
6. Categories of data stored in EHR and modes of their presentation
7. International transfer of medical records
8. Data security
9. Transparency
10. Liability issues
11. Control mechanisms for processing data in EHR

The Article 29 Working Party invites the medical profession, all health care professionals, all involved persons and institutions as well as the general public to comment on this Working Document.

TABLE OF CONTENTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

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[1], and in particular Articles 29 and 30 paragraph 1 (b) thereof,

Having regard to the Rules of Procedure of the Working Party[2], and in particular Article 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING WORKING DOCUMENT:

I. Introduction

The objective of this Working Document of the Article 29 Working Party is to provide guidance on the interpretation of the applicable data protection legal framework for electronic health record (EHR) systems and to establish some general principles. The opinion also aims at setting out the data protection preconditions for establishing a nation-wide EHR system, as well as the applicable safeguards.

The costs of public health care schemes are dramatically increasing and governments are calling for new strategies to address this issue. One of the answers often put forward is the "electronic health record (EHR)". Terms used in this field include "electronic medical record (EMR)", "electronic patient record (EPR)", "electronic health record (EHR)", "computer-based patient record (CPR)" etc. These terms can be used interchangeably.

For the purposes of this Working Document, an "electronic health record (hereinafter: EHR)" shall be defined as

> *"A comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form and providing for ready availability of these data for medical treatment and other closely related purposes[3]."*

Traditionally, documentation on medical treatment episodes was available with different health care professionals but would not be combined in a single record. In contrast, the concept of "EHR" aims at compiling existing documentation on medical treatments relating to an individual from different sources and from different periods of time. It would thereby furnish information on the past and present state of health of an individual as completely as possible, and for a considerable period of time, perhaps even a lifetime (*"from the cradle to the grave"*). Once compiled, the EHR data would be available in electronic form to all

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281, 23.11.1995, p. 31 (hereafter: "the Directive"); available at: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

2 Adopted by the Working Party at its third meeting held on 11.9.1996.

3 "Medical treatment and closely related purposes" refers to the purposes mentioned in Article 8 (3) of the Directive.

authorized health care professionals and other authorized institutions wherever and whenever this information is needed.

EHR is claimed to be an appropriate means to

- bring about better quality of treatment because of better information about the patient;
- improve the cost efficiency of medical treatments and thus prevent further rapid growth of health care budget deficits;
- furnish the necessary data for quality control, statistics and planning in the public health care sector which should also have a positive effect on public health care budgets.

Answers to a questionnaire circulated in 2005 amongst European data protection supervisory authorities showed that nationwide EHR schemes are relevant and urgent topics in most of the Member States. The degree of implementation of such projects differs widely, however: whilst most Member States are discussing EHR, others have already implemented EHR systems at least in part.

Due to the fact that health care is increasingly provided also across borders, the European Commission has underlined, in its Communication "*e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area*"[4], the importance of e-Health services and of the interoperability of electronic health records. Furthermore the European Community is financing relevant projects, for example on electronic patient records or on patient identifiers (e.g. the European Health Insurance Card). When implementing such programmes the European Commission is under an obligation, together with the Member States, to ensure compliance with all relevant legal provisions regarding personal data protection and, where appropriate, the introduction of mechanisms to ensure the confidentiality and safety of such data[5].

EHR systems have the potential to achieve greater quality and security in medical information than the traditional forms of medical documentation. However, from a data protection point of view the fact has to be stressed that EHR systems additionally have the potential not only to process more personal data (e.g. in new contexts, or through aggregation) but also to make a patient's data more readily available to a wider circle of recipients than before.

It should also be noted that electronic health information in an EHR system – apart from being accessible to health care professionals – might generally attract the interest of third parties such as insurance companies and law enforcement agencies. From the point of view of the protection of personal data, in compiling existing medical information about an individual from different sources with the result of allowing for easier and more widespread access to this sensitive information, EHR systems introduce a new risk scenario, changing the whole scale of possible misuse of medical information about individuals. Whereas this new risk scenario will be fully realized by most projects only in a future state of full-scale implementation, it is nevertheless necessary to be aware of these dangers now, when most existing models contain only a limited or partial application (e.g. only to a basic set of medical data or to hospitals of a certain region), since it is only a matter of time before they become generally applicable.

---

4 COM (2004) 356 final.

5 See, e.g. Article 5 (5) of Decision 1786/2002/EC.

II. The data protection framework for electronic health records

Any processing of personal data in EHR systems has to fully comply with the rules for the protection of personal data. The Working Party would like to stress that the framework applying to the use of EHR is set out in Recital 2 of the Directive which says that *"data processing systems are designed to serve man; (...) they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, in particular the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals"*.

The fundamental right to the protection of personal data is essentially based on Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and on Article 8 of the EU Charter of Fundamental Rights[6]. More precise rules are in particular laid down in the EC Data Protection Directive 95/46/EC and in Directive 2002/58/EC on privacy and electronic communications[7], and in the national laws of the Member States implementing these Directives.

Any processing of personal data in EHR must also comply with the rules laid down in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) and the Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181).

In the context of EHR, the Working Party would like to draw specific attention to the Council of Europe Recommendation No. R(97) 5 on the protection of medical data (13 February 1997). Reference is also made to the recommendations made in the "Working Document on Online Availability of Electronic Health Records" by the International Working Group on Data Protection in Telecommunications[8].

1. General principles

Data controllers collecting data in the context of EHR applications must therefore comply with all general data protection principles, including the following:

- Use limitation principle (purpose principle): This principle partially embodied in Article 6(1)(b) of the Directive, among others, prohibits further processing which is incompatible with the purpose(s) of the collection.
- The data quality principle: This principle in the Directive requires personal data to be relevant and not excessive for the purposes for which they are collected. Thus, any irrelevant data must not be collected and if it has been collected it must be discarded (Article 6(1)(c)). It also requires data to be accurate and kept up-to date.
- The retention principle: This principle requires personal data to be kept for no longer than is necessary for the purpose for which the data were collected or further processed.

---

[6] The right to protection of personal data is not absolute, and can be restricted if specific public interests do so require. However, these objectives in the public interest can only justify an interference with the protection of personal data, if it is in accordance with the law, is necessary in a democratic society for the pursuit of the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others, and is not disproportionate to the objective pursued (Article 8 (2) ECHR).

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37–47).

[8] Adopted at its 39th meeting in Washington D.C., 6-7 April 2006 (http://www.berlin-privacy-group.org).

- Information requirements: Pursuant to Article 10 of the Directive data controllers processing information in EHR systems must provide certain information to data subjects, such as information on the identity of the controller, on the purposes of the processing, on the recipients of the data and on the existence of a right of access.
- Data subject's right of access: Article 12 of the Directive provides data subjects with the ability to check on the accuracy of the data and to ensure that the data are kept up to date. These rights fully apply to the collection of personal data in EHR systems.
- Security related obligations: Article 17 of the Directive imposes an obligation upon data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or unauthorised disclosure. The measures can be organisational or technical.

2. Special protection for sensitive personal data

However, when the processing of such personal data relates to a person's health, processing is particularly sensitive and therefore requires special protection.

> The definition of personal data contained in Article 2 (a) of Directive 95/46/EC reads as follows:
>
> *"Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".*
>
> The definition of special categories of data contained in Article 8 (1) of the Directive reads as follows:
>
> *"Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."*

Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of the Directive[9]. This definition also applies to personal data when they have a clear and close link with the description of the health status of a person: data on consumption of medicinal products, alcohol or drugs as well as genetic data are doubtlessly "personal data on health" especially if they are included in a medical file. Also any other data – e.g. administrative data (social security number, date of admission to hospital etc) – contained in the medical documentation of the treatment of a patient will have to be considered as being sensitive: if they were not relevant in the context of the treatment of the patient, they would and should not have been included in a medical file.

As a consequence, the members of the Working Party are of the opinion that 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 in addition subject to the special data protection rules on the processing of sensitive information contained in Article 8 of the Directive.

---

[9] European Court of Justice, Judgment of 6 November 2003, Case C-101/01 - Bodil Lindqvist.

3. A general prohibition of the processing of personal data concerning health – with derogations

Article 8 (1) of the Data Protection Directive 95/46/EC prohibits the processing of personal data concerning health in general. So does Article 6 of the Council of Europe Convention No 108.

This special protection contained in Article 8 (1) complements the other provisions of the Directive, in particular Article 6 on the principles relating to data quality and Article 7 on the criteria for making data processing legitimate.

However, considering the importance of using information about a patient in order to medically treat him appropriately, there are exemptions to the general prohibition of processing medical data.

The Data Protection 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, exhaustive** and have to be **construed in a narrow fashion.**

4. Article 8 (2) (a): "Explicit consent"

According to Article 8 (2) (a) of the Directive:

> *"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;"*

a) Therefore a justification for the processing of sensitive data can be the **consent** of the data subject[10]. As already indicated in the Working Party's previous working documents WP 12[11] and WP 114[12], an important point is that in order to be valid, consent – whatever the circumstances are in which it is expressed – must be a "*freely given, specific and informed indication of the data subject's wishes*", as defined in Article 2(h) of the Directive.

aa) Consent must be given freely: '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 Article 29 Working Party takes the view that where as a necessary and unavoidable consequence of the medical situation a health professional has to process personal data in an EHR system it is misleading if he seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where

---

[10] Agreeing to undergo a certain medical treatment does not automatically furnish "consent" in the sense of Article 2 (h) to the processing (especially disclosure or transfer) of personal data collected during such treatment.

[11] Article 29 Working Party "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" (WP 12, 24 July 1998).

[12] Article 29 Working Party "Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995" (WP 114, 25 November 2005).

the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment.[13]

bb) Consent must be specific: 'Specific' consent must relate to a well-defined, concrete situation in which the processing of medical data is envisaged. Therefore 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.

cc) Consent must be informed: '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.

b) 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.

c) The Article 29 Working Party has observed that it is sometimes complicated to obtain consent due to practical problems, in particular where there is no direct contact between the data controller and the data subjects. Whatever the difficulties, the **data controller** must be able to prove in all cases that, firstly, he has obtained the explicit consent of each data subject and, secondly, that this explicit consent was given on the basis of sufficiently precise information.

d) 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.

5. Article 8 (2) (c): "vital interests of the data subject"

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. Accordingly, this exception could be applied only to a small number of cases of treatment and could not be used at all to justify processing personal medical data for purposes other than treatment of the data

[13] See also Article 29 Working Party "Opinion 8/2001 on the processing of personal data in the employment context" (WP 84, Section 10).

subject such as, for example, to carry out general medical research that will not yield results until some time in the future.[14]

> By way of example: assume a data subject has lost consciousness after an accident and cannot give his consent to the necessary disclosure of known allergies. In the context of EHR systems this provision would allow access to information stored in the EHR to a health professional in order to retrieve details on known allergies of the data subject as they might prove decisive for the chosen course of treatment.

6. Article 8 (3): "processing of (medical) data by health professionals"

Article 8 (3) allows for the processing of sensitive personal data under three cumulative conditions: the processing of sensitive personal data must be *"required", and this processing takes place "for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services"* and the personal data in question *"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"*.

a) 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 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).

b) Furthermore the processing of personal data on grounds of Article 8 (3) must be "**required**" for the specific purposes mentioned under a). The Working Party stresses that this means in an EHR context that any inclusion of personal data in an EHR would have to be fully justified; the mere "usefulness" of having such personal data contained in an EHR would not be sufficient.

c) The third condition under Article 8 (3) is that the processing of sensitive personal data is performed by medical or other staff subject to **professional (medical) secrecy or an equivalent obligation to secrecy.**

> The medical profession's ethical requirement of confidentiality was first set out in the "Hippocratic Oath"[15] and subsequently affirmed by the World Medical Association's Declaration of Geneva (1948). It protects the information collected by a health care professional in the course of the treatment of a patient. Use of this information is allowed only within the limits of the treatment contract. This relationship of confidentiality excludes all third parties, even other health care professionals, unless the patient has agreed to passing on his data or it is foreseen especially by law.

---

[14] For an interpretation of the similar provision contained in Article 26 (1)(e) with regard to data transfers outside the EU, see Article 29 Working Party "Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995", WP 114, (25 November 2005).

[15] *"All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."* (Source: http://en.wikipedia.org/wiki/Hippocratic_Oath).

The Working Party points out that the special obligation of professional secrecy must be either established in the national law of the Member States, or by national competent professional bodies with the power to adopt binding rules on the profession. These national rules on professional secrecy must also provide for corresponding effective sanctions in case of breach.

According to the Directive, should the necessity arise for non-medical staff to process these sensitive personal data, they also must be made subject to binding rules which ensure at least an equivalent level of confidentiality and protection. In particular, these rules must contain an obligation that the data will be used only for the purposes mentioned under Article 8 (3).

Health professionals with direct responsibility for the treatment of patients are generally under legal obligations to keep documentation on their medical treatment (actions, prescriptions, etc.) in patients' records. In accordance with numerous existing legal provisions on the obligation to professional secrecy of health care professionals, keeping and using patients' records is traditionally limited to the direct bilateral relationship between a patient and the health care professional/health care institution consulted by the patient.

d) As Article 8 (3) of the Directive is an exemption from the general prohibition to process sensitive data, this exemption must be interpreted in a restrictive way.

e) If the question were raised whether Article 8 (3) of the Directive could serve as the *sole* legal basis for the processing of personal data in an EHR system, the Article 29 Working Party is of the opinion that Article 8 (3) could only pertain to the processing of medical data for strictly those medical and health-care purposes mentioned therein, and strictly under the conditions that processing is "required" and done by a health professional or by another person subject to an obligation of professional or equivalent secrecy. Where the processing of personal data in an EHR goes in any way beyond these purposes or does not meet the said conditions, then Article 8 (3) cannot serve as the sole legal basis for the processing of that personal data.

However, even if all these prerequisites were fulfilled, the Article 29 Working Party must point out that EHR systems create a new risk scenario, which calls for new, additional safeguards as counterbalance: EHR systems provide direct access to a compilation of the existing documentation about the medical treatment of a specific person, from different sources (e.g. hospitals, health care professionals) and throughout a lifetime. Such EHR systems therefore transgress the traditional boundaries of the individual patient's direct relationship with a healthcare professional or institution: The keeping of medical information in an EHR extends beyond the traditional methods of keeping and using medical documentation on patients. On the technical side, multiple access points over an open network like the internet increases possible patient data interception. Maintaining the legal standard of confidentiality suitable within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online. Fully developed EHR systems thus tend to open up and facilitate access to medical information and sensitive personal data. EHR systems pose significant challenges in ensuring that only appropriate health professionals gain access to information for legitimate purposes related to the care of the data subject. They make the processing of sensitive personal data more complex with direct implications for the rights of the individuals. As a consequence an EHR system must be considered as a new risk scenario for the protection of sensitive personal data.

The main and traditional safeguard in Art. 8 (3) – apart from the purpose limitation and the strict necessity requirement - is the obligation of medical professionals to confidentiality concerning medical data about their patients. This may no longer be fully applicable in an EHR environment, as one of the purposes of EHR is to grant access to medical documentation

for the sake of treatment to such professionals who have not been party to the previous treatment documented in a medical file.

Therefore, the Article 29 Working Party is not convinced that, even if Article 8 (3) is used as a justification for processing, relying only on the obligation to professional secrecy provides sufficient protection in an EHR environment. A new risk scenario calls for additional and possibly new safeguards beyond those required by Article 8 (3) in order to provide for adequate protection of personal data in an EHR context.

7. Article 8 (4): substantial public interest exemptions

A number of provisions of the Directive contain a substantial degree of flexibility, so as to strike the appropriate balance between the protection of the data subject's rights on the one side, and on the other side the legitimate interests of data controllers, third parties and the public interest which may exist.

Article 8 (4) of the Directive allows the Member States to derogate further from the prohibition of processing sensitive categories of data:

> *"Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."*
>
> Recital 34 reads:
>
> *(34) "Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify 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 - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;"*

a) As a consequence, should a Member State intend to make use of this possibility, the exemption must be contained in a legal provision or a decision of the supervisory authority (**special legal basis**).

b) Such processing of sensitive personal data must be justified by reasons of **substantial public interest**. Recital 34 of the Directive gives examples of areas which are particularly apt to harbour cases of 'substantial public interest'. These include the fields of public health and social security, to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

The substantial public interest must be presented by the Member State for each case in the entire scope of the processing exempted, and the processing must be necessary in the light of that substantial public interest. Any such measure must be proportionate i.e. there must not be other less infringing measures available.

Furthermore, for any interference with the right to private and family life, in order to be legitimate it must be in line with Article 8 of the European Convention on Human Rights and must be read in the light of the Strasbourg jurisprudence: it needs to be done "*in accordance with the law*" and be "*necessary in a democratic society*" for a public interest purpose. The Strasbourg jurisprudence has repeatedly stated that the law providing for the interference "*must indicate the scope of any such discretion conferred on the competent authorities and*

the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference".

c) Member States are under the obligation to provide **specific and suitable safeguards** so as to protect the fundamental rights and the privacy of individuals in that context.

d) Any use of Article 8 (4) by a Member State has to be **notified to the Commission** in line with Article 8 (6) of the Directive.

In the context of EHR, the Article 29 Working Party notes that the arguments for introducing EHR systems (cf. I., above) may establish "substantial public interest". In some Member States a 'right to health protection' is enshrined in the constitution. This underlines the importance attributed to all appropriate means for bringing about "health protection". An EHR system in such legal environments would certainly be founded on "substantive public interest" as it is an instrument fundamentally intended to guarantee adequate medical assistance to patients.

Article 8(4) of the Directive could, therefore, serve as a legal basis for EHR systems, provided that all the conditions mentioned therein are fulfilled. In particular, suitable safeguards for the protection of personal data in an EHR system must be provided for.

The Working Party wishes to discuss such possible safeguards and the suitable legal framework for EHR systems in the following section.

III. Reflections on a suitable legal framework for EHR systems

The Article 29 Working Party gives details below on those topics where special safeguards[16] within EHR systems seem particularly necessary in order to guarantee the data protection rights of patients. Considering the impact of EHR systems and the special need for transparency of such systems the safeguards should preferably be laid down in a special comprehensive legal framework.

1. Respecting self determination

Even if an EHR system is not entirely founded on consent as a legal basis (Article 8 (2)), the patient's self determination concerning when and how his data are used should have a significant role as a major safeguard.[17]

a) The functionality of "agreeing" in the context of suitable safeguards is different from "consent" under Article 8 (2) of the Directive and therefore needs not meet with all requirements of Article 8 (2): e.g. whereas **consent as a legal basis** for processing health data would always have to be "explicit" according to Article 8 (2), **agreement as a safeguard** need not necessarily be given in form of an opt-in – the possibility to express self

[16] The general requirements foreseen in Directive 95/46/EC for lawful processing of personal data are not repeated in this part of the paper, as they apply anyway. This paper only elaborates on specific additional requirements for processing medical data in EHR systems, which seem necessary to counterbalance the special privacy risk scenario caused by EHR systems.

[17] In some jurisdictions there is not only a fundamental right to data protection but also a constitutional right to optimal health protection: as a consequence out of this obligation for providing optimal treatment, some Member States have provided health professionals with mandatory access to the data available via the EHR system. This seems acceptable as long as the necessary balance is achieved by means of stressing other safeguards, such as detailed regulations on the circumstances of lawful access and on – severe – consequences in case of misuse of access rights etc.

determination could – depending on the situation – also be offered in form of an opt-out/ a right to refuse.

b) In view of the varying damage potential of different types of health information, categories of use cases should be discerned with **different degrees of the possibility to exercise self determination**:

In the legal provisions introducing an EHR system, it should be laid down as a rule that entering data into an EHR or accessing such data should be governed by an incremental system of "opt-in" requirements (especially when processing data, which are potentially extra harmful such as psychiatric data, data about abortion, etc.[18]) and "opt-out" possibilities for less intrusive data.[19] This could guarantee the necessary amount of protection on the one hand and the necessary practicability and flexibility on the other hand.

c) It should in principle always be **possible for a patient to prevent disclosure** of his medical data, documented by one health professional during treatment, to other health professionals, if he so chooses.

Consideration should also be given to the question how suppression of access to information in an EHR should be handled: Whether the suppression should be masked in order to be undetectable or whether, maybe in certain cases, a message should be given that additional information is existent but available only under specific requirements.

d) Under the assumption that nobody could be forced to take part in an EHR system, in the legal provisions establishing an EHR system the question of **possible complete withdrawal from an EHR system** ought to be addressed. Rules must be foreseen whether this triggers an obligation to completely delete or merely prevent further access to the data in the EHR system; choice could also be given to data subjects.

2. Identification and authentication of patients and health care professionals

a) Reliable identification[20] of patients in EHR systems is of crucial importance. If health data were used which relate to the wrong person as a result of incorrect identification of a patient the consequences would in many cases be detrimental.

Health cards on smart card basis could contribute significantly to a proper electronic identification of patients and also to their **authentication[21] if they want to access their own EHR data.**

b) Moreover, the special sensitivity of health data requires that no access is possible for unauthorized persons. Reliable access control depends on reliable identification[22] and

---

18 Special features like "sealed envelopes" could be used, which cannot be opened without the cooperation of the data subject.

19 Opt-out solutions would, however, need adequate information for the patient in order to function effectively as a "suitable safeguard".

20 "Identification" means that a person is described by identifiers like name, date of birth, address etc.; in the given context this description will have to be officially certified by a birth certificate, a passport or a health card etc.

21 "Authentication means proof of the fact that a person, claiming a certain identity, really is this person. This is usually achieved by showing an official identity document containing a photo (e.g. a passport), or – in the electronic world – by using an electronic signature.

22 "Reliable identification" should not make use of identification numbers, which are widely used in other contexts, without specific safeguards, in order to avoid easy interconnectibility (see Article 8(7) of the Directive).

authentication. This makes it necessary to **uniquely identify and also properly authenticate users.** [23]

As one of the main advantages of EHR systems is their availability for access by electronic communication irrespective of time and location, routines for reliable electronic identification and authentication will have to be established. Authentication by means of electronic signatures – provided to authorized users together with proper official identification e.g. on special smart cards – should be envisaged at least in a longer term perspective in order to avoid the known risks of password authentication.

For health care professionals it will be necessary to develop an identification and authentication system, which proves not only identities but additionally also the **role in which a health care professional acts electronically**, e.g. as a psychiatrist or as a nurse.

3. Authorization for accessing EHR in order to read and write in EHR

a) General access safeguards:

Data in EHR systems are confidential medical records. Thus the **essential principle** concerning access to an EHR must be that – apart from the patient himself – **only** those **healthcare professionals**/ authorized personnel of healthcare institutions **who presently are involved in** the patient's **treatment may have access**. There must be a relationship of actual and current treatment between the patient and the healthcare professional wanting access to his EHR record.

It seems also necessary to regulate which categories of health care professionals/institutions at which level have access to EHR-data (practising physicians, hospital doctors, pharmacists, nurses, chiropractitioners?, psychologists?, family therapists? etc.).

Data protection could additionally be enhanced by **modular access rights**, that is by forming categories of medical data in an EHR system with the consequence that access is limited to specific categories of health care professionals/institutions[24]. The possible advantages of a modular EHR set-up will be dealt with more extensively under point 6.

b) Special access safeguards by involvement of the patient:

If feasible and if possible – that is with a patient present and able to act – the **patient should be given the chance to prevent access to his EHR data if he so chooses**. This requires prior information about who would when and why want access to his data and about the possible consequences of not allowing access. Procedures must be developed which avoid undue psychological pressure on the patient to consent to requests for accessing his data.

Where **proof of a patient's agreement** to accessing his EHR data is necessary, reliable instruments for such proof are indispensable, such as electronic checking of a patients' token or – if such instruments are already generally available – the patient's electronic signature etc. Presentation of such proof must be electronically documented for possible auditing.

Rules should be developed concerning the question whether the data subject should be able to demand that certain data are not entered into his file. A possible way to deal with this topic could also be "sealed envelopes" which cannot be opened without explicit consent of the data subject.

---

[23] In France the first experiments which are about to start on EHR are based on the creation of a specific identifier; it is not certain yet whether this system will be maintained in the final set up of the EHR.

[24] For instance, access to data about psychiatric treatment could be limited on a first level to psychiatrists; or a special medication module could be made accessible also for pharmacists, who do not have access to the other parts of an EHR system.

c) Access for the data subjects to their own EHR data:

Whether **direct (electronic) reading access** to their EHR should be granted to patients is a matter of medical feasibility. 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 into an EHR 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.

The question of whether **patients** should **enter data into their EHR** themselves or whether they should have them entered by a health professional also ought to be addressed in the provisions on an EHR system. Adequate transparency concerning the logging routines revealing the author of entries into an EHR record would most likely take care of possible problems of liability for accuracy. It could also be considered to limit writing access to a special module within an EHR record.

In this context, the abilities and the special needs of the chronically ill, the elderly, as well as the handicapped and disabled must be taken into account.

4. Use of EHR for other purposes

The acceptance of EHR systems by the citizens will depend on their **trust in the confidentiality of the system.**

The reason for legitimate access to data in an EHR should correspond to the main purpose of any EHR system, i.e. successful medical treatment by better information. **The Working Party is of the opinion that accessing medical data in an EHR for purposes other than those mentioned in Article 8 (3) should in principle be prohibited.**

This would for instance exclude access to EHR by medical practitioners who act as experts for third parties: e.g. for private insurance companies, in litigations, for granting retirement aid, for employers of the data subject etc. Additionally, disciplinary law applicable to the health care professionals should be designed to counteract infringements of these rules effectively.

Special measures should be taken to prevent that patients are illegally induced to disclose their EHR data, e.g. upon request of a possible future employer or a private insurance company. Education of the patient is essential to prevent that they comply with such requests of disclosure which would be illegal under data protection law. Technical means might also have to be applied e.g. special requirements for full print-outs from an EHR etc.

Processing of EHR-data for the purposes of **medical scientific research and government statistics** could be allowed as an exception to the rule set out above, provided that all these exceptions are in line with the Directive (cf. Article 8 (4) and the corresponding Recital 34): they must therefore be foreseen by law for previously determined, specific purposes under special conditions to guarantee proportionality ("specific and suitable safeguards") so as to protect the fundamental rights and the privacy of individuals.

Moreover, whenever feasible and possible, data from EHR systems should be used for other purposes (e.g. statistics or quality evaluation) only in anonymised form or at least with secure pseudonymisation[25].

[25] Pseudonymisation means transposing identifiers (like names and date of birth etc) into a new designation, preferably by encryption, so that the recipient of the information cannot identify the data subject.

5. Organisational structure of an EHR system

In the context of discussing different organisational alternatives for storing data in an EHR system the following main alternatives are usually mentioned:

- EHR as a system furnishing access to medical records kept by the health care professional, who has the obligation to keep records on the treatment of his patients – this is often called **"decentralised storage"**, or
- EHR as a uniform system of storage, to which medical professionals have to transfer their documentation; this is often called **"centralised storage";**
- a third alternative could be to enable the data subject to be "master" of his own medical records by offering him **storage of patients' medical data as a special *e*-service under the patient's control**, possibly even including the power to decide what goes into an EHR.[26]

a) Whereas the third alternative **(storage under the control of the data subject)** appears to be the best solution in terms of self determination, the quality of such documentation concerning accuracy and completeness might pose problems, if it is only the data subject who decides which data are kept in his EHR and no medical professional corrective is built into the system.

b) In case of a **"decentralised" storage** model, which only becomes a "system" by the creation of corresponding search paths, the existing structure of documentation of health data at the different health care providers would remain unchanged. The extent to which a patient's data can be located in this system depends on the quality of the search system.

In this organisational model the **health care professional/institution remains "controller"** of the file (more precisely: of that part of the EHR record which was created by him). Considering the complex system architecture of this model it could be necessary to appoint one central body to be responsible for steering and monitoring the whole system and also for ensuring the data protection compatibility of the operation of the system. It might also be useful, if data subjects could take their data protection problems to a central body instead of having to search among a multitude of controllers.

c) The main advantage of a so called **"centralised" storage** system would presumably be higher technical security and availability (24-hour access), which is not so easily guaranteed if an EHR system goes beyond hospitals. There will be a single controller for the whole system separate from the healthcare professionals/institutions who forwarded their documentation (in parts or as a whole) to the central system.

In terms of data protection, objections could be raised against a system of that kind regarding the higher potential of misuse of centralised data storage. Special arrangements and security measures (e.g. encrypted storage) could be foreseen in order to balance the security risks of centrally held data, at least to a considerable degree. However, liability for the confidentiality of the system is taken out of the hands of medical professionals which might influence the amount of trust invested by the patients into such a system.

The extent to which the patient can influence the content and disclosure of his EHR record would in both cases – decentralised storage as well as centralised storage – depend on the special system design (see item 3 b).

---

[26] This is the French model that is currently being put in place. Those service providers are called hosts ("hébergeurs") and their position is regulated by a Decree that was subject to the prior opinion of CNIL. It is complex and focuses on issues of accreditation of those service providers and the security of the system.

6. Categories of data stored in EHR and modes of their presentation

The idea of an "EHR system" is basically to collect about one specific person all health related data which are presumably relevant for his long-term state of health, so that in case of future treatment comprehensive, relevant information is available and patients have a better chance of successful treatment.

The Working Party considers that this might give raise to the following main problems:

a) "Completeness" of a health file is practically impossible and also not desirable: **Only *relevant* information should be entered into an EHR.** One of the most difficult questions when establishing an EHR system will be therefore to decide which categories of medical data should be collected in an EHR and stored for which period of time[27]. Whereas this question has foremost to be answered by medical experts, it also has a data protection dimension: According to the principles of relevance and proportionality of data collection, every compilation of data must be limited to those data which are relevant and not excessive for the defined purpose of the processing (Article 6(1)(c) of the Directive). The legitimacy of EHR systems will therefore also depend on an adequate solution of choosing the 'right' categories of data and the 'right' length of time for storing information in an EHR.

b) Concerning the presentation of data within the EHR: The fact that it is possible to discern different categories of health data which require quite different degrees of confidentiality suggests that it might be generally useful to create different **data modules** within an EHR system with different access requirements: A "vaccination data module" should be accessible at any time for the data subject and could also be accessible for a rather broad range of personnel within the health-care services; a "medication data module" could be supplied with special access to pharmacists if the patient agrees[28]; an "emergency data module" could have special technical means for access, etc. Setting up modules for special "recall systems" also would appear to make sense; they would serve to remind a patient automatically of necessary vaccination, health check-ups and post-treatment examinations.

Particularly sensitive data could also be better protected by storage in separate modules with especially strict conditions for access. Examples would be data on psychiatric treatment or on HIV or abortion. Instead of excluding such data from an EHR – which might be detrimental for future successful medical treatment – special restrictions for access to such EHR-data should be built into the system including explicit consent of the patient and special technical barriers (as e.g. "sealed envelopes").

c) When structuring EHR records, recurrent **special information demands** should also be taken into consideration. One example: Under national law, private insurance companies might be entitled to receive some (limited) information concerning health records, when necessary in the context of fulfilling their contractual obligations towards insured patients. Granting access to private insurance companies to the EHR of a patient seems unacceptable. For that reason a solution could be to establish a standardized special "documentation package" which, when necessary, meets the legitimate information interests of the insurer and, if authorized by the patient, could be (electronically) transmitted to the private insurance company.

---

[27] There are categories of data which are important throughout the whole life of a patient (e.g. allergies) but also data which are extremely important only for a short time, as e.g. incompatibilities of treatments.

[28] The advantage of having such a medication module within the EHR would be twofold, because it would also give the treating physician the opportunity to see the entire medication the patient is on.

7. International transfer of medical records

Electronic availability of medical data in EHR systems can considerably enhance diagnostic or treatment facilities by making use of medical expertise available only in foreign medical institutions. Additional consultation of foreign experts for diagnostic purposes usually does not require revealing the identity of the patient. Therefore, if possible, such data should be transferred to countries outside the European Union/European Economic Area only **in anonymised or at least pseudonymised form**. If there is no explicit consent of the data subject for the transfer of personal data[29], this would also avoid the necessity of obtaining permission for this data transfer, as the data subject is not identifiable to the recipient.

Considering the elevated risk to the personal data in an EHR system in an environment without adequate protection, the Article 29 Working Party wants to underline that any processing – especially the storage – of EHR data should take place within jurisdictions applying the EU Data Protection Directive or an adequate data protection legal framework.

A specific problem are transborder data flows in the course of clinical studies: the study group dealing directly with the patients might sometimes need access to EHR data in their original personalised form. For all transfer of data resulting from clinical studies to sponsors or other lawfully involved institutions, secure pseudonymisation must, however, be required as a minimum prerequisite, especially if such sponsors are established in countries without adequate data protection.

Special attention should in this context always be given to data security aspects, in order to avoid risks of unauthorized disclosure in environments which are possibly not safe from a data protection point of view.

8. Data security

The acceptability of a system of data processing with an exceptional risk potential is dependent on an adequately high level of data security for the complete performance of the system. **Access by unauthorised persons must be virtually impossible and prevented**, if the system is to be acceptable from a data protection point of view. However, availability of the system for authorized professionals must be virtually unlimited where there is a genuine need to know, if the system is to result in the promised advantages for the medical treatment of patients.

The legal framework for setting up an EHR system would have to foresee the requirement of implementing a series of measures of a technical and organisational nature appropriate for avoiding loss or unauthorized alteration, processing and access of data in the EHR system. Integrity of the system must be guaranteed by making use of the knowledge and instruments representing the present state of the art in computer science and information technology.

Privacy enhancing technologies (PETs)[30] should be applied as much as anyway possible in order to promote personal data protection. Encryption should not only be used for transfer but also for storage of data in EHR systems. All security measures should be construed in a user friendly way to broaden their application. The necessary costs should be seen as an investment into the fundamental rights compatibility of EHR systems, which will be one of the most important prerequisites if EHR systems are to become a success.

---

[29] In situations where a patient is physically unable to respond to a request for consent (e.g. because of coma) his medical data could nevertheless, in accordance with Article 26 (1)(e) of the Directive, be transferred to countries without adequate data protection if his vital interests so demand. .

[30] On PETs, see point 4.3 of the Commission's "First report on the implementation of the Data Protection Directive (95/46/EC)", COM (2003) 265 final.

Regardless of the fact that many of the safeguards discussed above already contain elements of data security, the legal framework concerning security measures should especially foresee the necessity of

- the development of a reliable and effective system of electronic identification and authentication as well as constantly up-dated registers for checking on the accurate authorization of persons having or requesting access to the EHR system;
- comprehensive logging and documentation of all processing steps which have taken place within the system, especially access requests for reading or for writing, combined with regular internal checks and follow up on correct authorization;
- effective back up and recovery mechanisms in order to secure the content of the system;
- preventing unauthorized access to or alteration of EHR data at the time of transfer or of back up storage, e.g. by using cryptographic algorithms;
- clear and documented instructions to all authorized personnel on how to properly use EHR systems and how to avoid security risks and breaches;
- a clear distinction of functions and competences concerning the categories of persons in charge of the system or at least involved in the system with a view to liability for shortcomings;
- regular internal and external data protection auditing.

9. Transparency

It seems evident, that an EHR has high potential for medical treatment but in principle also for misuse by unauthorized access. Public opinion and the individuals will therefore call for extra **transparency concerning the content and the functioning of an EHR system** in order to be able to trust in the system. **Notification** to Data Protection supervisory authorities combined with special **information, which is easily available and understandable** must be procured by the controller(s) of the system. The use of the Internet as the ideal information distributor may help to create the necessary transparency about the EHR system(s) nationally established.

Free of charge, easy to use but safe access points for data subjects to check on the content and on disclosure of their EHR record might also be a valuable contribution to transparency and thereby trust in the system.

10. Liability issues

Any EHR system must also guarantee that the **possible infringements of privacy** which are caused by storing and furnishing medical data in an EHR system are adequately **balanced by liability for damages** caused e.g. by incorrect or unauthorized use of EHR data.

In an analysis of possible problems of EHR systems from a data protection point of view, questions of liability for incorrect use of an EHR system can only be touched upon. In the opinion of the Working Party, any Member State wishing to introduce an EHR system should in advance carefully conduct in-depth, expert civil and medical law studies and impact assessments to clarify the new liability issues likely to arise in this context, e.g. regarding the accuracy and completeness of data entered in EHR, defining how extensively a health care professional treating a patient must study an EHR, or about the consequences under liability law if access is not available for technical reasons, etc.

11. Control mechanisms for processing data in EHR

Considering the **special risk scenario** created by the establishment of EHR systems **effective control mechanisms** for evaluating the existing safeguards are necessary. The complexity of the information contained in an EHR together with the multitude of possible users may call for new procedures concerning the access rights of data subjects:

a) A **special arbitration procedure** should be set up **for disputes** about the correct use of data in EHR systems; the data subjects should be able to make use of such a procedure easily and free of charge. Considering the fact that usually special medical expertise will be necessary to evaluate claims for false or unnecessarily processed information in EHR systems, the Data Protection Supervisory Authorities might not be the best choice for dealing with such claims, at least not in the first instance. Public "Patients' Advocates" could, where they exist already, be put in charge of this task.

b) An EHR system must ensure that the data subject is able to exercise his access rights without undue difficulties. In principle it is the data controller who is obliged to give access. **EHR systems are**, however, **information pool systems** with many different data controllers. In such systems with a large number of participating data controllers, **a single special institution must be made responsible towards the data subjects for the proper handling of access requests.** In view of the foreseeable complexity of a fully developed EHR and the necessity of building trust with patients in the system, it seems essential that patients whose data are processed in an EHR system know how to reach a responsible partner with whom they could discuss possible shortcomings of the EHR system. Special regulations to this end will have to be included in any regulation on EHR systems.

c) In order to establish trust, a **special routine for informing the data subject when and who accessed data in his EHR** could be introduced. Furnishing the data subjects in regular intervals with a protocol listing the persons or institutions who accessed their file would reassure patients about their ability to know what is happening to their data in the EHR system.

d) Regular internal and external data protection auditing of access protocols must take place. The already mentioned annual access report sent to the data subjects would be an additional effective means for checking legality of use of EHR data. Data protection officers in hospitals which take part in EHR systems would certainly improve the probability of correct use of data in these systems.

IV. CONCLUSION

All individuals and all patients have a right to privacy and may thus reasonably expect that confidentiality and protection of their personal information will be rigorously upheld by all healthcare professionals. This expectation is also valid as regards electronic health record (EHR) systems.

The Article 29 Working Party has drafted this Working Document in order to provide guidance on the interpretation of the applicable data protection legal framework for electronic health record (EHR) systems and to establish some general principles. The Working Document is also aimed at setting out the data protection preconditions for establishing a nation-wide EHR system, as well as the applicable safeguards, and at contributing to the uniform application of the national measures adopted under Directive 95/46/EC.

The Article 29 Working Party emphasises that establishing and operating EHR systems must be done in full compliance with the principles of protection of personal data, as enshrined in

Directive 95/46/EC. It considers that compliance with these principles helps all persons and institutions involved in ensuring the proper functioning of such systems. Additionally the Article 29 Working Party highlights the need to establish and operate EHR systems within a sound legal framework of safeguards aimed at protecting personal data, irrespective of the legal basis of such systems.

The Article 29 Working Party invites the medical profession, all other health care professionals and persons and institutions involved in providing medical services as well as the general public to comment on this Working Document.[31]

In the light of ongoing development in this field, further work, additional comments and follow-up by the Article 29 Working Party might be necessary.

Done at Brussels, on 15 February 2007

For the Working Party
The Chairman
Peter SCHAAR

[31] Comments to this Working Document should be sent to: Secretariat of the Article 29 Working Party
European Commission, Directorate-General Justice, Freedom and Security
Unit C.5 – Protection of personal data
Office: LX 46 1/43
B - 1049 Brussels
E-mail: Amanda.JOYCE-VENNARD@ec.europa.eu ; Fax: +32-2-299 80 94
All comments from both public and private sectors will be published on the Article 29 Working Party's internet site unless respondents explicitly state that they wish to keep particular information confidential.