SECURITY, PROTECTION AND PRIVACY OF INFORMATION IN HEALTHCARE

Radmila Jovanova,
Faculty of Economics, "Goce Delcev" University - Stip,
(Republic of Macedonia)

The development of information technologies which are based on the production and application of electronic systems for data processing, telecommunications equipment and other suitable equipment opens the opportunity for unlimited data concentration, their grouping and search based on various characteristics. This causes a massive use of data for individuals in different organizations, registries, etc. Patients and the public must be confident that their information is kept by all security measures and are exchanging under the law, legal, ethical and technological processes.

Before we start to talk about privacy and protection of health information, we must define what exactly personal data is, because the health information is some kind of their subcategory.

1. Personal data is any information relating to the identified person or individuals who can be identified.[1] Of special importance are name, surname, ID number, phone number, sexual orientation etc;

2. Health information can be defined quite broadly as information that is created or received in any form or medium by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse, and that "relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for health services provided to an individual".[2] For example, diagnosis, blood test results, blood group, medical treatment etc.

Almost every time we go to the doctor, we are sharing our personal data and information about our health. All of them in some way can be abused and can be threat for patient's privacy. The main question here is who can accede to this information? First of all, it is the whole medical personnel that the patient comes in contact with, when he is going to doctor. People, who carry out their practice in healthcare organizations, also have access to these data. If they don't know to keep the professional secrets, there could be a possibil-

[1] http://www.dzlp.mk/files/uploads/global/ZZLP_Precisten%20tekst.pdf, 17.02.2010

[2] William H. Roach, Medical records and the law, Jones & Bartlett Publishers; 4 edition , USA, April 24, 2006, page 125

ity to be undermined patient's privacy, reputation and honor. Privacy of health information can be defined as a professional obligation of doctors, nurse, non-medical researchers and other public health professionals. Privacy is right of any individual or institution to decide when and to what extent will share information about themselves and others. In any system of data protection must not neglect the human factor. It is important to know that non - medical employees must be motivated to adhere to the same principles of professional confidentiality which are required for healthcare employees.

Security of information is a result of various measures which contribute for information protection from unwanted things, such as modifications, deleting or loosening personnel and other data which are defining the patient. From one side, security is related to protection of the integrity of data, and from the other side, on serving privacy on the patient and the doctor.

For how long the information should be kept? [3]

1. Personal data should not be kept longer than necessary to fulfill the purposes for which are collected;

2. In healthcare organizations, basic medical documentation is kept for 15 years from the last data entry;

3. Medical history of the disease is kept 15 years after the death of the patient.

Information security deals with the protection of information within a given domain. In this context it is usually expanded into tree different directions:[4]

- Confidentiality - assurance that particular information is accessible (read, write or execute) by authorized personal only
- Integrity - assurance that during processing no unauthorized changes of information are possible.
- Availability - assurance that information can be used at will.

Issues which are related on the organizational measures and rules for data protection include:

1. Format and authority of a special organization which are entrusted to implement the law and the other measures for data protection.
2. Technical standards for handling with the computer center and using of programming techniques in the operating systems.
3. Taking precautions relating to computer equipment.
4. Training of the persons who will processing the data and more.

[3] http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/4282378027296612126011011481_ FILES/Preporaki% 20za%20graganite% 20zdravstvo.pdf, 17.02.2010

[4] http://books.google.com/books?id=Z6azHX3wJKUC&pg=PA50&dq=security+of+health+information&cd=1#v=onepage&q=security%20of%20health%20information&f=false,17.02.2010

Today, many countries in the world that have laws which are regulating the issues of data protection, namely the right to privacy. Hence, the problem of privacy is the subject of many resolutions, guidelines, directives, recommendations are adopted by the Council of Europe, Economic and Social Council, the UN office in Geneva, the European Parliament and Council of the European Union. In these documents are determined the basic goals and principles of data protection of the individuals, criterions related to quality and legitimacy of data processing for individuals, especial categories of data, exceptions and limitations to these rights and other similar issues. International organizations especially World Health Organization (WHO) and Organization for Economic Co-operation and Development (OECD) have long time experience in accumulation, distribution and using data health to inform public health and to understand the whole public health systems.

As a conclusion of all this, we can say that all public health organization should have an integrated electronic system who will restrict the information access to the patient's personal information. For example, the guard cannot access into clinical information, and the medical personnel cannot access into the data for invoices.

References

1. Adi Armnoni, *Healthcare information system: Challenges for the new millennium,* Idea group publishing, USA, 2000;
2. Computer science and telecommunications board national research council, *For the Record : Protecting Electronic Health Information*, National Academies Press, USA, 1997
3. William H. Roach, *Medical records and the law*, Jones & Bartlett Publishers, 4 edition , USA, April 24, 2006;

Web sources

1. http://dzlp.mk/FILES/1164/PUBLIC/CONTENT/428237802729661212626011011481_FILES/Preporaki%20za%20graganite%20zdravstvo.pdf;
2. http://www.dzlp.mk/files/uploads/global/ZZLP_Precisten%20tekst.pdf;
3. http://books.google.com/books?id=Z6azHX3wJKUC&pg=PA50&dq=security+of+health+information&cd=1#v=onepage&q=security%20of%20health%20information&f=false;
4. http://www.scribd.com/doc/12391658/Security-in-health-information-systems;
5. http://www.scribd.com/doc/18429810/Dictionary-of-Health-Information-Technology-and-Security;
6. http://www.himss.org/content/files/PrivacySecurity/PIIWhitePaper.pdf.