PROTECTION OF CLINICAL DATA
Comparison of European with American Legislation and Respective Technological Applicability

C. Pereira[1,2], C. Oliveira[1,2], C. Vilaça[1,2] and A. Ferreira[1,3]
[1]*Faculty of Medicine of the University of Porto, Al. Prof. Hernâni Monteiro, 4200-319, Porto, Portugal*
[2]*Faculty of Sciences of the University of Porto, Rua do Campo Alegre, s/n, 4169-007, Porto, Portugal*
[3]*CINTESIS – Center for Research in Health Techonologies and Information Systems, University of Porto, Porto, Portugal*

Keywords: Health legislation, Computer security, Health insurance portability and accountability act, Recommendation No R (97)5, Privacy.

Abstract: The use of computer applications in health services is essential but difficult to make it right. The challenge is to balance two values: the free access to patient sensitive and personal information and the protection of the privacy and confidentiality of the patient. The European Union and the United States tried to solve this challenge by implementing legislation on the protection of clinical data. The European legislation is comprehensive and regulated by Supervisors and each Member State creates its own legislation in accordance with the Recommendations. On the other hand, the American legislation is specific, the organizations have a self-regulatory system and each state creates the State Law which is governed by Federal Law. The aim of this paper is to compare the European legislation - "Recommendation No R (97)5"with the American legislation – "Health Insurance Portability and Accountability Act" at the level of information security in healthcare, regarding new security technologies and mechanisms applied in the area of safety monitoring of clinical data. Both legislations are neutral concerning the selection of technology that the State wants to use. These laws must be adaptive to the changing technology, to ensure patients' privacy under any circumstance.

1 INTRODUCTION

One of the biggest challenges of the informatics' era arises from the use of computer applications in health services while maintaining the same traditional principles. This challenge involves achieving a balance between: the free access to patient sensitive and personal information and the protection of the privacy and confidentiality of the patient.

Currently healthcare services are supported by new information and communication technologies which includes hardware and software linked to databases to register, manipulate and search data in different formats. The amount of data and access to it has increased against the spread of computer networks within each institution but also between different health institutions. The increase in the availability of healthcare Information Systems (ISs), coupled with the high sensitivity of clinical data stresses the need for its proper regulation and protection. These healthcare ISs must use protection mechanisms to ensure compliance with the legislation in force. Therefore, there is an urgent need to develop new security mechanisms that can be taken within the health organizations.

This article aims to compare the European and American legislation on the security and protection of clinical information and to identify the respective technological applicability.

2 BACKGROUND

The concept of information security in the clinical area has undergone a great development. From the 4th century BC that doctors comply with the Hippocratic Oath, which is expressed to protect the privacy of the patient.

Several authors agree that in the clinical area it remains valid the decomposition of information security into three dimensions: confidentiality,

Pereira C., Oliveira C., Vilaça C. and Ferreira A..
PROTECTION OF CLINICAL DATA - Comparison of European with American Legislation and Respective Technological Applicability .
DOI: 10.5220/0003165505670570
In *Proceedings of the International Conference on Health Informatics* (HEALTHINF-2011), pages 567-570
ISBN: 978-989-8425-34-8
Copyright © 2011 SCITEPRESS (Science and Technology Publications, Lda.)

integrity and availability. The **Confidentiality** is necessary to ensure that patient data is protected and cannot be accessed by unauthorized persons, whether accidental or deliberately. The **Availability** is necessary to preserve the resources and services of healthcare ISs that must be accessible when needed, particularly in emergency or intensive care situations. The **Integrity** is necessary to ensure that clinical information stored or in transit is not corrupted or changed improperly by unauthorized users or through operational errors (in the introduction and manipulation of data), software bugs, viruses or equipment malfunction (ISO, 2006).

Since 1997, European legislation regulates the protection and treatment of confidentiality, integrity and availability of medical data trough "**Recommendation No. R (97) 5** of the Committee of Ministers to Member States on the Protection of Medical Data", which stated in Principle 3.1 that "The respect of rights and fundamental freedoms, and in particular of the right to privacy, shall be guaranteed during the collection and processing of medical data" (Rec, 1997). This European recommendation was the basis for the creation of specific legislation in each Member State.

Since 1996, American legislation, through **Federal Law 104-191**, known as the **"Health Insurance Portability and Accountability Act of 1996" -** HIPAA (HIPAA, 1996) rules privacy, information security and standards of all entities providing healthcare or having access to data from healthcare units. For this legislation, two regulation documents were created. They provide a set of best practices that healthcare institutions must follow in order to guarantee a minimum level of information security. These documents are called **Security Rule** (2003) and **Privacy Rule** (2002) that rules the organizations in the use and disclosure of confidential, personal and identifiable health information about patients that is designated "Protected Health Information" (PHI). The PHI includes information such as demographic data that is utilized for the user identification, data from their past, present or future health status and data related with the healthcare services.

3 EUROPEAN LEGISLATION *VS* AMERICAN LEGISLATION

European legislation is a comprehensive law, implemented by supervision, which creates European directives and recommendations that are followed by the Member States trough the creation of national legislation. The right to privacy is explicit in the Charter of Fundamental Rights. One the other hand, American legislation is a specific law, implemented by different mechanisms, which creates the federal law that is followed by the United States of America. The right to privacy is not explicit in the Constitution.

Another relevant difference is concerned about the regulation of the legislation. In Europe this adjustment is made by authority Supervisors such as the European Data Protection Supervisor (EDPS), the Europol Joint Supervisory Body and the Schengen Joint Supervisory Authority. Within each Member State there is an authority for the data protection that should create recommendations and ensure its compliance. In American legislation, it is assumed that organizations govern themselves autonomously.

For this comparative analysis a selection regarding the security issues of clinical data was made of both legislations. In the European legislation, it was selected the chapter 9.2 of the "Recommendation No. R (1997) 5" and in relation to American legislation this study focused on the Security Rule document from HIPAA.

Table 1, presents the analysis of clinical data security recommendations from both legislations and some examples and their descriptions of technologies or mechanisms that could have applicability in the different types of control, at the level of: the physical entrance to installations, data media, memory, utilization, access, communication, data introduction, transport and availability.

4 DISCUSSION

Regarding the security of personal information the authors consider that the European legislation has the advantage of being: (1) a good reference model for the good practice with flexibility in the recommendations to Member States; (2) technologically neutral; and (3) with an increased awareness and concern about the security of clinical data. However, European legislation presents some weaknesses, such as for instance: (1) the dubious association between certain key concepts ("personal data" and "real privacy"); (2) the difficulties in practical implementation due to the inconsistent role of data protection authorities; and (3) the outdated rules in transferring information to other countries. Moreover, most Member States are governed by national rules of clinical data protection and the harmonization remains more apparent than real. This

Table 1: Recommendation No. R (97) 5 *vs* HIPAA in terms of clinical data security and respective technological applicability.

Recommendation Nº R (97) 5	HIPAA	Technological Applicability	Description
Control of the entrance to installations			
To prevent any unauthorized person from having access to installations used for processing personal data.	To control and validate physical access to its facilities containing information systems having electronical PHI (ePHI) or software programs that can access ePHI.	1-Biometry 2-Smart card 3-Access code	1-Identification through a physical characteristic. 2-Card with memory chip or internal. 3-Access to systems through a PIN (ISO, 2006).
Control of data media			
To prevent data media from being read, copied, altered or removed by unauthorized persons.	To use encryption to protect the confidentiality, integrity, and availability of its ePHI.	4-Passwords and Automatic logoff 5-Encryption 6-Access control 7-User profiles 8- Policies and security protocols 9-Digital signatures and certificate	4-Login mechanisms with secret passwords associated to user that could have an automatic logoff associated. 5-Process of converting text into cipher text.
Memory control			
To prevent the unauthorized entry of data into the ISs and any unauthorized consultation, modification or deletion of processed personal data.	To protect the integrity of its ePHI.	10- Audit /Monitoring 4, 5, 8	8-Plan or course of action adopted for providing computer security (ISO, 2006).
Control of Utilization			
To prevent automated data processing systems from being used by unauthorized persons by means of data transmission equipment	To maintain an effective process for creating, changing, and safeguarding passwords. To implement security measures sufficient to reduce risks and vulnerabilities of the wireless infrastructure. To establish management direction, procedures, and requirements to ensure safe and successful delivery of e-mail. To define standards to be met by all equipment Internet firewalls.	11-Firewall 12- PKI 13-IDS 5, 8, 9, 10	11-Data traffic filter that prevents unauthorized access to a private network. 12-Set of procedures, equipment, people and policies needed to create, manage, store, distribute and revoke public key certificates (ISO, 2006).
Access Control			
To select access to data and to maintain security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of: - identifiers and data relating to the identity of persons - administrative data; medical data; social data; genetic data.	To purchase and implement information systems that complies with its information access management policies. To ensure that all persons or entities seeking access to its ePHI are appropriately authenticated before access is granted.	6,7,8	6-Assurance that the resources of a data can be accessed only by authorized entities in authorized ways (ISO, 2006). 7-Subset of privileges assigned to a user groups with similar functions (ISO, 2006).
Control of Communication			
To guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment.	The organization should appropriately protect the confidentiality, integrity, and availability of the ePHI it transmits over electronic communications network.	14-VPNs 5, 8, 9, 13	13-Software for detecting, identifying and responding to unauthorized or abnormal activities of the system.
Control of data introduction			
To guarantee that it is possible to check and establish a posteriori who has had access to the system and what personal data have been introduced into the information system, when and by whom.	The organization should appropriately track and log all movement of information systems and electronic media containing ePHI to various organizational locations. Discusses what the organization should do to implement appropriate electronic mechanisms to confirm that its ePHI has not been altered or destroyed in any unauthorized manner.	6, 8, 9, 10	9-Certificate of PKI that consists in data structure that associates a public key to a specific agent which are certified by authority. 10-Measures to verify the existence of access control to information (ISO, 2006).
Control of transport			
To prevent the unauthorized reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media.	Should document repairs and modifications to the physical components of its facilities related to the protection of its ePHI.	6, 8, 14	14-Private network that uses a public telecommunication infrastructure which uses encryption to ensure privacy and security of communications.
Availability control			
To safeguard data by making security copies.	Should be able to effectively respond to emergencies disasters that impact its ePHI. Organizational processes to regularly back up and securely store ePHI.	8 15-Backup Software 16-Redundancy of equipment	15-Make copies of data to recovery (ISO, 2006). 16-e.g. power supplies, redundant servers, etc.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

fact is due to the gap in the European Directive of information protection that allows the Member States to define their own exemptions and simplifications to some constraints imposed.

As for the American legislation, the authors consider that it has the strength to promote the patient empowerment through greater control of their PHI, because the patient has the right to access and correct the information at any time and also the power to decide who has access to their clinical data. But this condition can also weaken the law because of the problems associated with the excess of freedom given to the patient in relation to access their own clinical data may intervene in the lack of preserving the "psychological integrity". This could happen when an individual has access to very sensitive data that is published on the internet, which isn't protected by the actual law. More disadvantages of this legislation are: the fact of adding to the workload of healthcare providers with the function of protects clinical information and the privacy policy that could enter in conflict with other countries due to the regulation differences.

Information security is a dynamic issue because the pace of technological change continually generates new challenges for global security policy, so the effort to security must be continuous and change accordingly by the development of new security measures and mechanisms.

There is a great difficulty in controlling, monitoring and ensuring that all procedures are what they are meant to be and lives should not be exposed by poor performance of healthcare ISs. Thus, great efforts should be made to ensure that healthcare legislation is properly applied and enforced.

The laws that under any circumstance. we have referenced in this article must be adaptive to the changing technology, to ensure patients' privacy.

ACKNOWLEDGEMENTS

The authors acknowledge the help of Professor Luis Filipe Antunes on initial discussion of this work.

REFERENCES

Cavalli E., M. A., Pinciroli F., Spaggiari P. 2004. Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics,* 73.

CEN/TC 2003. Health Informatics - Electronic Health Record Communication. *Part 4 - Security requirements and distribution rules.*

HIPAA 1996. Health Insurance Portability and Accountability Act *In:* Congress, T. (ed.). USA.

ISO 2006. Health Informatics - Privilege management and access control *Part 2: Formal Models.* Switzerland.

Joshi, J. B. D., Aref, W. G., et al. 2001. Security models for web-based applications. *Commun. ACM,* 44, 38-44.

Lumini, A. & Nanni, L. 2008. Over-complete feature generation and feature selection for biometry. *Expert Syst. Appl.,* 35, 2049-2055.

Ravera L., Colombo I., et al. 2004. Security and privacy at the private multispecialty hospital Instituto Clinico Humanitas : strategy and reality. *International Journal of Medical Informatics,* 73, 321-324.

Rec 1997. Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data. *In:* Europe, C. O. (ed.).

Tan, J. 2005. E-Health Care Information Systems: An Introduction for Students and Professionals. *Jossey-Bass / Wiley*.

Waldo, B. H. 1999. Managing Data Security: Developing a Plan to Protect Patient Data. *Nursing Economic$,* 17, 49-52.