Patient Education on Safety and Privacy

Tatjana WELZER a,1, Marko HÖLBL a, Marjan DRUŽOVEC a, Aida KAMIŠALIĆ a, Ana HABJANI b

a Faculty of Electrical Engineering and Computer Science, University of Maribor, Slovenia
b Faculty of Health Science, University of Maribor, Slovenia

Abstract. The individual’s right to determine if, when and how data about them will be collected, stored, used and shared with others is called the right to privacy. The problem of data collection and sharing arises daily among health services. Among medical staff, there are numerous message flows, including the medical records of patients and other patient’s personal data. These data are often completely unprotected and available to anyone who knows where it is. Unfortunately, the same data might not be available for patients, despite the fact that each individual has the right to view their own medical record and despite the fact that many other persons connected directly or indirectly to the patient has this access without limitations. In the paper, we will not concentrate on actions that medical staff has to perform nor on the knowledge that they have to have in order to protect a patient’s personal data and enable a patient’s access to their own data, but we will concentrate on the problem of educating patients about their rights and duties with regard to safety and privacy. Our educational suggestions will be given on the basis of corresponding Slovenian legislation and guidelines for medical staff regarding the protection of personal data.

Keywords. safety, privacy, education, health care, personal data, education

1. Introduction

An essential part of everyday work in healthcare and medicine has become the security and protection of data. In order to protect personal data gathered during medical treatment, privacy has been applied to medical records. Privacy ensures that medical records are accessed only by authorized parties. This means that data can be accessed only by those who should have access to them [1]. In addition to reading such data, access to data can also be defined as: viewing, printing, auditing or simply knowing that a particular record exists. Information privacy aims to prevent the illegal or unauthorized intrusion into an individual’s (personal) data in every relevant area [2]. Personal data is data that defines an individual’s property, state, or relationship, regardless of the format in which it is expressed. Personal data is combined into data collections (medical records) that are automatically or manually processed. Data is processed in the sense of collecting, storing, changing, uniting, deleting and transferring. Devices on which data can be written or recorded are defined as devices on which data is stored. The data collection user, or rightful claimant, is a subject who

1 Corresponding Author: Tatjana Welzer, Faculty of Electrical Engineering and Computer Science, University of Maribor, Smetanova ulica 17, 2000 Maribor, Slovenia; E-mail: welzer@uni-mb.si.
is by law or written consent authorized to establish, manage, maintain, supervise and use the data collection (medical record).

The paper is structured as follows: we will introduce Slovenian legislation, and the organizational regulations for personal and sensitive data. Educating patients on safety and privacy will follow.

2. Legislation of Data Protection in Slovenia

The Republic of Slovenia’s data protection legislation is restricted by contemporary legislative acts that tend to simulate real life situations, and mirror legislative acts from the European Union and similar guidelines [3]. Slovenia has a modern personal data protection act. In the public sector, there are other laws and acts regulating the methods and time limits for the storage of documentation, which emerges during the process of administrative procedures and archiving of material. The acts define physical, organizational and technical data protection methods as well as legal documents respective to internal provisions that companies and organizations have to develop for introducing and managing procedures and measures to protect data. The Healthcare Databases Act covers the collecting of medical data that are managed, used and exchanged between legal and natural persons.

Rapid technological progress demands new ways of collecting, storing and processing personal data. Because of this, the need arose to renew the Personal Data Protection Act [3] for the protection of individuals when processing their personal data and to assure the better flow of such data. The Personal Data Protection Act [4] in principle states that personal data protection is intended to prevent illegal and unauthorized interventions of an individual’s private information. In this sense, the protection of personal data is not the protection of data as such, but rather the protection of one individual’s rights, which the data refers to. Personal data can be processed only if so determined by law or if the manager behind the data collection has the written consent of the individual. Legal and natural persons, who carry out a public service or a service restricted by the companies act can, on the basis of this act, process personal data for people who are in a contractual relationship – but only if the personal data is needed for the fulfilment of contractual obligations. For state agencies, local authorities and carriers of public mandates, the regulations are different as they can only process personal data as defined by law. For an individual whose personal data is processed on the basis of their written consent, the consent has to be previously acquired in written form with the intention of data processing, the use and the period of storage.

Data collecting for healthcare services, i.e., the collecting, processing and transferring of data – carried out according to the law by legal and natural persons who provide health services – is covered by the Healthcare Database Act [5]. The assembling, processing and transfer of personal data included in data collection is regulated by the Personal Data Protection Act, if not otherwise defined by this act. The data collection managers are from the Institute for Health Care of Slovenia and other healthcare providers in Slovenia. Data collection managers most often acquire personal data directly from individuals. They have the right to use health insurance numbers from health insurance cards as a linking point for collecting, processing and transferring data as defined by law. The health insurance card infrastructure is also used for data collection, while simultaneously assuring separate access to health insurance
data and health insurance card data. Data transferred between the health insurance card and other central collection agencies defined by this law are the ones needed for assuring health care services. Personal data can also be acquired by a doctor if this is necessary for the preservation of someone’s life. If the personal data refers to race, national or any other origin, political, religious or other belief or sexual orientation, the data collection manager can only acquire the data through an individual’s consent.

3. Organizational Regulations for Personal and Other Sensitive Data

Different corporations and organizations have to define the organizational and technical policies in general catalogues, in which the measures taken to protect and ensure the confidentiality of personal data are described in detail. According to Slovenian legislation [4, 5] itself based on European guidelines, healthcare and medical institutions must also manage a catalogue for data collecting, which describes all the relevant regulations. Additionally, the procedures and measures for protecting personal data are regulated. It is regularly updated and all personnel dealing with personal data must be acquainted with its content.

Such regulations define the circumstances under which the transfer of confidential data with the use of information technology is possible [6]. Moreover, the transfer of physical media with confidential data is defined and the procedure carried out on the receiver’s side. For every transfer of personal and other confidential data, the rightful claimant must apply in written form and the application must be noted. Healthcare employees and other employees must protect any data that they access, and they do not have the right to communicate them to others – with the sole exception of authorized personnel. The medical documentation includes all written data about patients, including their illnesses diseases, as well as familial and other relationships. The first copies are stored in the institution and are protected. The institution has to enable patients’ access to their medical records and a copy of their medical records within the defined time limit. Lawyers accessing a patient’s personal data have to have special authorization from the patient.

But who is making decisions regarding access to data? The medical doctor treating the patient must make a judgment, based on the patient’s state of health, which data can be revealed to the patient without causing harm or deterioration to their health. The patient or legal representative in case of children, patients in coma or persons that could not make a decision on themselves, decides how much information can be given to their relatives and the public about their health state [6]. Healthcare personnel can be released from their obligation to professional secrecy by the patient or by a court, with the exception of cases where it is deemed that secrecy is to the benefit of the patient. After a patient’s death, specific members of the family can be granted access to the diagnosis and epicrisis of the patient via a written claim, except in cases when the deceased has strictly prohibited it. The institution can use the data for statistical purposes, or medical research work, but only in a way that does not enable the identification of a patient [4, 5].

Access to data in the institution and the use of other sources are secured by a user identification and authorization system. For access attempts, a log is maintained, which is managed by an employee of the institution competent in data protection. The time limit for accessing data storage is equal to the time limit for protected records. After the time limit passes, the data has to be archived. When in the institution data access and
records of access to protected data is based on passwords, the user must change their password after three months at the latest. The changed password must not be the same as the old one.

4. Education of Personnel and Patients

Do we have to educate personnel or patients – or both? To educate healthcare and medical personnel, we suggest introducing appropriate training courses and task specific training for healthcare and medical personnel on relevant topics like privacy, data management, regulation and legislation and at last but not least some special IT topics selected by the personnel, as well as establishing educational programs (formal and semi-formal) as a response to information technology’s influence on healthcare and medical systems. Training can be organised either informally or on an internal level by information technology staff or formally by companies, different institutions that are specialised in information privacy (information privacy for medical records) and even through special courses given by adequate faculties and other higher education institutions.

Permanent education can be carried out by formal educational institutions like universities, faculties, and schools with educational programs that are specialised in information technology for healthcare and medical students. Programs can be either undergraduate or postgraduate. According to our experience, the latter provide better results [7] since participating students already have knowledge and experience in healthcare and can therefore cope more easily with the new topic, even though many are surprised (if not shocked) as to why they should study a specialised topic (general security, privacy) that is so far afield from their main topic of study – healthcare or medicine. On the other hand, undergraduate students are generally not handicapped by primary and secondary topics, since they are younger, and therefore often have more information technology background than postgraduate students.

Do we have to educate patients as well? Do we have to educate them when they first become patients or educate the whole population or educate just the interested population? We believe that we have to work on different levels. Education, and/or informing about safety and privacy, has to be available for the whole population, and to all possible patients. Brochures, flyers and other promotional material have to be developed and distributed among the population. Of course, we have to be aware that this material will be either read or studied by only a small percentage of receivers. At any rate, this approach is still important for the informing of the general population (population as whole). Probably this distribution has to be restricted to healthcare centres, hospitals, health insurance offices and similar places. IT can also be used (e-mails, internet pages, forums, blogs, e-learning including e-lectures and tests).

Besides the activities suggested above, we have to take care about the informing and educating of patients (actual patients). This can be done by their personal physician, or nursing staff (more informing as educating). The aforementioned brochures can be used with a short and simple explanation as to why the patients have to take care of not only their illnesses, but also their safety and privacy. On this level, we would still need serious talks and real education. But education can be also organized in the form of informal meetings or seminars given by the health centres, as they occasionally do about nutrition, for example. Education can be also done more generally and not for actual patients and family members but to anyone concerned. It should probably be free
and could be done by the staff of companies and different institutions that have
specialised in this topic. The level of education has to be suited to the visiting
population, which would probably best be grouped according to interest, knowledge
and status (possible patient, actual patient, family and relatives).

Of course, we have to be aware that we will still not have educated the entire
population. The question of efficiency therefore arises. The third group or environment
where we have to organize this education is the hospital. Patients in the hospitals are
probably more aware about the situation and more interested in receiving information
about their own rights and duties. The aforementioned approaches and methods can be
implemented there as well and special forms can be used, like discussions groups for
the same or similar illnesses, self-education guided by the hospital staff (safety and
privacy instructors) and finally courses/talks given by information commissioner.

5. Conclusion

In the paper, we have examined Slovenian legislation for protecting personal medical
data and provided an overview of the knowledge demands on information privacy for
personal data in medical records, which also govern the regulations of our selected
institutions [1, 4–6, 8, 9] which was also presented in the most important points.

The covered topics are very sensitive and comprehensive. For this reason, they
demand continuous work on regulations, recommendations and related reports [6]. It is
important that healthcare and medical personnel are aware of security, privacy and their
own responsibility for it. They also need to be able to give proper and/or adequate
information to patients. Besides receiving spoken information, patients should also get
written material and training (informative meetings, courses, workshops) with the goal
of making them better aware of the importance of informational privacy. Lastly,
patients need to be aware of their own rights, as well as the rights of relatives and/or
legal representatives connected with their medical records. They will be aware if they
are regularly informed, trained and educated.

References

curriculum – An outcome from the Nice project. In Mantas, J (Ed.) Proceedings of HTE 98, 36–45.
May 2005.
health care and nursing program. In Abidi, R., Bath, P., Keselj, V. (Eds.) The Eleventh International
information security in the “Health Care and Nursing” postgraduate program. In Venter, H. (Ed.) IFIP
TC-11 International Information Security Conference – SEC 2007, IFIP International Federation for
Information Processing, 232:479–484.