

Analysis of the Legal Aspects Concerning Data Protection in Electronic Medical Registry

Iacob SANDEA*, Andrei B. ACHIMAȘ CADARIU

“Iuliu Hațieganu” University of Medicine and Pharmacy Cluj-Napoca, 6 Louis Pasteur, 400349 Cluj-Napoca, Cluj, Romania.

E-mail: iacob_sandea@yahoo.co.uk

* Author to whom correspondence should be addressed; Tel.: +4-0744-164875.

Abstract: The European and national legislation establish legal aspects regarding personal data protection in electronic records. The protection of medical personal data can be improved in relation with development of new modalities for medical evidence and electronic health storage, even if laws already establish some aspects. Development and implementations of e-Health approaches revealed the necessity of creation of new adapted and functional laws needed to solve critical health conditions, conditions that are more important than to date than law constrains regarding personal data protection.

Keywords: Legal aspects; Law; Electronic Health Record; Personal Numeric Code; Health Card.

Introduction

Electronic health record (EHR) (electronic patient record or computerized patient record) is defined as a longitudinal collection of electronic health information about individual patients or populations [1]. Medical data are recorded in digital format in order to provide secure, real-time, patient-centric information needed to clinical decision-making through providing the access to a patient's health information at the point of care [2]. Such records may included a whole range of data in comprehensive form, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, and billing information.

The electronic health records become part of the practices of physicians in the United States of America [3,4], Canada [5], England [6,7], Western [8,9] and Eastern Europe [10-12]. Their used proved to improve the patient care and procedures [13,14].

The European and national legislation establish legal aspects regarding personal data protection in electronic records. The protection of personal data represents a new field for Romania's legislative space. Its' essence regards, in a generic form, the natural person's right of protection of those specific features which lead to his/her identification and the state's correlative obligation of adopting adequate measures to ensure an efficient protection. The present study aimed to analyze the legislation and reglementations in European and Romania and to highlight positive and negative points.

Material and Method

Studies which refer to the legal aspects beside data protection were identified through electronic literature search of BMC Medical Informatics and Decision Making, accessing the site of Official Journal of the European Union online and the national official site of the competent authority in this area from Romania. All the collected information's regarding data protection is laying down in relation with health card strategy for Romania to find solutions to improve the legal of personal medical data protection.

Results and Discussions

International, Community and National Legal Aspects

In USA, Health Insurance Portability and Accountability Act of 1996 (HIPAA) [15] was introduced to improve portability and continuity of health insurance coverage in the group and individual markets. It was introduced in order to: • to combat waste, fraud, and abuse in health insurance and health care delivery; • to promote the use of medical savings accounts; • to create national standards to protect medical records; • to improve access to long-term care services and coverage; • to simplify the administration of health insurance; • and for other purposes.

There are two sections to the Act. HIPAA Title I deal with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of healthcare-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.

HIPAA seeks to establish standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data.

The Act mandates:

- Standardized formats for all patient health, administrative, and financial data;
- Unique identifiers (ID numbers) for each healthcare entity, including individuals, employers, health plans and health care providers;
- Security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual.

In the European Community and also in Romania the law that guides the data protection is represented by the Directive 95/46/EC [16]. This Directive define the principles of the processing of personal data wholly or partly by automatic means, and the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

In Romania, the authority that implements the Directive 95/46/EC is the National Supervisory Authority for Personal Data Processing. Set up, under the Law no. 102/2005 [17], the Authority exerts the competence established mainly by the Law no. 677/2001 [18], in terms of independence from any public authority or private entity.

The competences of the National Authority for the Supervision of Personal Data Processing are specific for any institution of control, including the investigation of personal data processing conducted under the Law no. 677/2001 [18] and the sanctioning, if it comes out that the legal dispositions were infringed by the personal data processors, as a result of self-notification or based on complaints filed by the people who's rights were infringed.

The 677/2001 [18] law applies to personal data processing, performed, totally or partially, through automatic means, as well as to the processing through means other than automatic ones, which are part of, or destined to, a personal data filing system.

This processing can be carried out within the activities of data controllers established in Romania, as well as by controllers not established in Romania, by using any means on Romanian territory (the data controller must designate a representative which must be a person based in Romania).

Legitimacy Regarding the Personal Data Processing

The main condition of legitimacy data processing is represented by the consent of the subject.

Therefore, personal data processing cannot be done if the subject has given his/her express and unequivocal consent for that processing.

The data subject's consent is not required in contract to which the data subject is party of, or in order to take some measures, at his/her request, before signing that contract or previous agreement and when the processing:

- a) Is required in order to protect the data subject's life, physical integrity or health or that of a threatened third party;

- b) Is required in order to fulfil a legal obligation of the data controller;
- c) Is required in order to accomplish some measures of public interest or regarding the exercise of public official authority prerogatives of the data controller or of the third party to which the data are disclosed;
- d) Is necessary in order to accomplish a legitimate interest of the data controller or of the third party to which the data are disclosed, on the condition that this interest does not prejudice the interests, or the fundamental rights and freedoms of the data subject;
- e) Concerns data which is obtained from publicly accessible documents, according to the law;
- f) Is performed exclusively for statistical purposes, historical or scientific research and the data remain anonymous throughout the entire processing;

The Rights of the Data Subject

As a guaranty to achieve the aim of the law, the rights of the subject were expressly included by the legislative [18]:

- a) Informing the Data Subject
- b) The Right of Access to Data
- c) The Right of Intervention upon the Data
- d) The Right to Object
- e) The Right Not to be Subject to an Individual Decision
- f) The Right to Refer to a Court of Law

Despite that the law states clearly that the subject data processing regarding health status is forbidden, it leaves two legal ways to do this:

1. If the subject has given his/her express and unequivocal written consent – this way involves a pragmatic approach of the patient in the attempt to explain the scope of collected information's and the way how it is protected, the patient's privacy during the data processing. This approach can be done only by well-trained personnel beside communication techniques with the patient.
2. The second way is represented by the possibility of data processing when the target is to achieve what we want in the moment of admission in the medical facility – healing the patient. This way can be used only to collect medical data in the facility, but prevent transmission of the data to another part if the data contain information's which can lead to person identification. This aspect does not represent an obstacle when the data's are used for statistical, scientific or research purposes. But, when we intend to use the data's to trace the time evolution of medical status for person's who receive medical care from different medical facilities it becomes compulsory the possibility to realize the correlation between personal identification data and medical history data of the person. In this situation a written consent became compulsory [19].

Relation between Community and National Law and Health Card

E-health strategy suggests, for short and medium time, building of an Integrated Informatics Health System (IIHS) [20]. One of the main targets of this strategy is represented by "National health card with UE level compatibility". This target established that for each person included in the Romanian health social system to be provided a health card. This health card will have minimum information's:

- a) Identification data and personal numeric code;
- b) Medical disease which can threaten patient life
- c) Allergy;
- d) Blood type and Rh;
- e) Expire data;
- f) Identification number and the acronym for Healthy Ensure House where the patient is registered
- g) Card number

According to this strategy in year 2011 the health card will be put in place and is expected starting that moment to have some benefits regarding access of the health electronic systems:

- Because these cards involve in the same time a card reader is obviously that the identification procedures of the patient and of the Health Ensure House where the patient is registered will be accelerates.
- All identification data for a patient will be automated included in the Electronic Health Record;
- The health care provider and drugs suppliers will have on line information's regarding emergency conditions for a patient (blood type, Rh, life threatening diagnostics, allergy)

The link between Health Card and the classic system used for person identification is represented by the Personal Numerical Code (PNC) of the health ensured person. Because the system implemented by the PNC is in use, until the Health Card will be implemented, these represent the best solution for patient identification in medical networks. After the Health Card will be available it can be used for identification the number of the card, but till the system implemented by this card will be stabilized the optimum way will be PNC.

What can be an advantage for the health card is represented the possibility to include, in the law what will be promote for the health card, a specific point that specified the acceptance to read all medical data available on the networks in the moment when an ensured person give to the medical personal the card to be read in a card reader. This part of the law must be prepared in time by discussion with civil society, health ensured organizations, law writer, representative of the private and state medical care units, to find a common accepted formula and what to not violate EU norms. It rest an open point the issue of the patient which are not able to give them consent when arrive in a medical care unit. In this situation the principle of life rescue must be more important than the law specification regarding personal data protection.

Conclusions

Country with traditions in data processing has established legislation that rules this activity. These rules involve also personal data protection.

The legislation that government the data protection in Romania is based on the European legislation. They are not significant differences between European and Romanian law.

The health card will be the next logic step to improve the quality of health care. The task to put in practice this card will be not easy. It will be necessary to prepare the moment when this card will operate so that it achieve entire potential. The aspects what must be take in consideration are the following: the law aspects, the management aspects, the infrastructure aspects.

References

- 1 Gunter TD, Terry NP. The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions. *J Med Internet Res* 2005;7(1). Available from: URL: <http://www.jmir.org/2005/1/e3/HTML> (cited 28 October 2009).
- 2 Electronic Health Record [online]. Available from: URL: http://en.wikipedia.org/wiki/Electronic_health_record (cited 10 September 2009)
- 3 Jha AK, Ferris TG, Donelan K, et al. How common are electronic health records in the United States? A summary of the evidence. *Health Aff (Millwood)* 2006;25:w496-w507.
- 4 Hing ES, Burt CW, Woodwell DA. Electronic medical record use by office-based physicians and their practices: United States, 2006. Advanced data from vital and health statistics (DHHS publication no. (PHS) 2008-1250). No. 393. Hyattsville, MD: National Center for Health Statistics, October 26, 2007:1-7.
- 5 Orchard MC, Dobrow MJ, Paszat L, Jiang H, Brown P. Access to electronic health records by care setting and provider type: Perceptions of cancer care providers in Ontario, Canada. *BMC Medical Informatics and Decision Making* 2009;9(1):art. no. 38.
- 6 Dwivedi AN, Bali RK, Naguib RNG. Implications for healthcare knowledge management systems: A case study. *Annual International Conference of the IEEE Engineering in Medicine and Biology - Proceedings* 2005;7:5668-5671.

- 7 Mitchell N, Randell R, Foster R, Dowding D, Lattimer V, Thompson C, Cullum N, Summers R. A national survey of computerized decision support systems available to nurses in England. *Journal of Nursing Management* 2009;17(7):772-780.
- 8 Hübner U, Schaubmayr C, Flemming D, Sellemann B, Aehlen C, Ammenwerth E. ICT supporting nurses and physicians in hospitals: results of a comparative survey in Austria and Germany. *Studies in Health Technology and Informatics* 2009;146:20-24.
- 9 Daniel C, Jais J-P, Fadly NE, Landais P. Electronic health records and biomedical research. *Presse Medicale* 2009;38(10):1468-1475.
- 10 Karahoca A, Bayraktar E, Tatoglu E, Karahoca D. Information system design for a hospital emergency department: A usability analysis of software prototypes. *Journal of Biomedical Informatics* 2009, doi:10.1016/j.jbi.2009.09.002.
- 11 Sherman SW. Electronic health records. *Journal of the Medical Association of Georgia* 2009;98(3):3.
- 12 Siantou V, Athanasakis K, Kyriopoulos J. The Greek healthcare system. *World hospitals and health services : the official journal of the International Hospital Federation* 2009;45(1):32-34
- 13 Deckelbaum DL, Feinstein AJ, Schulman CI, Augenstein JS, Murtha MF, Livingstone AS, McKenney MG. Electronic medical records and mortality in trauma patients. *The Journal of Trauma* 2009;67(3):634-636.
- 14 Ram MB, Carpenter I, Williams J. Reducing risk and improving quality of patient care in hospital: The contribution of standardized medical records. *Clinical Risk* 2009;15(5):183-187.
- 15 Health Insurance Portability and Accountability Act of 1996 [online]. Available from: <http://www.cms.hhs.gov/hipaageninfo/downloads/hipaalaw.pdf> (Accessed: October 9, 2009).
- 16 DIRECTIVA 95/46/CE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. [online]. Available from: URL <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:17:31995L0046:RO:PDF> (Accessed: October 9, 2009).
- 17 LEGE nr. 102 din 3 mai 2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal Parlamentul României adoptă prezenta lege. [online] Available from: URL: <http://www.dataprotection.ro/servlet/ViewDocument?id=39> PDF (Accessed: October 9, 2009).
- 18 Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date [online]. Available from: URL: http://legislatie.resurse-pentru-democratie.org/677_2001.php (Accessed: October 9, 2009).
- 19 Halamka J, Ascenzo C, Bates D, Debor G, Glaser J, Goroll A, Stowe J, Tripathi M, Vineyard G. Health Care IT Collaboration in Massachusetts: The Experience of Creating Regional Connectivity *Journal of the American Medical Informatics Association* 2005;12:596-601.
- 20 Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal [online]. Available from: URL: <http://www.dataprotection.ro> (Accessed: October 9, 2009).