Medical Informatics Europe '96
J. Brender et al. (Eds.)
IOS Press, 1996

An Actual Point of View of the Security of Medical Data: Slovenian Perspective

Gregor CERKVENIK[(1)], Mladen MARKOTA[(2)], Smiljana SLAVEC[(3)], Miran REMS[(4)], Tristan AŽMAN[(5)] and Igor PODBOJ[(6)]

[(1)] *University Medical Centre, Department of Plastic Surgery & Burns, Ljubljana, Slovenia*

[(2)] *Institute of Public Health of the Republic of Slovenia, Ljubljana, Slovenia*

[(3)] *INFONET - Engineering of Medical Informatics, Kranj, Slovenia*

[(4)] *University Medical Centre, Department of Internal Medicine, Ljubljana, Slovenia*

[(5)] *IBM Slovenia, Ljubljana, Slovenia*

[(6)] *NEOSYS: Graphics-Imaging-Networking-Integration, Ljubljana, Slovenia*

Abstract. Data security has been increasingly dealt with at various professional meetings and congress on medical informatics in Slovenia and worldwide. Recently, a number of specialization workshops have been held with the aim of setting up an effective system of data security. In the field of data security the following points need to be emphasized: (1) Data security is an integral part of planning, creating and managing the health care information systems at all levels; both in public health institutions and in private practice. (2) In addition to strictly medical information, a broad spectrum of personal, business and other data bases, which in the modern information society are closely interlinked, also need special protection. (3) Current information systems make use of various media, including classical as well as computer-assisted ones. Since in Slovenia, medical information systems are still in the phase of development, a comprehensive and legally regulated system of security should be established in order to prevent possible errors, abuse and organisation inconsistencies. (4) All those concerned with the aquisition and protection of medical data, i.e. both clerical, nursing and doctor staff, should be given adequate education, either through regular or periodical training courses, but first of all, they should be encouraged to apply the principles of data security to their everyday work. Finaly this paper presented framework of data security in health care, as well as the management, processing and exchange of medical data with to introduce a new step of the computer technology, constructed by principle of the Electronic Document Management.

1. Introduction

This paper discusses two synonymous terms: *security - protection*, which should be sometimes differentiated in theory and in practice.

Security is a broader term comprising general principles, organization and procedures for securing data, in accordance with the legal-formal basis of society (constitutional provisions and laws), ethical and moral principles, and awareness of the professional security it is intended for [1]. Due to different links between countries and the introduction of a multidisciplinary approach, there is an

increasing emphasis on international recommendations, standards, classifications and nomenclatures (in the field of health care, for example WHO and EU recommendations and conventions).

The term protection, on the other hand, denotes the methods and implementation of physical data protection.

The security and protection of data are not newly formed categories. The problem of the protection and security of data in health care, as a complex of issues, remains the basic unresolved dilemma of all discussions, meetings, symposia, conferences and congresses everywere in the world.

One has to acknowledge the fact that complete protection of data in practice *is not possible* [2]; data abuse is always possible, despite the consistent use of modern methods of data protection and even more restrictive regulations. With the introduction of new technologies, the primary principle of trusting the established data security system, trusting the reliability of personnel, and emphasizing their personal responsibility, hardware, software and communications security need to be emphasized.

The Health Care system in Slovenia has undergone important changes over past five years. In the spring of 1992 new Health Care Legislation has been adopted (Health Care in Health Care Insurance low) introducing a new system in many aspects (private practice, new Health Care Insurance system, transfer of many administrative roles to medical and pharmaceutical chambers, etc.). Within the new Health Care low, article 54 requires a preparation of a new law regulating records in Health Care System. On the other hand, the Data Protection law, which was adopted in 1992, requires that a national low should define personal data to be processed analysed or transacted.

A major step in the development of medical informatics in Slovenia was made at the beginning of 1993, when the Institute of Health Insurance of the Republic of Slovenia bought 2,750 IBM PS/1 personal computers and distributed them to health institutions, public as well as the first private ones.

The comparability of the Slovenian health care system with western systems (especially in Austria and Germany), as well as the Scandinavian countries (the Netherlands, Sweden and Denmark) in introducing information technology into the health care system at all levels of organization (from primary to tertiary, in the state and private sectors) demonstrates that Slovenia has kept pace with the introduction of new computer technologies [3]. The fact that partically all institutions in the field of health care (more than 95%) are equipped with personal computers and appropriate software, while in Germany this amounts to only 50 - 60%.

This paper at the same time draws attention to the fact that in the *transitional period (approx. 5 years)*, when one comes across both the *classical* methods of securing data (classical archive records), as well as the *modern* methods, a gradual introduction of *new, computer-assisted technologies* (such as data storage and document management stored on optical media with the advantage of "on-line" access).

2. Formal legal basis

Data security is a collection of legal, organizational and other rules and regulations, as well as, the usage of technical protective measures for ensuring the privacy of personal data. Legal aspect depends on the meaning of the word "privacy" [4], which in different countries does not imply the same thing. According to the Slovenian law, security of personal data is provided for each individual, regardless of his citizenship or place of residence.

The law regulates the basic framework for data protection and security in health care comprises not only medical professional data (from the process of treatment of patients and health care), but also different collections of personal, business and other data arising in health care as a business system. The law states detailed regulation of the degree of prevention of data privacy violation and data abuse, and imposing sanctions on them.

Recognising that Slovenia is a member of Council of Europe and considering that the aim of the Council of Europe is to achieve greater unity between its members it was necessary to implement the fundamental values of European recommendations.

On this basis Institute of the Public Health of the Republic of Slovenia has prepared a draft of the new Health Care Record law that is now in parlamentary procedure, which deals with the content and forms as a legally valid documents, regardless of electronic media, it also validates the electronic signature and the extent of documents prescribed in health care.The purpose of the project was to define the most vital elements of standardisation and harmonisation of the new law related to European recommendations. On the state level, the ministry is responsible for personal data security and supervises the compliance with laws relating to the acquisition, processing, and the use of personal data. The new legislation regulates the competencies of the Inspector for Data Security and his authorities in the event of irregularities [5].

Within the framework of the National Program of Health Informatics a public tender was oficially published by the Ministry of Health. The Institute of the Public Health was selected to perform the project. A group of experts in the field of Health Informatics and experts from all Health Care levels have prepared a document "Principles and Guidelines for the Data Privacy and Security of Health Information Systems". The document contains a set of 68 guidelines which were developed by detailing principles. Document refers to physicians, experts in health informatics, patients and Health care authorities, but also to data objects such as communication, storage, procurement etc. In the first stage, the document will be dispatched to all public and private Health Care providers [6].

3. Privacy and data security

It is important to distinguish between the terms *privacy and security* in the field of data protection. Privacy means preventing data abuse and abuse of information on individuals or organizations practically expressed in the form of laws, regulations and instructions. Privacy cannot be ensured without security, while security alone cannot guarantee privacy.

Access to data, *authorized as well as unauthorized.* is easier with the aid of computer-assisted databases and large information flows. With unauthorized access, we can understand:accidental disclosure of data, which is likely to occur because of a systemic error in electronic equipment or software, *negligence of an unauthorized user or purposes of data abuse.* Intentional unauthorized access means unlawful use or abuse of data, be it in the field of data creation, processing, storage or transfer [7].

4. Interdisciplinary approach

The introduction of medical informatics into health care with computer-assisted data processing is an unstoppable process inevitably required in medicine respecting two basic premises: - *that it is introduced through modern organizational and technical methods,* - *that it offers support to the medical profession.*

We therefore speak of an interdisciplinary approach of different professional teams, whereby the link between e.g. a doctor and an information scientist is essential.

A fundamental dilemma of incompatibility is presented between a perfect model of legal-formal data security on one hand and *the "doctor's view"* on the other, whereby it is our opinion that in practice it is necessary to have the right amount of diametrical opposition between the security system and the doctor's view of the problem [8]. On the doctors' side, legal restrictions exist at two levels. In basic health care or in the case of a chosen, personal doctor, the work methods are such that most treatment methods and medical and personal data management depend on the personal doctor (one man band). During treatment in specialist and therapeutic units, outpatient clinics and hospitals, consultation between different specialists is also necessary. Hospitalization is a great advantage for a patient in the therapeutic sense, since many specialists at the same time can discuss his disease or injury, and they have the option of reviewing medical documentation on a concrete patient from other wards, while they can only enter data for patients in their ward. Such a model for data security is more complex and

requires accurate definition of users and their right to access data. Data security can in this case be reasonably ensured only if we derive from it the assumption that the patient who came into the hospital for treatment is protected by the hospital as an institution and not by his doctor, naturally with the assumption of preserving all ethical and moral values in the process of treatment. All data on the patient must be available to all doctors included in a concrete process of treatment, whereby each of them has the possibility of reviewing the entire patient's medical documentation and adding new diagnostic or therapeutic findings to it. These requirements lead the doctor to the above dilemma of deviation from the strict legal framework of patient data security. We believe that this exclusive deviation is justifiable (with written approval from individual patients for which treatment is intended), since the patient consciously gives up a part of his own personal freedom and integrity by being admitted into the hospital. In its essence, the hospital comprises elements of "prison" and "military subordination". Computer-assisted medical documentation in addition presents a new element - data collection and management in one place, which has both good aspects (faster availability, better surveyability of data) and bad (more difficult security, more frequent abuse of data).

5. Data storage and distribution

Medical data, information and documents are stored on different media, ranging from classical, collections of which *still comprise 70 - 80%*, to computer-assisted, in which medical informatics in Slovenia is in its initial phase of development.

It is necessary to draw attention to two aspects: (1) The following terms should be distinguished: *data* (as basic attributes), *information* (as a series of data), and *documents:* the latter is the outer material vision/image of a lawful record and (2) *The method of organization of data storage*, storage of information and documents, meaning classical storage methods as well as electronic archives.

Defining the data protection and security procedures during the transition to a new information period requires: - good organizational regulations on data security and protection, derived from legal regulations; - physical protection of premises with limited access; - systemic protection of access to the system and data with the use of special passwords in the case of computer-created data; - a direct connection between the computer system for the archiving of medical documentation and computer data exchange in compliance with the EDI, UN/EDIFACT standard.

At the level of applied software, supervision of the rights of users is covered by providing the possibility of different settings in different environments, such that all authorized persons can obtain the required data on patients quickly and in a simple way. One of the simplest and quickest ways of identifying users and related rights is an identification card which must be physically present at the working station so that the user of the identification number on the card can use the password as a second level of protection. Personal identification cards are in the testing phase in some hospital information systems [9].

With the introduction of the "smart" or "chip" card into the health insurance system in Slovenia (the project - of the PHARE program will be performed by the Institute of Health Insurance in 1996), the replacement of the EMSO (*the thirteen-digit unified registration citizen number)* with an *eight-digit national health care identification number* is proposed [10].

6. Conclusion

While studying the problems of data protection and security, it is quite obvious that all dilemmas and open issues in this field cannot be solved at once; new solutions should constantly be sought and supplemented.

Users both in public institutions as well as in private medical practice should be provided with: - *an appropriate method for archiving documents (classical and electronically kept).* in accordance with the legislation and requirements of the profession, which will be simple and direct access to which will be possible only for authorized users; - *a higher level of protection and security of data in health*

care. in accordance with optimal financial possibilities and with the introduction of new information technologies, including standardized and compatible mechanisms for data protection and security; - *secure communication of users at different levels during electronic data exchange* should be ensured at the national level (coordination of the acquisition, maintenance and distribution of public keys) [11].

The presented framework of data protection and security in health care, as well as the management, processing and exchange of documents, with the introduction of new, modern EDMS (Electronic Document Management System) computer technologies forms a good basis for the superstructure of information systems in health care and their transition into a well-developed information society.

Integration means storage of and connection between electronic documents following the principle of "on-line" access in "real-time", computer generated documents, graphic materials and multimedia documents using standard graphic interfaces for Windows environment in a unified stored and indexed on high-capacity exchangeable optical disks (EOD) with fast access to chosen documents, taking into account the classical organizational archive structure: *"document ⇒ file ⇒ drawer ⇒ archive"* (Fig. 1).

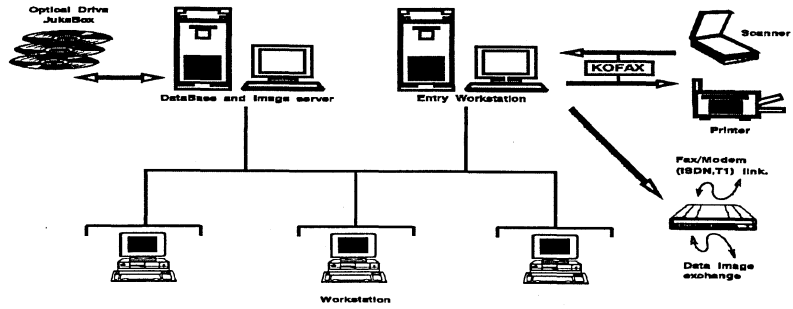

Fig. 1 Electronic Document Management System (EDMS)

In the future, our objective is to incorporate a managerial information system into the Slovenian health care system to provide management staff with the tools for strategic planning and business decision-making, as well as the building of expert systems for individual fields of medicine, supporting of a new computer technology: multimedia, 3D - medical digital image processing with virtual reality.

References

[1,2] Cerkvenik G., Slavec S., Rems M. Problems with Protection and Security of Medical Data. Medical Informatics '95. Proceedings of the 2nd Symposium of Croatian Society for Medical Informatics with International Attendance. Zagreb 1995. Med. Inform. (2); ISSN: 1330-1799; 123-130.

[3] Brus A. Development Policy for Protection of Computer-aided Information System in Health Services. Proceedings of the Congress of Slovene Society for Medical Informatics with International Attendance, MI '92. Bled 1992; UDK 312.6:681.31; 213-225.

[4, 6] Lavrenčič D D. Keeping Confidential Health Records. Inform. Med. Slov., 1994; ISSN: 1318-2129; 1 (1): 49-51.

[5] Katsikas S.K., Gritzalis D.A. A High Level Security Policy (HLSP) for Health Care Establishments. AIM/SEISMED (A2033) Project. Commission of the European Communities, 1993; 1-41.

[7] Vallbone C, Beggs-Baker S. Data protection in community medicine environment. In: Griesser CG (ed). Relization of data protection in health information systems. Amsterdam, 1976: 214.

[8, 9,10,12] Cerkvenik G., Ritonja S., Šašek-Vilhar C., Rems M., Podboj I, Slavec S. Protection and Security of Medical Data. Proceedings of the Eleventh International Symposium on the Creation of Electronic Health Record Systems and Global Congress on Patient Cards of the TEPR '95, Medical Records Institute, Newton - Massachusetts, USA, 1995; 121-133.

[11] Premik M. Sucurity of Medical Data. Proceedings of the Congress of Slovene Society for Medical Informatics with International Attendance, MI '92. Bled 1992, UDK 61:659.21; 191-197.