IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 9 (September. 2013), ||V3|| PP 52-55

Personal health information security - Regulatory framework

H. Hamidović, J. Kabil
[1] *PhD, CISO, MCF EKI Sarajevo, Bosnia and Herzegovina*
[2] *M. Sc, Speech therapist, University Clinical Center Tuzla, Bosnia and Herzegovina*

Abstract: **-** Personal health information is regarded by many as being among the most confidential of all types of personal information. Due to violation of the right to privacy the European Court of Human Rights issued large number verdicts against EU countries, for failure to protect citizens' medical records and confidential data that they contain. Many data protection laws and the EU Data Protection Directive require that the data controller must implement appropriate technical and organizational measures to protect personal data. Personal health information is considered a special category of personal data, for which an extra level of protection is required under data protection rules. Taking into account increasing use of automatic processing of medical data by information systems, this paper presents issue of personal health information protection and the situation in this matter in Bosnia and Herzegovina.

Keywords: **-** *Data Protection, Health Information, Information Security*

I. INTRODUCTION

Privacy is a global issue. Citizens, today more than ever, are fearful of what information is being gathered about them and by whom, what information is being shared about them and with whom, how that information is being used, and how long it is being retained. Privacy concerns have sparked debates and provoked legislators to enact laws both protecting and restricting privacy. [1]

The Organization for Economic Co-operation and Development (OECD) has been a frontrunner in the privacy and security arenas and has contributed strongly to the development of the global legal framework. In 1980, the OECD developed its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines). Virtually all privacy legislation and directives find their foundation in this OECD document. [2] [3]

General principles from the OECD Privacy Guidelines include [3]:

- Collection limitation principle—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of a data subject.
- Data quality principle—Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- Purpose specification principle—The purposes for which personal data are collected should be specified no later than at the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes, or such others, (unclear) as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- Use limitation principle—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.
- Security safeguards principle—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.
- Openness principle—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, the main purposes of their use, and the identity and usual residence of the data controller.
- Individual participation principle—An individual should have the right to a) obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him/her, and b) have communicated to him/her data relating to him/her in an intelligible form within a reasonable time and manner and at a charge that is not excessive. If such a request is denied, he/she should be able to challenge both the denial and the data relating to him/her. If the challenge is successful, the data should be erased, rectified, completed or amended within a reasonable time;
- Accountability principle—A data controller should be accountable for complying with measures that give effect to these principles.

In 1995, the European Union (EU) raised global awareness of privacy issues with the adoption of the EU Data Protection Directive. In adopting the directive, the EU wanted to ensure that "fundamental" privacy rights were protected when personal information was processed, regardless of the national citizenship of the individual data subjects and without restricting the free flow of personal information within the EU. [4]

Bosnia and Herzegovina's data protection law is based on the EU Data Protection Directive.[5] Data protection legislation in Bosnia and Herzegovina, as well as in many other countries, require that the data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures need to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Special categories of personal data include all personal data that, among other things, reveal state of health and genetic code. The data controller must take additional technical and organizational measures in the processing of special categories of personal data. [6]

Due to violation of the right to privacy the European Court of Human Rights issued large number verdicts against EU countries, for failure to protect citizens' medical records and confidential data that they contain. [7]

II. SECURITY MEASURES

Being aware that to provide full protection of medical data it was not enough to lay down legal rules and that the controller had to take actual steps to prevent unlawful access to or use of data, whether accidental or ill-intentioned, Council of Europe, Recommendation No. R (97) 5, on the Protection of Medical Data, Principle 15.1 presents the technical and organizational steps which should be taken to ensure data security. [8]

In order to ensure in particular the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken [8]:

a. to prevent any unauthorized person from having access to installations used for processing personal data (control of the entrance to installations);
b. to prevent data media from being read, copied, altered or removed by unauthorized persons (control of data media);
c. to prevent the unauthorized entry of data into the information system, and any unauthorized consultation, modification or deletion of processed personal data (memory control);
d. to prevent automated data processing systems from being used by unauthorized persons by means of data transmission equipment (control of utilization);
e. with a view to, on the one hand, selective access to data and, on the other hand, the 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 (access control);

f. to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);
g. 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 (control of data introduction);
h. to prevent the unauthorized reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport);
i. to safeguard data by making security copies (availability control).

Implemented security measures shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks.

III. SELECTION OF SAFEGUARDS

There are two main approaches to safeguard selection, i.e. using a baseline approach and carrying out detailed risk analyses [9]:

- Baseline protection for an IT system can be achieved through the identification and application of a set of relevant safeguards which are appropriate in a variety of low risk circumstances, i.e. they fulfill at least the minimum security needs. For example, the appropriate baseline security safeguards can be identified through the use of catalogues which suggest sets of safeguards for types of IT systems to protect them against the most common threats.
- If the organization's business operations are heavily dependent on the IT system or service, and/or the information handled is very sensitive, the risks may be high, and a detailed risk analysis is the best way to identify appropriate safeguards.

Conducting a detailed risk analysis has the advantage that a comprehensive view of the risks is achieved. This can be used to select safeguards which are justified by the risks, and thus should be implemented. This avoids the provision of too much or too little protection. As this can require a considerable amount of time, effort and expertise, it may be most suitable for IT systems at high risk, whereas a simpler approach can be considered to be sufficient for lower risk systems. [9]

In 2009 Council of Ministers of Bosnia and Herzegovina adopted Regulation on storage and specific technical measures of personal data protection. This regulation prescribes specific technical and organizational measures for protection of personal data in Bosnia and Herzegovina. [6]

Comparative analyses of 133 information security controls from Annex A of the International Standard ISO/IEC 27001 [10] and the measures prescribed by regulation of the Council of Ministers of BiH [6] shows that some of the essential security controls has been omitted by the regulator in Bosnia and Herzegovina, such as:

A.6.1.8 - Independent review of information security - The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur. [10]

Although baseline security safeguards identified through the use of catalogues or prescribed by law can protect IT systems against the most common threats [11], one should know that many organizations mistake compliance with security. Documenting adherence to sometimes overly simplistic regulatory or contractual requirements may not necessarily result in actual security improvements. In fact, there is growing evidence that the resources applied to compliance may actually detract from true security efforts. While it is clear that regulatory and/or contractual requirements must be abided, it is a mistake to assume good compliance necessarily equates to a safer organization. [12]

IV. CONCLUSION

Health informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. At the same time, the data they contain is confidential and its integrity must be preserved. Because of these critical requirements, and regardless of their size, location and model of service delivery, all health care organizations need to have stringent controls in place to protect the health information entrusted to them.

Data protection laws in many countries require that the data controller must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks represented by the processing of the personal data. Health information is considered a special category of personal data, for which an extra level of protection is required under data protection rules.

To provide full protection of medical data it was not enough to lay down legal rules. Data controller had to take actual steps to prevent unlawful access to or use of data, whether accidental or ill-intentioned.

Although, baseline security safeguards prescribed by law can protect IT systems against the most common threats, for IT systems at high risk detailed risk analysis is the best way to identify appropriate safeguards.

Application of best practices proposed by the international industry standard such as ISO/IEC 27001 is no guarantee of compliance with legal obligations, but it may offer health care organizations a good starting point on the road to addressing international legal requirements for security in health. However, the challenge is sustaining these good practices.

REFERENCES

[1] Westby, J. R. (editor), *International Guide to Privacy*, American Bar Association, 2004

[2] Hamidovic H., *An Introduction to the Privacy Impact Assessment Based on ISO 22307*, ISACA Journal, Volume 4, Information Systems Audit and Control Association, 2010

[3] Organization for Economic Co-operation and Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980
[4] European Union, *The Data Protection Directive*, Directive 95/46/EC
[5] The Parliamentary Assembly of Bosnia and Herzegovina, *The Law on Personal Data Protection*, Official Gazette of Bosnia and Herzegovina, no. 49/06, 2006
[6] The Council of Ministers of Bosnia and Herzegovina, *Regulation on storage and specific technical measures of personal data protection*, 2009
[7] The Council of Europe, *The case-law of the European Court of Human Rights concerning the protection of personal data*, DP (2009) CASE LAW, Strasbourg, March 2009
[8] The Council of Europe, Committee of Ministers, *Recommendation No. R (97) 5 on the Protection of Medical Data* (Feb. 13, 1997)
[9] ISO/IEC TR 13335-4:2000 Information technology -- *Guidelines for the management of IT Security -- Part 4: Selection of safeguards*, 2000
[10] ISO/IEC 27001:2005 Information technology -- Security techniques -- *Information security management systems – Requirements,* 2005
[11] Verizon Business Risk Team, *2008 Data Breach Investigations Report,* URL: http://www.verizonbusiness.com/resources/security/databreachreport.pdf
[12] Internet Security Alliance (ISA) / American National Standards Institute (ANSI), *The Financial Management of Cyber Risk*, 2010