Legal Updates & News

Bulletins

Health Data: Article 29 WP Working Document: e-health records

April 2007
by Karin Retzer

Privacy Bulletin, April 2007

At a time when member states are seeking to centralise electronic health record systems, the Article 29 Working Party recently issued a Working Document addressing the key issues to be considered by states when processing electronic health records. Karin Retzer, Of Counsel, at the Brussels office of Morrison & Foerster LLP examines the Document.

The application of European Union data protection law presents particular challenges in the context of electronic health records. At a time when governments, health care professionals and service providers move to centralize and outsource electronic health records systems for cost efficiency and better health treatment due to improved access to patient records, several national data protection authorities have raised concerns regarding the confidentiality and safety of such data.

The recent 'Working Document on the processing of personal data relating to health in electronic health records' ('Working Document') by the Article 29 Data Protection Working Party ('Working Party') seeks to harmonize patients' rights with respect to health records across the EU, and sets forth recommendations on appropriate safeguards.[fn1] Unfortunately, the Working Document calls for Member State legislation, frowning on existing schemes, while leaving it for health care professionals and providers of information technology, electronic records management and other services to navigate through a minefield of complex and conflicting obligations.

The legal framework

Directive 95/46/EC,[fn2] the main legal instrument of EU data protection law, protects health information as 'sensitive data'.[fn3] Generally, sensitive data cannot be processed[fn4] unless the subject of the data (that is the individual) gives explicit (opt-in) consent, or another exemption applies.[fn5] Article 8 of the Directive expressly provides that Member State laws may prohibit the processing of certain sensitive data, irrespective of the individual's consent.

Without obtaining consent, organizations may generally only process data where it is:

- necessary for exercising the organization's obligations or rights related to employment 'in so far as authorized by national law providing for adequate safeguards';[fn6]
- necessary to protect the vital interests of the subject of the data or of another person, provided the data subject is physically or legally incapable of giving consent;
- necessary for the establishment, exercise or defense of legal claims;
- necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to professional secrecy or by another person subject to an equivalent obligation of secrecy; or
- solely related to data that were 'manifestly made public' by the data subject.

Member States have implemented the various exceptions rather differently and inconsistently, a problem recognized by the European Commission Report on the implementation of the Data Protection Directive (95/46/EC).[fn7] The Directive provides further leeway in that it permits Member States' legislators or data

protection authorities to adopt additional exceptions 'for reasons of substantial public interest.'

In addition, the processing of sensitive data generally requires prior approval from national data protection authorities. In Italy, for example, a detailed security policy document is required, and specific technical requirements must be met.[fn8] In Spain, the processing of health-related data triggers a requirement for more rigorous security measures under Royal Decree 994/1999.[fn9]

The Working Paper

Electronic health records, for the purposes of the Working Paper, are defined as any '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.'

Application of the General Data Protection Regime

The Working Party reiterates the data protection requirements applicable to any personal data, in particular the notice requirement under Article 10 of the Directive. In brief, organizations must provide certain information to data subjects, such as information on the identity of the organization controlling the data, on the purposes of the processing, on the recipients of the data, and on the existence of a right of access.

The general prohibition of processing health records

The Working Document reiterates the general prohibition of sensitive data[fn10] under Article 8 of the Directive, as well as Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108.[fn11] Consequently, the Working Party argues that the exemptions provided in Article 8 of the Directive have to be interpreted narrowly, and Member States may not introduce exemptions under national law in addition to what is permitted under Article 8. The Working Party examines the different exemptions that may legitimize the processing of health records. In particular:

Consent

The Working Party stresses that consent must be given freely, that it be through a voluntary decision by an individual in possession of all of his/her 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 would render consent invalid. The Working Party takes the view that where the medical situation requires the health professional to process certain health records, it would be misleading to seek to legitimize the processing through consent. In any event, consent must relate to a well-defined, concrete situation; a 'general agreement' of the individual to the collection of his/her medical records and to subsequent transfers between different health professionals would not constitute specific consent.

Valid interest

The Working Party stresses that this is limited to situations where processing is necessary for a lifesaving treatment in a situation where the individual is not able to express his or her intentions.

Processing by health professionals

Here the Working Party states that this provision only covers processing of health records 'indispensable' for the specific purpose of providing health related services, and does not cover medical research, litigation, or general measures in the area of public health and social protection, such as quality and cost control or reimbursement and the settling of claims under a health insurance scheme. Health professionals must be under secrecy obligations under statutory law or binding professional rules by competent bodies. According to the Working Party it is possible, however, to extend these secrecy rules to non medical staff.

Public interest

Article 8(4) allows Member States to permit processing of sensitive data for reasons of substantial public interest. The Working Party states that the arguments for introducing electronic health records systems - that is, cost efficient and high quality health services - may constitute a 'substantial public interest'. In the Working Party's opinion, Article 8(4) would be the most appropriate basis for centralizing health records held by different

health professionals, provided the Member States introduce suitable safeguards for the protection of such data through either statute, or a decision issued by the data protection authority.

Safeguards for the protection of health records

The Working Document sets forth in great detail the safeguards needed, in the Working Party's view, for processing health records. The purpose of the issuance seems to be twofold: first, Member States, when allowing health records to be shared on public interest grounds, should ensure that these safeguards are present. Second, in order to render existing health records schemes legitimate, and to 'counterbalance the special privacy risk scenario caused by electronic health records systems', these schemes should comply with the safeguards. In particular:

Self-determination

The Working Party stresses that nobody should be forced to have his/her medical records included in an electronic health records system. When setting up such a scheme, an incremental system of 'opt-in' requirements (and, possibly, 'opt-out' for less intrusive data) should be provided. It should, in principle, always be possible for a patient to prevent disclosure of his/her medical data. Requiring patients to opt-in and/or opt-out seems, however, inconsistent with the Working Party's view that requiring consent from a patient may be waived where the processing is indispensable.

Access controls

Reliable access controls to identify and authenticate users, for example through electronic signatures or smart cards, should be envisaged at least in a longer-term perspective in order to avoid the known risks of password authentication. Also, apart from the patient, only those healthcare professionals with a need to know for actual and current treatment should have access. Also, different categories of health care professionals should have different access rights. Presentation of such proof must be electronically documented for possible auditing.

Patient Access Rights

In the Working Party's opinion, providing patients with direct (electronic) access to their electronic health records depends on medical feasibility. Also, while granting direct access may enhance the patient's trust in the system, secure identification and authentication routines would be needed in order to avoid misuse. The access right under Article 12 of the Directive need not necessarily always mean direct access.

Use of electronic health records for other purposes

The Working Party states that the use of health records should be limited to the provision of health related services, and would exclude access by experts appointed by insurance providers, employers in civil litigation, etc., for employers of the individual, etc. Accessing health records for the purposes of medical scientific research and government statistics should only be permitted in exceptional situations, and preference should be given to using data in anonymous form or at least with secure pseudonymisation.

Content of electronic systems

The legitimacy of electronic health records systems will depend on an adequate solution for choosing the 'right' categories of data and the 'right' length of time for storing information in an electronic health record. Also, different data sets may be created with different access requirements. Particularly sensitive data, such as information relating to psychiatric treatment, HIV or abortion, should be protected by storage in separate modules with especially strict conditions for access.

International transfers

While the Working Party recognizes that the electronic availability of health records systems can considerably enhance diagnostic or treatment facilities, it argues that consultation of experts for diagnostic purposes would not usually require revealing the identity of the patient. Therefore, if possible, data should be transferred to countries outside the EU only in anonymous or at least pseudonymised form. Also, in the course of clinical studies, the study group dealing directly with the patients might sometimes need access to electronic health records in their original personalized 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.

Data security

The legal framework for setting up an electronic health records system should provide the requirement of implementing a series of measures of a technical and organizational nature appropriate for avoiding loss or unauthorized alteration, processing and access of data in the electronic health records 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) should be applied as much as possible in order to promote personal data protection. Encryption should not only be used for transfer, but also for storage of data in electronic health records systems.

Conclusion

In summary, the Working Party takes a very conservative view and suggests a narrow interpretation of the Directive's exemptions to process medical records. In the Working Party's view, Member State legislators or data protection authorities should suggest a framework for processing health records and make use of the possibility provided under the Directive to allow processing on public interest grounds. Most useful for practitioners are, perhaps, the detailed additional safeguards suggested that governments, medical practitioners, and service providers have to account for when centralizing and outsourcing the processing of medical records.

Footnotes

1. Working Document on the processing of personal data relating to health in electronic health records (electronic health records) adopted on 15 February 2007, WP131, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.

2. 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 information and on the free movement of such data ('Directive'), published in the Official Journal on 23 November 1995, L 281/31, available at: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett.

3. Article 8 of the Directive defines sensitive data to include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health.

4. 'Processing' is very broadly defined and includes collection, recording, storage, transmission, or use of personal data.

5. Current German law extends this obligation to data processors and requires providers of medical data archiving systems to inform clients that patient data may only be processed with the explicit and informed consent of the individuals.

6. See Article 8(1)2b of the Directive.

7. Section 3.1, COM/2003/0265 final.

8. Legislative Decree 2003/196. Available in English at: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp.

9. https://www.agpd.es/upload/reglamento_ingles_pdf.pdf.

10. The Working Party considers any data with a clear and close link with the description of the health status of a person to be sensitive. Therefore, 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.

11. http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

This article appeared in *Data Protection Law & Policy*, Volume 4 Issue 3, March 2007, and is reprinted with permission.