Masuma H. Mammadova
Institute of Information Technology of ANAS, Baku, Azerbaijan
masuma.huseyn@iit.ab.az

DOI: 10.25045/jpit.v06.i2.02

THE INFORMATION SECURITY OF PERSONAL MEDICAL DATA IN AN ELECTRONIC ENVIRONMENT

This article investigates the problems of personal data security in the electronic medical system. Approaches to information security support of patients' medical data are presented, features of personal medical data are specified, and potential threats to the privacy and safety of the data in medical information systems are identified. The legal basis of personal data security in Azerbaijan is reviewed, and the feasibility of regulating the information security of personal medical data in Azerbaijan is justified.

Keywords: *personal medical data, information security, safety, privacy, unauthorised access, threats.*

Introduction

Computerisation has penetrated almost all spheres of public life, including medicine. New conceptual approaches to the computerisation of medicine, which have included the introduction of electronic health records (EHR) of patients, are part of healthcare modernization. The EHR system expands access to medical records (e.g., a patient's medical history and the results of a recent examination) and encompasses a shift to electronic document management and the integration of each person's medical data in the specialised data processing centres. The development level of information technology, which defines the possibility of implementing personal medical data (PMD) infrastructure, has contributed to the expansion of the following: a) the availability of health services regardless of the time and location of registered medical data; b) the technical possibilities for copying, reusing and disseminating information; c) the access to the means of mass communication. New opportunities have opened up for the development of telemedicine technology, which facilitates remote consultations, examinations and the processing of information in specialised centres, reducing examination times and improving diagnostic accuracy. Behind these positive changes, the integration and prompt processing of PMD have been disrupted by hackers, creating a threat to the rights and legal interests of individuals. Therefore, the information security of personal data in electronic medicine (e-medicine) is quite relevant.

Problems with the privacy and security of medical data have always been important in terms of the development of the information society, and they have become even more pressing. The need to ensure the security of personal data has become an objective reality of our time that is particularly acute in medicine. International practice shows that the vulnerability of the privacy and security of PMD is the key obstacle in the effective development of e-health (e-health). Thus, healthcare organisations, which have access to personal data about individuals, are obliged to ensure the confidentiality and safety of all medical information. Any personal medical information, regardless of its medium should be securely managed by the patients and the providers of professional medical services. Each party with access should be sure that the data has been handled only by the authorised persons. The typical medical information system (MIS), which provides the establishment of a common information space in a medical institution, automates and optimises clinical processes and other aspects of the organisation from workflow to electronic medical history and clinical records, and provides information and intelligent support for the performance of all the services of the medical institution and management's decision making. Being designed to support the performance of the medical institution, MIS differs from other software products primarily in that it stores and processes personal and confidential data. Legally, medical data refers to information that is confidential; access is restricted and regulated by the current legislation of each country. When establishing MIS, a number of measures should be implemented to ensure the safety of both the information and the information system as a whole, otherwise the use of MIS is inappropriate. Any user accessing MIS is fully responsible for ensuring the confidentiality of the information that she or he introduces, uses or disseminates to other users. Consequently, data security and confidentiality are key requirements for a modern MIS because its application in information, communication and computer systems can be problematic [1-4]. Confidentiality of PMD means that medical facilities accessing personal data are obligated to not disclose or disseminate personal data without the patient's approval. Legally, this requirement means that any healthcare worker accessing PMD must store such information and not disseminate it to third parties without the consent of its owner. In the context of e-health, data security refers to the status of the protection of individually identifiable medical information that is transmitted or maintained through electronic media or any other technical means of transmission and communication. Such protection encompasses internal or external threats; and protection of data from leakage, theft, loss, unauthorised termination, modification (falsification), duplication and blockage.

In international practice, the information security of the e-health system shall provide the following: 1) confidentiality (medical confidentiality and protection of personal data), that is, protection from access by unauthorised users; 2) a guarantee of the authenticity and comprehensiveness of the information during an exchange, and the protection of unauthorised modification of the data; 3) availability, which is the access of authorised users to the information, and it is associated with the availability of a fault tolerance mode in MIS when the system is hacked or overloaded with requests [5-7]. The concept of the person-centred approach, which is the foremost in healthcare in the EU, US, Canada and Australia, is based on the principle of "the easier access is to medical information, the better medical care will be". This principle involves the simplification of access to personal medical data of patients to provide qualified medical aid, and yet it presents serious challenges to the regime of information security in these countries, which is provided for by their regulations. According to the EU Data Protection Directive (1995), the EU member states have unified legislation throughout Europe, and today, many hospitals have the right to access personal medical data [8]. Information security support in information systems, including MIS, is established by the International Organisation for Standardization in the ISO 27001 framework, which has been adopted in Azerbaijan as well [9]. Information security is guaranteed at the organisational (administrative and procedural) level through a security policy, wherein objectives have been formulated; at the procedural level through the development and implementation of a guide for staff and through physical protection measures; at the technical (hardware and software) level through the use of approved and certified solutions and a standard set of countermeasures: backups, anti-virus and password protection, firewalls, encryption, etc. To identify the sender (author) of the e-document and to guarantee the absence of information distortion, an electronic signature is used that expires if the e-document is changed. As for data correction, as opposed to viewing, the requirements are even more stringent, and changes to the PMD cannot be made after a certain point. Corrections to a previously created document with an e-signature should be maintained, remaining inaccessible to medical workers when viewing PMD; in this way, an accountability mechanism is implemented, which is referred to as action logging and auditing [5-9]. The Health Insurance Portability and Accountability Act (HIPAA), adopted in 1996, is the US federal law that specifies the rules of confidentiality and the secure exchange of personal health information protecting it from unauthorised use. The law is applied to personal health information that is printed and stored electronically. [10] HIPAA is based on two important ideas of patient care: privacy and confidentiality. Privacy concerns the patient's right to limit who is aware of her/his medical status, and what information should be available; and to be aware of who has access to the data and for what purpose (the transparency principle).

The specific features of personal medical data

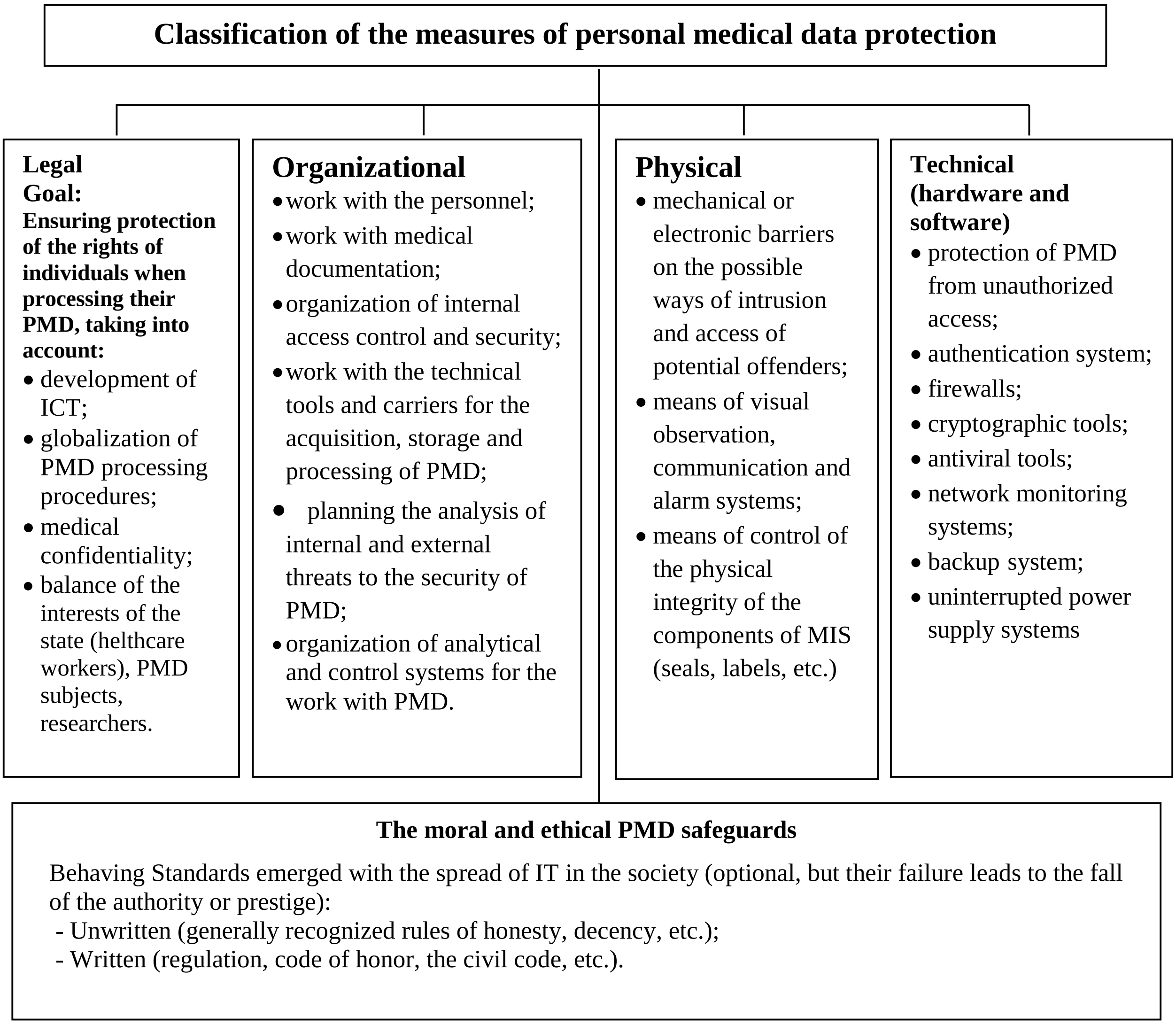
The characteristics of security violations and the personnel who will be processing the patient's information should be considered while developing the security system for PMD and choosing the optimal information security mode for MIS. The analysis of the literature [11-14] reveals the following specifics of a patient's PMD: 1. The personal health information of the patient is private (confidential) information, and the legal owner and a person in charge of the data is the latter, not a medical institution or medical worker. This leads to a particular relationship between the patients as data subjects and the users of their personal information. Thus, it is necessary to protect their privacy, interests and confidentiality, along with the responsibility and interests of healthcare professionals and the legitimate interests of researchers and other third parties. PMD may contain confidential information, the contents of which include not only medical information, but also any other information obtained by the physician as a result of communication with the patient. 2. Time regulations for medical documentation, driven by the need for timely medical aid, are necessary. Delays in data availability for physicians may threaten the patient's health and sometimes even his/her life. Therefore, a reasonable compromise between the three components of information security, that is, confidentiality, integrity and availability of data should be provided. 3. The patient's PMD is sent to various medical institutions, which organises them into: a) personal data, which provides the unique identification of the patient; b) the type of medical data (information on the diagnosis, health status, recommendations and prescriptions, treatment, results of laboratory analyses and statistics; c) storage location (registry, maternity hospital, ultrasound, laboratory, etc.);d) medium (paper, video, electronic files); and e)the authors of individual health information (doctors and hospitals of different fields, nurses and technicians. 4. PMD obtained in geographically dispersed and remote medical institutions is usually not stored in one place. This means that information about the medical services provided in one medical institution is not available in another automatically. Confidential information is only the set of all or most of the distributed pieces of data, and some sections of medical data are not secrets. Therefore, to ensure information security, the management should restrict access while taking into account the multilevel roles, responsibilities, authority and priorities of health professionals, providing them with information in accordance with its purpose [15, 16]. Currently, this approach is used in the MIS of developed countries, ensuring access to certain elements of PMD for users in accordance with their authority.

Potential threats to the privacy and security of personal data in MIS

As shown in [11, 14, 17-19], information security threats may occur when dealing with personal health data. First and foremost are the threats to the privacy and security of information, which can be placed in two categories. The first category is organisational threats that arise from the unauthorised access to patient data by an insider (medical worker) or an outsider (a hacker), and the threats due to the vulnerability of medical information systems. Organisational threats fall into five levels in increasing order of complexity: 1. Unintentional disclosure of personal information: the medical staff may unintentionally disclose the patient's information to others via email, an SMS sent to the wrong address or during data exchange. 2. Curiosity of an insider: medical personnel with the privileges to access a patient's PMD can obtain information about a colleague's illness out of curiosity, or to leak personal data of celebrities to the media, for example. 3. Disclosure of PMD confidentiality by the insider: medical staff with direct access to a patient's PMD consciously steals the information for a profit, and in some cases, to cause moral or material damages to the patient, colleagues or others. The most common leaks occur to provide a list of patients to pharmaceutical companies for a substantial reward. 4. Violation of the integrity of PMD by an external agent through a physical intrusion into the institution where the PMD is stored: a hacker gains access to the information infrastructure of the organisation for data theft or its intentional failure. 5. Unauthorised access to the network infrastructure of MIS: outsiders (former employees, patients, hackers, etc.) gain access to the network system of the organisation from outside to obtain patient data or to make the system inoperable, often for self-assertion. As of today, [20] the greatest threats to information privacy and security are caused by insiders; the attacker can be any member of the medical institution, from a nurse to the manager of the highest rank.

The second category is technical (system and physical) threats that arise due to irregularities in the chain of information flow as a result of unauthorised or accidental access to the database, unauthorised distortion, data destruction, destruction of the hardware, equipment failures, file deletion or damaged data, the unintended consequences of remote backup and unauthorised modification (falsification) of data, etc.

Since the concept of an information system is particular to a situation, healthcare institutions have developed guidelines and documents defining the general and private threats of a typical MIS and appropriate protective measures for processing PMD. International experience shows that the greatest threat to privacy in the infrastructure of e-health records is associated with the reuse of PMD. This concerns cases in which the information to be disclosed for a specific purpose may be used for other purposes as a result of authorisation [14]. Medical organisations generate and store vast amounts of data, and turning big data into the most important practical information is a difficult task. Yet, processing this unstructured information could offer unique knowledge [17]. Thus, PMD plays an important role in clinical, epidemiological, environmental and other scientific studies to develop new treatments for various diseases, to collect and analyse statistics, test the pharmacological effects of new drugs, improve healthcare quality and predict the potential outbreak of various diseases. Nevertheless, the disclosure of health information to researchers raises concerns about privacy violations. The terms defined in legal acts such as HIPAA allow healthcare organisations to disclose medical information to researchers only if they have the patient’s consent, or in exceptional cases, as outlined in HIPAA, and depersonalisation of personal data is required for the use of health information. The regulation of access to health information includes public and private hospitals, insurance companies, administrators, physicians, pharmacies, employers, educational institutions, research institutions, data centres, organisations for accreditation and standardisation, laboratories, pharmaceutical companies and financial agents. Another third party interested in the patient’s information includes relatives, healthcare workers, marketing experts, representatives of various public assistance programs, credit bureaus and law enforcement agencies. In short, many individuals are interested in the acquisition of impersonal PMD. However, with all the good intentions regarding the future use of anonymous PMD, there is a possibility of information abuse. The availability of online public information through social networks and data obtained from pharmaceutical companies and other sources reveals the material conditions and health conditions of the patient. The pharmaceutical companies and insurance agencies may manipulate the acquired information. In addition, there is a theoretical threat of “de-anonymisation” of the e-health record compared to the data from different sources. Sales of medical information have occurred in a separate segment of the black market, and the confidential information trade has a high-yield. Every year, millions of records of the patients’ personal data are leaked from the medical data centres of developed countries, and clinics lose billions of dollars due to this. The larger and more deeply embedded the electronic information system, the greater the leakage of illegitimate content. Statistical data on the US healthcare market shows that the most common source of leaks is theft: data loss occurs in 45.2% of cases, and in most cases, the perpetrators are medical personnel of various ranks who have direct access to the data [21]. In 22.1% of cases, data loss occurs as a result of unauthorised access to the information, in 9.5% it is a result of lost media, in 6.1% cases it is due to a hacker attack, and in 4.0% it is due to the absence of a password on an electronic device. The common violations of the security of PMD are the following: 1) data leakage and theft, that is, breach of confidentiality (a full breach when an attacker accesses the database, or a partial breach when an attacker acquires unauthorised access to the information); 2) data loss due to unauthorised data termination, deletion when accessing the data directly or through the system; PMD loss (information on drug reactions, allergies, previous diseases, the results of laboratory tests, therapies, etc.), which may cause time to be wasted on information recovery, perhaps jeopardising a human life; 3) accidental or intentional distortion or unauthorised modification (falsification) of the data through the system; or direct access to the database, leading to erroneous medical information that in turn causes incorrect medical decision making, endangering human life and health. The violation of the security of PMD may have quite serious moral, physical and material consequences, affecting privacy; personal health and safety; financial and commercial confidentiality; unjustified discrimination by employers and insurance companies; obstacles to political or career growth, and so on. The information security of PMD in e-medicine is provided for by the coordinated and integrated use of an appropriate legal framework, organisational measurements, safety software and hardware devices. The moral and ethical aspects of the disclosure of PMD, legislative responsibility for privacy violations and the damage caused to the citizen should be taken into account [22]. Figure 1 shows the classification of the measures of PMD protection. Although in various regulations of the developed countries (the US, Canada, Australia, and the EU) the responsibilities of data centre operators for the dissemination of personal data are specified, and the penalties of fines are fixed, these measures have not yet prevented leaks of confidential information. There are at least two reasons for the growing number of leaks: the imperfection of medical information systems and the weakness of the legal framework [21, 23, 24].



Classification of the measures of personal medical data protection

Legal
Goal:
Ensuring protection of the rights of individuals when processing their PMD, taking into account:
- development of ICT;
- globalization of PMD processing procedures;
- medical confidentiality;
- balance of the interests of the state (helthcare workers), PMD subjects, researchers.

Organizational
- work with the personnel;
- work with medical documentation;
- organization of internal access control and security;
- work with the technical tools and carriers for the acquisition, storage and processing of PMD;
- planning the analysis of internal and external threats to the security of PMD;
- organization of analytical and control systems for the work with PMD.

Physical
- mechanical or electronic barriers on the possible ways of intrusion and access of potential offenders;
- means of visual observation, communication and alarm systems;
- means of control of the physical integrity of the components of MIS (seals, labels, etc.)

Technical (hardware and software)
- protection of PMD from unauthorized access;
- authentication system;
- firewalls;
- cryptographic tools;
- antiviral tools;
- network monitoring systems;
- backup system;
- uninterrupted power supply systems

The moral and ethical PMD safeguards

Behaving Standards emerged with the spread of IT in the society (optional, but their failure leads to the fall of the authority or prestige):
- Unwritten (generally recognized rules of honesty, decency, etc.);
- Written (regulation, code of honor, the civil code, etc.).

Fig.1. Classification of the measures of protection of personal health information

The legal framework for the protection of personal health information in Azerbaijan

Over the past two decades, the process of informatisation in Azerbaijan has intensified, and the country has made great strides towards the establishment of an information society. Despite this, healthcare remains one of the least informatised sectors of the national economy in terms of the level of digitalisation, and the development of MIS in this area is still at an initial stage [25-27]. Nevertheless, the problems of storage and transmission of medical data, protecting the patient's electronic data in governmental agencies and private medical institutions and ensuring the confidentiality of patients' medical information and the activities of medical institutions are being addressed by the authorities, researchers and developers. Currently, the information security of personal health information in Azerbaijan is regulated mainly by the following political documents:

1. Universal Declaration of Human Rights, the United Nations (UN), 10 December 1948
2. Convention on Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, January 28, 1981
3. Constitution of the Republic of Azerbaijan, August 3, 2003
4. Law of the Republic of Azerbaijan on Personal Data, May 11, 2010
5. Law of the Republic of Azerbaijan on Health Protection, 25 June 1997
6. Law of the Republic of Azerbaijan on Information, Informatization and Protection of Information, 3 April 1998
7. Law of the Republic of Azerbaijan on Electronic Signature and Electronic Document, March 9, 2004

The Article 12 of the Universal Declaration of Human Rights [28] states "No one shall be subjected to arbitrary interference with his privacy, family, home correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Considering the importance and value of information about a person and respecting the rights of the citizens requires the government to mandate that organisations and individuals safeguard the reliable protection of personal data. For example, the Council of Europe adopted the Convention on Protection of Individuals with regard to Automatic Processing of Personal Data [29] in 1981, ratified by the members of the Council and open for adoption by non-member countries. The Convention, ratified in 2009 by the Milli Majlis (Parliament) of Azerbaijan, was enacted in September 2010, obliging the Republic of Azerbaijan to adopt the activities to protect personal data subject to the European legislation. The Law on Personal Data [30] was adopted in May 2010 in Azerbaijan, which regulates the acquisition, processing and protection of personal data; the development of a personal database in the national information medium; and the issues related to the cross-border transfer of personal data, specifying the rights and obligations of existing state agencies and local authorities, individuals and legal entities. Article 32 (Personal Inviolability) of the Constitution of the Republic of Azerbaijan [31] states "Everybody shall have the right to preserve personal and family secrets", and Article 41 (Right to Health Protection) declares that persons of authority shall be made responsible for concealing facts that create danger to a person's life and health.

Protection of confidential information is one of the most pressing problems to be solved in medical institution that are digitalising healthcare systems. The Law of the Republic of Azerbaijan on Information, Informatisation and Protection of Information considers documented information to be confidential, the access to which is limited in accordance with the legislation of the Republic of Azerbaijan and is not transferable to third parties without the consent of its owner [32]. The use of e-signatures in accordance with the Law of the Republic of Azerbaijan on Electronic Signature and Electronic Documents [33] improves the confidentiality of the exchange of health information, and promises the authenticity of the content of electronic documents, which expire when amendments are made. The law of the Republic of Azerbaijan on Personal Data considers personal data as any information that directly or indirectly indicates the identity of a person. This law requires all institutions to fulfil the necessary requirements for the processing and protection of personal data. The Law on Personal Data is also applied to medical institutions of the Republic of Azerbaijan, where general personal data (name, passport number, address, etc.) and special categories of personal data such as information about the health status of patients are processed. Medical data becomes known to the medical institution when providing medical services. However, since health issues and the patients' rights, including the right to medical secrecy, its protection and liability for its disclosure are governed by the law of the Republic of Azerbaijan on the protection of public health [34], as interpreted based on the Law of Personal Data, PMD causes certain misunderstandings and disagreements. In accordance with the law of the Republic of Azerbaijan on the protection of public health, information containing medical data is defined as an "official" secret and "personal data"; that is, any information about the facts, events and circumstances of one's private life and personal or family secrets that could enable identification of the person. In Article 53 of the law on the protection of public health, medical secrecy is: 1) information about healthcare claimed by the citizen; 2) diagnosis of the illness; 3) the health condition; 4) other information obtained during the examination and treatment. The information to be kept secret and the responsibility for its disclosure is legally guaranteed. The same article states that confidential medical information may be transferred to other citizens, researchers interested in information on the examination and treatment of the patient for scientific research and scientific or educational publications only with the consent of the citizen or his/her legal representative. However, in some cases, according to the public interest and requirements specified in Article 53 of the law, the physician is free from the obligation to comply with medical confidentiality. The physician is obliged to report infectious diseases and the risk of their spread, mass poisoning, suspected illegal activities and harming to the health of citizens. In accordance with Article 52 of the Law of the Republic of Azerbaijan on the protection of public health, the physicians who violate the Hippocratic Oath, reflecting the moral and ethical aspects of medical practice for many centuries (since the third century BC), have a legal responsibility.

The new realities that determine the feasibility of the development of the legal framework and conceptual approaches to the protection of PMD

Today, the medical system in CIS member countries, including Azerbaijan, is within the scope of the general legal framework in the field of information security of personal data, and thus institutions must ensure the protection of the rights of citizens when processing their data, including the protection of rights to privacy, personal and family secrets. The experts have focussed on specific sectors in which the development of a separate regulatory framework similar to those in a number of sectors (e.g., banking) seems to be appropriate. The lack of a regulatory framework that governs the protection procedure and security of information in the medical sector in the CIS countries often causes inadequate decision-making. In practice, there are many conflicting situations, the legislative resolution of which is not available today [35-37]. For example, there is a very real threat that an employee of a medical institution who has been fired could access a customer database. However, the current legislation does not specify the protection of PMD from data leaks even with a full set of documents regulating the PMD processing. Furthermore, most personal data of the patients processed in MIS is referred to as a "special category of personal data" (health information, laboratory tests, etc.), but in other cases the category of "biometric personal data" is specified, which enhances the system security requirements [38].

The safe cross-border transfer of patients' personal data can be provided by medical institutions during telemedicine. Personal information should be protected, but some data is required to be disclosed (published). According to the legislation, medical personnel are responsible for confidentiality, but the written consent of the patient is required for the processing of the patients' PMD by non-medical professionals, who are not obliged to keep medical secrets. In addition to the medical staff of an institution, there are workers performing other professional functions. For example, the performance of any MIS relies on administrators (of the system, database applications, etc.), who are not medical professionals, although they have access to the information.

The rapid introduction of the Internet of Things in medicine should also be noted. Today, most people use networked portable devices to monitor health, to control nutrition, to perform exercises and track vital signs. Physicians are able to rapidly and accurately adjust and optimise implantable devices such as pacemakers, often without resorting to invasive procedures [39]. However, along with the advantage of the introduction of network technologies in the medicine, the risks of confidential information about the personality and health of the patient are growing, as medical information is considered especially valuable among hackers. International practice shows that, although legal documents in the field of personal data offer a flexible tool for effective protection from possible security threats, there is a need to develop additional recommendations with document templates and typical threat models for the typical MIS of medical institutions [40-42]. The US, the UK and some other countries have a separate legislative framework governing the issues of information security of personal health information, including medical and health secrets [9, 10, 43]. Thus, there is a need to develop internal regulations and frameworks that can clarify for medical institution employees how to act in terms of informatisation of medicine. Subsequently, a typical threat model must be developed, according to which measures should be taken for the protection of confidential information, and the level of PMD security should be defined. At the same time, when selecting the level of protection for a certain MIS, the following items should be taken into account: 1) type of personal data; 2) number of subjects, the details of which are stored in MIS; 3) status of the medical institutions (e.g., potential threats in a small medical institution may not pose a great danger); 4) the relevance of threats, depending on the vulnerabilities in the system software, applied software. All of these factors constitute a particular way of applying PMD protection. Considering the global experience in the development of specific legal acts regulating the information security of personal health information, the Ministry of Healthcare in Azerbaijan should develop legal and methodological documents regulating MIS implementation in medical institutions, the relationship between personal data and medical information, and the protection and security of medical information. This will enhance the awareness of the managers of medical institutions, medical personnel and other interested parties of the protection of patients' personal information. With the development of e-health, the widespread introduction of computer processing technology of PMD, cross-border exchange of information, and the development of MIS, a comprehensive and innovative approach is required for the development of legal, organisational and technological safeguards to preserve health information, including medical data, from unauthorised access. This requires taking into account the features of the actual situation in the field of PMD. So, first of all, we should take into account the fact that information security of PMD is not one-time process but continuous [44]. It means that an information security system must be constantly updated, taking into account the specific characteristics and dynamics of MIS, the increased technical capabilities of intruders to copy and disseminate information, the efficient solution of the safe data transfer problem, the resources, the typical threat model, and the protection level of PMD in a particular organisation, and so on. Many medical institutions neglect the protection of PMD; the resources allocated for the protection of e-databases of the patients' HER are insufficient or there is a lack of qualified staff members who are competent in the technical protection of information and familiar with the relevant legislation [36]. One of the most effective approaches in this situation may be the development of decision support systems (DSS) to generate recommendations to support the authorised persons in decision making with respect to the information security of PMD in medical institutions through the knowledge of highly qualified experts. DSS ensures the identification and formalisation of decision making in the design process of PMD security systems, including the identification and assessment of potential threats to the information security of each medical institution, and the corresponding measures to protect PMD, eliminate threats and determine the information security level required for its regular functioning [45 -47].

Conclusion

The study leads to the following conclusions: 1. Because of the development of e-health, the widespread introduction of computer technology for PMD processing and cross-border data exchange, the development of health information systems requires an integrated, innovative approach to the development of legal, organisational and technological safeguards to protect health information, including medical data, from unauthorised access. 2. The problem of personal data protection in medical institutions has its own particularities; according to which separate legislation has been developed in countries with advanced e-health systems. This legislation regulates the issues of the information security of personal health information, confidentiality and privacy, access to personal data and responsibility for its use. 3. There are normative and methodological documents that regulate the activities, rights and duties of personnel in the medical institutions of Azerbaijan in terms of e-health, and define the protection and security of medical data and PMD during internal and international data exchange. 4. The development of new conceptual approaches is required to support decision making by the authorised persons to ensure the information security of personal health data in medical institutions.

References

1. Chao H., Twu S., and Hsu C. A Patient-Identity Security Mechanism for Electronic Medical Records During Transit and At Rest, // Medical Informatics and the Internet in Medicine, vol.30, no.3, 2005, pp.227–240.
2. Abdumanonov A.A. Karabayev M.K. Algorithms and technologies of information security in the health information system Externet // Software and Systems, 2013, No. 1. pp. 150–155.
3. Wang J., Zhang Z., Yang X., Zuo L., Kim J. Data Security and Privacy of e-Healthcare in Electronic Medical Environment / Proc. of the 2nd International Conference on Sensor and its Applications, 2013, pp. 92–98.
4. Wilkowska W., Ziefle M. Privacy and data security in e-health: Requirements from the user’s perspective. Aachen University, Communication Science, Germany/ Health Informatics Journal, 2012, vol.18, no.3, pp.191–201.
5. Kobrinsky B.A. Privacy and protection of personal health information in e-health. Federal guide. http://federalbook.ru/files/FSZ/soderghanie/Tom%2015/XI/Kobrinskiy
6. Ameen M. A., Liu J. W. and Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications // Journal of Medical System, 2012, vol.36, no.1, pp.93–101.
7. Baker D.B. Privacy and Security in Public Health: Maintaining the Delicate Balance between Personal Privacy and Population Safety / The 22nd Annual Computer Security Applications Conference, 2006, pp.3–22.
8. European Parliament and Council Directive 95/46/ EC of 24 October 1995 http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm
9. ISO 27001:2013 Information technology. Security techniques. Information Security management systems. Requirements.
10. Choi Y.B., Capitan K.E., Krause J.S., Streeper M.M/ Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules. // Journal of Medical Systems, 2006, vol.30, no.1, pp.57–64.

11. Nazarenko G.I., Mikheyev A.E., Gorbunov P.A., Guliyev Y.I., Focht I.A. Focht O.A. Features of solving information security problems in medical information systems, http://www.interin.ru/datas/documents/pib.pdf.
12. Agrawal R., Johnson C. Securing Electronic Health Records Without Impeding the Flow of Information // International Journal of Medical Informatics, 2007, vol.76, no.5-6, pp.471–479.
13. Gostin, L.O., Hodge, J.G. Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule // Minnesota Law Review, 2002, vol.86, pp.1439–1449.
14. Brands S. Privacy and Security in Electronic Health, www. credentica.com/ehealth.pdf
15. Gallaher M.P., O'Connor A.C., Kropp. B. The Economic Impact of Role-Based Access Control, National Institute of Standards and Technology Report, 2002.
16. Li N., Tripunitara M.V. Security Analysis in Role-Based Access Control. //ACM Transactions on Information and System Security, 2006, vol.9, no.4, pp.391–420.
17. Alyass A., Turcotte M., Meyre D. From big data analysis to personalized medicine for all: challenges and opportunities. BMC Medical Genomics 2015, www.biomedcentral.com/1755-8794/8/33
18. Appari A., Johnson M.E. Information Security and Privacy in Healthcare: Current State of Research. 2008. http://www.ists.dartmouth.edu/library/416.pdf .
19. Mammadova M. Problems of information security of personal data in the electronic medicine. Proceeding of the Second Republic Scientific and Practical Conference on the Multi-disciplinary Problems of Information Security. Baku, 14 May, 2015, pp. 52–55.
20. McAfee Labs. Threats Report – February 2015. www.mcafee.com/ru/security-awareness/articles/mcafee-labs-threats-report-q4-2014.aspx
21. Kanigina O., Zhuravlyova E., Silva-Vega M. Global practice of information leakage http://vademec.ru/magazines/article31896.html
22. Laurinda B. Harman, Cathy A. Flite, Kesa Bond. Electronic Health Records: Privacy, Confidentiality, and Security.// AMA, Journal of Ethics, 2012, vol.14, no.9, pp.712–719. http://journalofethics.ama-assn.org/2012/09/stas1-1209.html
23. Protection of information leakage (DLP-system), www.zecurion.ru/
24. FL-152 in health care: how to "protect" LPU?, www.cnews.ru/reviews
25. Mammadova M.H., Aliyev A.G. The problems of formation and development of e-health system, First Republic scientific-practical conference on the Problems of E-government formation", Baku, December 4, 2014, pp.160-162.
26. Regulations of the Ministry of Health, www.health.gov.az/sehiyye-nazirliyinin-esasnamesi. html
27. E-health. http://e-sehiyye.gov.az
28. Universal Declaration of Human Rights. United Nations, 10 December 1948. www.un.org/ru/documents/decl_conv/declarations/declhr.shtml
29. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.http://conventions.coe.int/Treaty/EN/Reports/Html/108.htm
30. Law of the Republic of Azerbaijan on Personal Data, May 11, 2010 http://www.rabita.az/uploads/qanunverilcik/qanunlar_ru/opersonalnidannix.pdf
31. Constitution of the Republic of Azerbaijan, August 3, 2003 http://ru.president.az/azerbaijan/constitution/
32. Law of the Republic of Azerbaijan on Information, Informatization and Protection of Information, 3 April 1998 www.e-qanun.az
33. Law of the Republic of Azerbaijan on Electronic Signature and Electronic Document, March 9, 2004 www.e-qanun.az
34. Law of the Republic of Azerbaijan on Health Protection, 25 June 1997. www.sehiyye.gov.az

35. The protection of medical confidentiality. What can informatisation of medicine cause? http://www.aif.ru/society/healthcare/1158820
36. Stolbov A. Processing of personal data in medical organizations // Doctor and Information Technology, 2007, No 4, pp. 39-43.
37. Zinovyova O.V. The procedure for the provision of information and the responsibility for their disclosure. www.onegingroup.ru/
38. Imamverdiyev Y.N., Teoh A.B.J., Kim J. Biometric cryptosystem based on discretized fingerprint texture descriptors // Expert Systems with Applications, 2013, vol.40, no.4, pp.1888–1901.
39. Internet of Things in the healthcare. The benefits and risks. www.mcafee.com/ru/resources/reports/rp-healthcare-iot-rewards-risks-summary.pdf
40. Magnusson, R.S. The Changing Legal and Conceptual Shape of Health Care Privacy // Journal of Law, Medicine & Ethics, 2004, vol.32, no.4, pp.680–691.
41. De Vimercati SDC, Foresti S, Livraga G, Samarati P. Protecting privacy in data release / Aldini A., Gorrieri R. (eds) FOSAD VI. Berlin: Springer, 2011, pp.1–34.
42. Magnusson R.S. The Changing Legal and Conceptual Shape of Health Care Privacy// Journal of Law, Medicine & Ethics, 2004, vol.32, no.4, pp.680–691.
43. Hodge J.G., Gostin L.O., Jacobbson P.D. Legal Issues Concerning Health Information: Privacy, Quality, and Liability// Journal of American Medical Association, 1999, vol.282, no.15, pp.1466–1471.
44. Vasilyev V.I., Belkov N.V. Decision support system for the security of personal data // Bulletin USATU 2001, Vol.15, No5 (45) pp.54-65.
45. Korolyova N.A., Tyutyunnik V.M. Expert decision support system to ensure information security. Tambov, publishing house Nobelistika 2006, 198 p.
46. Abbasov A.M., Mammadova M.G. Methods of the organization of knowledge bases of fuzzy relational structure. Baku, Elm, 1997, 256 p.
47. Eta S. Berner. Clinical decision support systems. Theory and practice. Springer Science+Business Media LLC, 2007, 278 p.