Aspects of healthcare computer networks security in the education of students of medicine and healthcare management

Iskra Mircheva

Dept. Social Medicine and Biostatistics, Medical University, Varna, Bulgaria

Preface

Preserving the privacy of medical data is a question that for centuries has been considered fundamental in medicine and healthcare. Ever since the 4-th century BC the medical professionals take the oath of Hyppocrates that obliges them to keep in secret the information they have obtained from their patients during the process of delivering health care.

The ever-growing implementation of information technologies in healthcare and medicine, especially the developments of electronic medical records (EMR) and the connection of clinical data bases, as well as the freedom these systems offer in relation to their usage force the development of new policy and security procedures for protection the privacy and confidentiality of medical data. As more healthcare organizations acquire, process and store information in electronic format and use local and public communication systems and networks to transfer medical information between the different healthcare institutions, they have to secure adequate mechanisms for the protection of this information.

The field of data security and protection is not static. The increasing use of information technologies and computer applications in medicine and healthcare makes the question of data security even more important, especially when these applications concern patient care and personal patient medical data. Besides, the new technologies offer new opportunities as well as new threats that require new security measures.

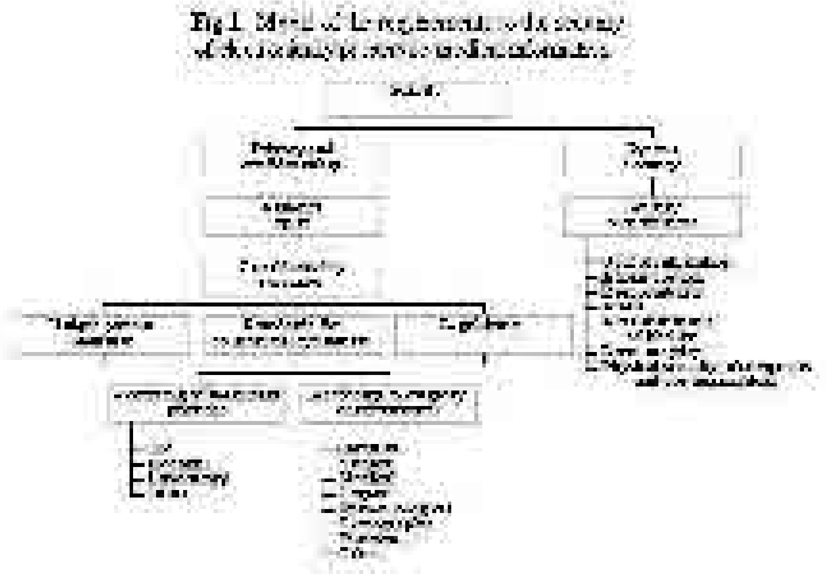
That is why the education of medical students on the questions of medical data security is of enormous importance.

This paper discusses the additional knowledge that students of medicine need in conjunction with the development and the implementation of adequate policies and measures for protection of the electronically preserved and transferred medical informatin.

1 Confidentiality and security measures

1. The requirements to the security of electronically preserved medical data might be generalized in the model shown on Figure 1.

The computerization of clinical information and especially the implementation of computer networks in medicine and healthcare could not be achieved if the individuals are not convinced that there exist sufficient and adequate measures for the protection and the security of the privacy of their personal medical data.



This is what medical specialists should be aware about as early as possible in their professional career.

The recognition of patient's right for privacy of his/her medical data should be in the base of all security measures. Confidentiality measures are in conjunction with this patient's right. Confidentiality concerns legal issues.

In order to attain the balance in confidentiality three different activities should be achieved:

The first activity concerns the development of universal patient identifier. The shared use of the medical data from the EMR and the medical computer networks brings forward the importance of developing a universal patient identifier for the whole healthcare system. In Bulgaria we have a system (ESGRAON), according to which every Bulgarian citizen and permanently residing foreigners are given unique personal 10-digit identification number (UID). This UID is a convenient instrument for organization of different sets of personal individuals information, for registry, statistics etc. However, the use of this UID as a unique patient identifier is not appropriate. First, it is well known that every number (and this UID is a number, although comprising some protective elements), used as a universal identifier could easily cross the boundaries of its initial use and to spread over to other domains. This makes it absolutely inappropriate for the area, using such sensitive information as personal medical data. On the other hand, this UID is written along with the name of the individual on a number of his/her personal identification papers. This makes the UID too unconcealed and therefore inapplicable as a unique patient identifier.

My personal opinion is that the UID should be extended with some additional personal patient information, as for example two characters representing the patient father's name and two characters representing the patient's mother maiden name.

The second activity covers the development of standards for the confidentiality measures concerning medical information. Such standards are currently being developed in USA by three committees: E31.17 - Privacy, access and confidentiality; E31.20 - Security of data and health information systems; E31.22 - Medical transcription and documentation. Other organizations that work in this area are HL7, ACR/NEMA - DICOM, the Institute of electronic patient record in USA. In Europe, CEN/TC-251 (Medical informatics) deals with the problems of confidentiality and security of medical data. A number of standards have been approved: ENV 12924:1997 - Medical informatics - categorization of security and protection of information systems in healthcare; ENV 13608:1999 - Medical informatics - Security of communications in healthcare; ENV 13694:1999 - Medical informatics - Standards for the quality of the software for protection and security of data in healthcare; ENV 12388:1996 - Medical informatics - Digital signature algorithms.

The third activity concerns the legal issues. In Europe act the Council of Europe Convention 81/108/EC[1] for the Protection of Individuals with regard to Automatic Processing of Personal data and the Council of Europe Directive 95/46/EC[2] on the Protection of Individuals with regard to the Processing of Personal Data. According to Directive 95/46/EC every member state is obliged to develop standards and legal issues concerning data acquisition, protection and storage of personal data (medical data is not exclusively envisaged). The aim of this Directive is to harmonize the legislation for data security and protection in all EC member states. The European countries were supposed to bring their legislation in concordance with this Directive till the end of 1998 (24/10/1998). Medical data is specially foreseen in additional Recommendations R(97)5 for security of medical data.

In a number of states (Finland[3], New Zealand[4],[5], United Kingdom, Canada[6]) act different legal issues.

The security measures originate along with the confidentiality measures but substantially differ from them. They concern the system and are related to the responsibilities of the organizations and functional requirements.

The security of health information comprises different areas as for example user identification, access control, availability and reliability, data integrity, responsibility, audit, control etc. Most of them go in parallel with the confidentiality measures.

Health organizations should assess the technologies for data protection in two aspects: efficiency of the protection of patient medical data privacy and the costs of these technologies including the restriction or prohibition of physician's access to information, necessary for medical decision making; the purchase of security technologies in the information system environment; prices for current management, operation and maintenance of the information system; prices for user dissatisfaction, generated as a result of improper operating interfaces and procedures; prices for the time spent by the user for fulfilling the security requirements.

Organizations should aim to implementation of balanced measures concerning the threats to information security and the risks against unauthorized acts but on reasonable price. This will acquire appropriate education of managers, system maintenance personnel and above all users, including the patients themselves.

At the moment the existing data security technologies are directed to information security in the frames of the healthcare institution and do not concern the problems of unlimited use of health information, once it leaves this institution and is transferred to other health information users.

1.1 User identification

Every computer system should be able to unmistakably identify the individual who seeks access to the information, stored in it. The identification is base on one or more of the following criteria:

- something that is possessed (i.e. a key, a card);
- something that is known (i.e. a password, personal identification number etc.);
- something concerning the individual (i.e. a signature, a finger print, voice, DNA, model of the retina or the iris etc,);
- something concerning the location (i.e. a cable connected terminal, a phone number for return call, network address etc.)

The most reliable way of user identification in the healthcare field is the personal user unique account identifier and a password or a personal identification number used along with a card. Both, the password and the card are required for user identification. This method combines something that is known with something that is possessed. This approach does not depend on user location.

Concerning user identification, CEN/TC-251 has developed the standard ENV 12251:1999 - Medical informatics - Management and security through password identification - user identification in healthcare. This standard is intended to improve the identification of individuals who want to use healthcare information systems. It covers such items as: unique user identification; system login procedures; storage and operation with passwords; end of password session warning; changing passwords etc. Another standard is ENV 12018:1997 - Medical informatics - Identification and structure of administrative and common clinical data for the implementation of temporary connecting devices (including electronic cards). This standard offers a common framework for structured data, used in temporary connecting devices to the system, such as electronic cards. It also notes the structure for data interchange, that uses the international standards ASN.1 and EDIFACT for electronic data interchange between electronic cards and medical systems.

1.2 Access control

The assignment of access rights is one of the main problems of electronically preserved medical data security. Access control should be assigned on the basis of precise analysis of the needs and the requirements of the users (user aspect) for access to the different sets of medical data (data aspect) in relation to the healthcare institution (institutional aspect).

We propose some basic criteria for different specialists access to the different types of data in the electronic medical record (EMR). According to our model of the access criteria, the information, contained in EMR might be logically divided to the following main categories (Figure 2):

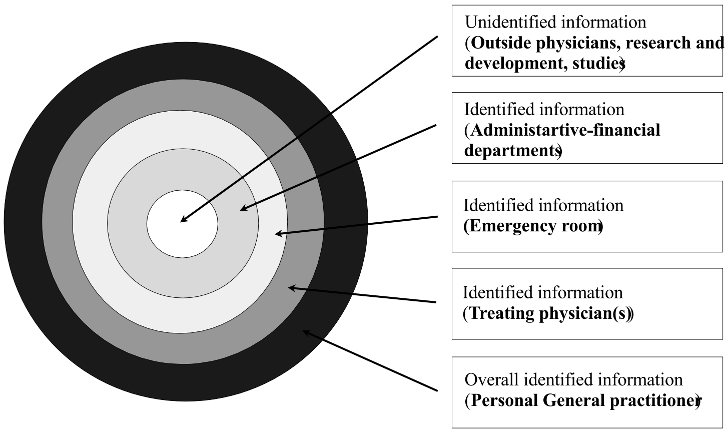
- Unidentified information that can be used for different clinical and epidemiological studies. It should be easily accessed. The only restriction at organizing such information is to respect the principles of informed patient consent;
- Identified administrative-financial information. This is the information about diagnoses, procedures, treatment, hospital stay etc. used for the costs assessment. Access to such information should be granted to administrative personnel considering to extremely high level the security of the confidentiality of such data;
- Identified information, representing basic patient data, including chronic diseases, allergies, risk factors, current treatment etc. Physicians can use this information in case of emergencies. As this information might be very sensitive (i.e. diagnosis AIDS), access to it should be limited to only specified personnel in emergency rooms. These could be physicians, but considering that the main task of the physician in emergency room is to save patient's life, such an access could be granted to lower rank medical personnel (i.e. nurses). Another alternative is to grant the emergency departments access to such information in the EMR;
- Identified information, concerning current episode of care. A full physician's access to such information should be granted to treating physician(s). Other clinicians in the same healthcare unit could be granted access to this information only in case of necessity (i.e. when on duty or when patient care requires it). Outside physicians should not have access to such information except the patient's general practitioner.
- Identified patient information, concerning the patient health status as a whole. Practically this is the patient's EMR. Access to this information should have only the patient's personal physician (his/her general practitioner) who is held responsible about the overall health status of the patient.

Adequate access control should be secured to all levels of information, except to unidentified information. The personal medical information should also be easily accessible by the patient himself.

The security of medical information can improve if an independent national healthcare network is established. Such an independent network is generally used for the most important national services (i.e. state defense, power engineering, banking etc.). Healthcare has also to be regarded as one of the most important national services and requires the establishment of such independent healthcare network. As for Bulgaria, this can be easily achieved, as networks are not so common at the moment. Concerning Internet access, there are a number of Internet providers but the quality is far from the desired. So, the establishment of an independent healthcare network, starting from ”zero” will save at least those costs, required for the adaptation of existing networks.

1. In order to carry out the access control to medical information, the specialized healthcare network has to focus the interfaces from Internet to control gateways and firewalls thus accomplishing first level of security, so the networks of the individual organizations could function using adequate access control. Such a network has to be designed to use cryptographic and other information security measures.

Fig. 2. Access model of different specialists to EMR


Unidentified information
(Outside physicians, research and development, studies)
Identified information
(Administartive-financial departments)
Identified information
(Emergency room)
Identified information
(Treating physician(s))
Overall identified information
(Personal General practitioner)

2 Balance between confidentiality and security

Two categories of factors influence both confidentiality and security.

On one hand the patients' attitude, the general opinion, the press and other factors contribute to the fear that computerization will violate the right for privacy of the personal medical information. The computerization raises the risk of improper use of health information.

On the other hand, three main questions against confidentiality and security could be raised.

First, the confidentiality may restrict access to medical information and therefore cannot only hamper the work of the medical specialists, but it can have negative influence on the quality of health care.

Second, the strict confidentiality and security measures may prove too hard for the users of medical information.

Third, confidentiality and security may require and consume enormous financial and human resources.

At present it is better to pay attention mainly to security policy, as hardware measures are still to be improved and security devices are too expensive.

3 Confidentiality and security in the medical informatics curriculum

One of the main reasons to pay special attention to security and confidentiality issues in medicine and healthcare is derived from the results of the study wå carried out among the physicians in Bulgaria. The anonymous enquiry was filled in by 1384 physicians, working in hospitals and general practices in different regions in the country. This is about 1/5 of all physicians in Bulgaria. The results of this study show that although 91.8% of the participants in the study declare the need of special measures for security of the privacy and confidentiality of medical data, 76.1% are not aware of such measures. Practically, no such measures exist. This concerns not only Bulgaria, but also a number of other well to be countries. On the other hand, 21.5% of the physicians think that paper based medical records can be better preserved from unauthorized access than electronic medical records. All these made us consider seriously the issues on privacy and confidentiality of electronically preserved medical data.

As such topics are not included in any of the subjects of the curriculum of neither medical nor students of healthcare management, we included them in the modified curriculum of medical informatics.

Medical informatics is in the regular curriculum of healthcare management students. For students of medicine it is currently electable discipline, as the expectation is that next academic year (starting September 2001) it will be included in the regular curriculum. It covers some basic topics as medical data, information and knowledge, electronic data interchange, standards and classification systems, Hospital information systems, electronic medical records etc. A new topic was added recently - privacy and confidentiality issues of electronically preserved medical data. It covers all issues, mentioned above and mainly those concerning the basic requirements to healthcare networks security, with which the future medical specialists should be well acquainted having in mind the ever growing implementation of information technologies including electronic medical records in daily medical practice.

References

[1] Council of Europe Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal data, Strasbourg, 28 January, 1981

[2] Council of Europe Directive on the Protection of Individuals with regard to the Processing of Personal Data, 95/46/EC, L.281/31-50, 23 November 1995, *Official Journal of the EC*, L-2985, Luxemburg

[3] The Finnish Act on the Patients' Legal Status and Personal Rights, 1993

[4] The Privacy Act, New Zealand, 1993

[5] Health Information Privacy Code, New Zealand Privacy Commissioner,1994

[6] EU/SO-GIS, document 030/95, March 16, 1995, the case of Canada