Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@lan.ab.az
DOI: 10.25045/jpis.v08.i1.03

PROBLEMS OF INFORMATION SECURITY IN E-HEALTH

E-health promises various perspectives in the field of availability of high-quality medical services and information for the whole society. Moreover, it facilitates several threats in terms of violations of private life and information security. This study sheds some light on main development trends in e-health sector, evaluates main threats to information security from the point of view of potential risks and analyzes viable mechanisms of information security assurance. Scientific-empirical problems of information security ensuring are identified in e-health systems, as well as in wireless body sensor networks.

Keywords: *e-health, m-health, personal medical information, information security, privacy, WSBN.*

Introduction

Human health is an important social value, and it is possible to judge the level of development and welfare of any country according to the health status of its population. The maintenance of public health at high level is a significant socio-political problem, and its addressing requires uniting the efforts of the whole society. The healthcare system provides the production and quality of labor resources generating a basis for socio-economic prosperity of any country.

Modern information and communication technologies (ICT) create principally new opportunities for innovations in healthcare. Electronic health (e-health) encompasses the tools facilitating the disease prevention, diagnostics, monitoring and healthcare management by employing ICT ("telemedicine" termin has been extensively used till mid 90's) [1]. E-health – contributes to the wellbeing of the society by improving the accessibility and quality of healthcare services and making healthcare sector more effective.

E-health was discussed in Geneva Summit on information society in 2003 and adopted by WHO (World Health Organization) with corresponding decree on e-health in 2003. Since that period, countries have commenced to shape and implement national strategies on e-health development [2].

The formation and development of e-health are accompanied by several political (strategic), legislative (standardization), social, economic, technological and etc. problems [3]. One of the important problems in this field is the provision of information security [4]. Medical institutions process significant volume of confidential information; this information entails individual information of patients and medical staff, as well as treatment privacy. This, in turn, requires the provision of information security of medical information systems at high quality, while the violation of information security in such systems may pose threats for human life directly [4-7].

The aim of this paper is to analyze the current state of scientific-practical research on information security and confidentiality of personal data within the e-health environment and determine topical research directions.

E-health: main trends

The countries have passed some stages in e-health development as reflected in WHO reports [8]. Some works are being carried out towards the establishment of corresponding legislative framework in several countries, the architecture of e-health is determined, several components of infrastructure are established and various medical information systems and services are put into service. In order to identify information security problems in e-health, it is necessary to analyze main ongoing tendencies in current stage of e-health. For this purpose, a brief analysis of tendencies is given below.

Digitalization of medical information. E-health aims to achieve the maximum availability of medical aid for citizens and considers facilitating the provision of all required information and consultation regardless the location of doctor and patient. It is no coincidence that the main concept of e-health is the electronic health record system [9]. Firstly, hardcopy of information is digitalized and compiled in information system consisting of distributed data bases. Electronic health record comprises personal, medical (disease history, examination, treatment, currently used medication, blood type, vaccinations, etc.) and insurance information, and enables the card holder to receive high-quality, effective and quick medical service.

It is to be noted that English-speaking sources mostly use *"*Electronic Health Record (EHR)", *"*Electronic Medical Record (EMR)" and "Electronic Case Record (ECR)" [10]. [11] discusses the issues of terminology on electronic medical cards in Russian. Several countries have adopted legislations facilitating the establishment and use of EHR systems. The building of EHR system satisfying specific requirements is required at the first stage of healthcare informatization in the USA. In 2014, 14,6 billion US dollars were spent to induce doctors for EHR application; currently, some fines are provided for postponement in application.

"Health Insurance Portability and Accountability Act" (HIPAA) adopted in USA in 1996 envisages that patients preserve the right to access their information and monitor the methods of its use [12]. Such legislative acts generate a need for *personal health records* (PHR) alongside with growing interest of patients for using the Internet in order to find information on their diseases and treatment methods of those; these records are based on applicative web programs and enables people to access their medical information, control them and present to others.

Another advantage of EHR systems is related to the transmission of information on patients and electronic prescriptions among organizations, including trans-border transfer [13], the most known project in this sphere was epSOS Europe project completed in 2014 (http://www.epsos.eu/).

Mobile health (m-health). Mobile phones become a new tool for providing healthcare services via audio, as well as video and multimedia data [14]. Mobile health (mHealth) – envisages the application of mobile devices for addressing healthcare problems and possesses some advantages (mobile are phones are a sole means of communication in some locations, in some cases, there is no need for sending doctor staff, and it enables the maximal use of telecommunication technologies for the communication between a doctor and a patient).

M-health is at the early stage of development and has not fulfilled its potential extensively. Japan is the leader in m-health and 6% of world turnover is accrued to this country. In global report of WHO on e-health, it is mentioned that, the dominating form of m-health is characterized with small-scale experimental projects which considers some issues of common use of information and access to information [15].

Personalized medicine. The development of computation technologies and study of genome data pledges large innovations in personalized medicine. National Institute of Oncology in the USA defines the personalized medicine as "a tool which uses information on genes, proteins and the environment surrounding human for the prevention and diagnostics of medical diseases". Personalized medicine generates wide opportunities for early diagnostics of medical diseases, highly personalized treatment tools and foreseeing and preventing adverse side effects of medications [16].

Social network services and 2.0 healthcare technologies. Social network services (Web 2.0 technologies) – technologies considered for interactive communication and user-created content also penetrate the healthcare sector. One of the emerging technologies is related to the control in online regime to the date on the health status of patients and the health statues of old parents or children. Another trend is the application of online reputation systems for the rating of medical services [17].

Patients turn to websites and social network services for medical information. Most of such social network pages propel positive behavior in healthcare. In some cases, web pages enable

patients to ask questions and obtain answers on diagnoses and treatment. It raises some concerns regarding the wide incidence of inaccurate and non-professional online medical recommendations.

While using social network pages for remote clinical treatment, the main concern is related to the issues regarding the legal responsibility for providing medical aid, technical and social issues necessary for protecting the confidentiality of treatment, and providing the adequate security and reliability of the information transmitted via the Internet with social network services [16, 17].

Cloud computing in e-health. EHR systems provide the exchange of information among various medical organizations by not violating the privacy of personal data and supporting corresponding security. Cloud platforms are the most feasible option for building such systems which provide substantial scaling and flexibility as requirements change; [18] suggests Fusion platform for this purpose. Fusion is an open experimental cloud platform for the common use of medical information at large scale and management of information security. The aim of this platform is to reduce the costs spent on EHR implementation. Moreover, Fusion creates new opportunities for establishing new services which use medical information.

E-health and Big Data. E-health systems are accompanied by Big Data: it includes genome data, diagnostics descriptions, test results, research samples, insurance and financial information and large number of different type of information. Big data generates big opportunities for the aggregation and intellectual analysis of medical data [19].

Standardization in the field of E-health. The future of e-health is determined by the interoperability of medical data systems in some sense. However, e-health is one of the most complex and problematic sectors of standardization, which entails some specific complexities [17]. One of the main complexities is that it must be surrounded by not one, but several fields of technology. Standardization is required at content level – medical data, diagnostics descriptions and medical research. Another field of standardization must cover wide variety of medical devices, software systems and database management systems. One more field of standardization includes e-health infrastructure and telecommunication systems, information security and the exchange of medical data. Semantic operability must be provided by medical inquiry books and terminology standards (ICD, LOINC, SNOMED CT).

Another feature complicating the situation in the field of standardization in e-health sector is the abundance of organizations engaged in standardization activity, coordination of their activities and the provision of interoperability between standards. It is to be noted that various organizations, such as ISO/TC 215, CEN/TC251, ITU-T, IEEE 11073, HL7, epSOS, DICOM, GS1 Healthcare, Continua Health Alliance, are engaged in standardization in e-health sector.

Information security threats in e-health

Malicious software. One of the side effects of e-health is that malicious software can infect critical medical systems and devices. The Ministry of Veteran Affairs of USA reported in 2013 that, at least 327 devices in ministry hospitals were infected by virus since 2009. More than 40 virus sorts have infected equipment manufactured by companies such as General Electric Co., Philips N.V., and Siemens AG, including X-ray equipment and laboratory equipment.

In one case, computer equipment required for opening procedures of clogged arteries after heart attack was infected with virus and it was necessary to close down the laboratory for a while. In another case, virus was sending confidential patient data from one device to remote server. The cases of infection of medical equipment with malicious software are numerous and extensive information can be found in [20].

Loss of medical identification data. One of the threats is the theft of medical identity data. According to investigations of Ponemon, medical identity data of 1.98 million Americans were stolen in 2013. In this case, 36% of them were incapable to pay the bills presented to them. Some of them were forced to pay the full price for medication and medical services while their insurance

expired. Others had to pay for medical services received by thieves. The average volume of an account was 18.660 dollars.

According to 2014 Healthcare Breach Report, 68% of all healthcare data was due to the loss or theft of equipment since 2010 [21]. Medical identity data of approximately 2 million Americans were stolen in 2014. However, this figure has reached 112 million due to hacker attacks to medical databases in 2015 (medical identity data of every third American was stolen). The largest loss of data was reported by Anthem insurance company in February 2015; hackers have stolen personally identifiable data of 78,8 million people by hacking into servers. Anthem announced that medical data and financial data were not stolen. It is to be mentioned that, stolen data were not encrypted, which is not required by law [22].

However, this is not the worst case. If anyone has an access to your medical identifier and uses it for receiving medical services and prescriptions, all corresponding information will be recorded in your personal health record. Your information will be mixed with the information of swindlers. First, all recorded information will be false. The incident occurred in Anthem system included 80 million patients and such events were often observed. According to the information of Anthem Company, stolen data included the name of patient, date of birth, membership identifiers and number of social insurance card, phone numbers, e-mail address and job place. This information can be partially used for swindler accounts as well.

Medical identity data are regarded as more valuable in comparison with credit card or social insurance cards. According to World Privacy Forum information, the value of such information in black market is 50 dollars, whereas the price of credit card or social insurance card is approximately 1 dollar [23]. The average profit from one medical record is 20 thousand dollars, while this figure is valued as 2 thousand dollars due to the theft of regular identification data.

According to the information of Ponemon Institute, one of the main reasons of growing number of cybercrime in healthcare sector is that it takes more time to detect fraud here; it is more complex to fix the situation [24]. It is possible to close bank accounts and obtain new credit card, whereas it is more complex to correct electronic medical information.

Cyber attacks on medical equipment. Most of medical equipment uses widespread operating systems; hence, those are also vulnerable to attacks like regular computers. However, equipment with special operating systems can also be exposed to cyber attacks, the mechanism of updating software tools are used in most cases [25,26].

Wireless technologies expose medical equipment to cyber attacks. The Ministry of National Security of United States published recommendations on the use of modern medical equipment in 2012 [27]. In brochure, the experts of the ministry admit that, new technologies facilitate to improve the results of work, reduce costs and improve the quality of services provided to patients; however, some risks emerge from the point of view of security, for which the healthcare sector may not be ready. In the ministry's report, it is indicated that the communication security in medical equipment creates serious concerns; hence, it is necessary to adopt additional security measures for protecting against malicious interventions and the theft of medical data.

In 2011, one of the researchers demonstrated the possibility of unauthorized connection to insulin pump and changing the parameters of user without his/her awareness in Black Hat conference. That researcher has demonstrated how the data transmitted by sensor showing the level of glucose in blood can be obtained with the help of oscillograph.

In 2009, one of the researchers of Massachusetts Institute of Technology (Amherst) demonstrated the possibility of unauthorized connection to implant device – defibrillator; defibrillator – stabilizes the functioning of the heart with the help of electrical impulses. He has re-programmed the device so that, the current would strike the heart. Moreover, the researcher was able to shut down the energy saving mode of defibrillator, as a result of which the battery can be exhausted in several hours instead of several years on regular work regime.

Approximately 25% of hospitals do not carry out the annual check of the security of patient data. This was stated by the opinion poll carried out by the medical data and management systems society specialized in information security in healthcare in 2011 by showing that the hospitals spend less than 3% of their IT budgets on information security.

It is mentioned in the report that the hospitals can be called to account for the loss of patient information. For example, USB carrier can locate the patient medical record of around 25 thousand patients. The loss of such carrier may cost 6 million dollars for a hospital; this includes fines, legal expenditure, costs on notifying the patients and costs spent for the monitoring of personal data of victims.

Other threats. In the United States, the design, manufacturing and the regulation of sale of medical equipment is regulated by the Food and Drug Administration, however, this institution is yet to develop the documents regulating the connection of medical equipment to communication devices. Hence, the employees of medical institutions are solely responsible for protecting the devices with the access to patient medical data from hackers.

Although security tools are usually considered in medical equipment, those are not always used due to their complexity and unawareness. While the majority of technologies used in e-health are new, users may not be familiar with the tools of providing security in these technologies and as a result, malicious persons may abuse these mistakes.

The absence of accurately developed security software may adversely affect the protection opportunities of medical information of organization's patients against the theft, loss or damage.

If the budget designated for information security is small, the problem can be aggravated: funds can be spent not on the security provision of enterprise priority, but on other issues. Despite such problems, the security should not better if it was present standpoint.

Information security systems in e-health

Personal medical data belongs to the category of confidential information, the acquiring, processing and use of such information is limited with the purposes of its compilation. E-health information systems provide the storage, access and use of personal medical data only for the purpose of providing medical aid and during the period of provision of medical aid.

Protection of personal medical data is carried out with the implementation of the set of legal, organizational and technical tools and targets the following goals:

- inviolability of personal life, realization of rights to personal and family secret;
- provision of the integrity and confidentiality of personal medical data;
- realization of the right to the access to personal data;
- prevention of unlawful compilation and processing of data.

It is recommended to place network displays in the borders of networks, use network monitoring and intervention detection systems and locate devices to separate segments of network when possible. It is also recommended to apply strict control policy, coding and authentication at both ends of communication channels.

Access control. It is recommended to use role based access control in e-health systems (RBAC) [28, 29]. Only persons appropriately authorized by the governing body of medical enterprises are allowed to access e-health systems within the functions carried out (roles). For example, a member of a medical staff has the right to access the disease history of patient within his/her competence only. Registering nurse can view and change the passport data of patient, and the time of doctor appointment and analysis appointment during registration only within his/her competence.

Authentication and authorization. In order to control the access of remote users to resources of terminal servers, the machine-software operating in terminal regime can be used. For example, in accordance with the methodical recommendation on the provision of medical enterprises of the Ministry of Healthcare of the Russian Federation with computer equipment and

software. It is recommended to apply a special device – thin client which is different from personal computers. Recommended thin client employs special local operating system, the sole task of which is to organize the session in local server for the user work.

Local authorization of users in thin client is carried out after personal identifiers are presented and PIN-code is entered. If PIN-code is entered correctly, the operating system of thin client is loading. During the secure loading of operating system of thin client, the integrity of the image of operating system is being checked.

E-signature. All changes and amendments to personal data on health are approved by advanced electronic signature of nurse. The specific devices-software exists which operates in web-entry regime in thin client base for creating and checking e-signature. It is possible to view and sign documents with the help of special browser.

Audit. In order to provide the audit of changes and amendments to personal medical data, the description of changes and amendments made, the time and date of changes and amendments, the identification of the member of medical staff who has done it, viewed, copied or printed are automatically registered in a special log file. Audit enables to detect unauthorized access cases when it is not possible to prevent the access to personal data and there are doubts regarding unauthorized access.

Reserve copying. Reserve copies of personal medical data must be regularly created and protected.

Certification. Software, as well as machine-software tools on information security used in e-health solutions must be appropriately certified in accordance with legislation.

De-identification of personal data (depersonalization). During the conduction of statistical, social and scientific research in healthcare, it is necessary to use depersonalized data by using personal data [30]. Depersonalized data must also be used while employing statistical and analytical systems and obtaining various reports.

Several methods, such as anonymization, pseudonymization, encryption, key-coding and etc., can be used for depersonalization of personal data. HIPAA ***safe harbor method***: it is required to delete 18 specific identificators of a person or his/her relatives, family members or employers:

- names, addresses, dates, telephone numbers, fax numbers,
- medical insurance numbers, social insurance numbers, medical documentation numbers, electronic mail addresses, account numbers,
- license/certificate numbers, car identifiers and serial numbers, device identifiers and serial numbers;
- URL (universal resource locator), IP addresses, biometric identifiers, full face photos and another unique identification number, characteristics or code.

Depersonalized information is stored in one segment of information security, whereas data allowing identifying the owner of this data are stored in another segment during the method of depersonalization suggested by Microsoft Corporation. Such separate information is only comprised when patient data is directly about user, for example, during doctor appointment. After patient leaves, the data is "disaggregated" again which enables to provide the security of them.

Information security in wireless body sensor network

Doctors of first aid, medical nurses and paraprofessionals use wireless medical devices for the diagnosis, treatment and monitoring the patient status. These devices can be portable in the pocket, mobile or implant (for example, cardio monitor).

Wireless body sensor network (WBSN) is a set of physiological sensors connected to transceiver or a small connected computer (for example, mobile phone) via wireless network for the purpose of monitoring of patient health status. The architecture of WBSN can be shown as 3-layered network as seen in figure 1 [31].

Each sensor node is constituted of a microcomputer (computation component), transceiver (communication component), energy source (usually, battery) and specific sensors depending on the field of implementation. Some smart-sensors also include actuator – electromechanical device in order to manage various system components. Sensors measure some activities, collect information and send the information to special station named sink node. Such biomedical sensors send the measured data to coordinator located near body, and the coordinator carries out data processing and aggregation. Sink node, in turn, sends the information to medical facilities or other designated locations via Internet.

The sink node can also play a role of a gateway between the internal network and external network. It is possible to monitor the traffic by applying security mechanisms such as authentication, network display, etc. in administration device.

The security infrastructure of WBSN is different from other types of network according to its specific characteristics [32]. Energy, computation and communication opportunities of sensor networks are limited; these networks are in close mutual contact with physical environment and people; this situation increases the possibility of physical attack and causes new security challenges.

Malicious cyber attacks to WBSN can change the designated address of packages and disturb the routing, steal medical data by illegal listening to wireless communication environment, detect the location of patient and track his activities, make changes to data, create fake emergence signals in medical data, can carry out DoS-attacks (Denial of Service), interventions to physical devices and "jamming" attacks, side channel attacks, exhausting energy source – the battery, analogous sensor injection, and other attacks [32,33].

In IEEE 802.15.6, three levels of security are determined for WBSN: level 0, level 1, and level 2. Level 0 (Unprotected) – is used for unprotected communications. Packages are transmitted without encryption, and information integrity, protection from repeated attacks, authentication and etc. are absent. Level 1 (Authentication) – data are transmitted in authenticated manner, however, data is not encrypted and its integrity is not checked. Level 2 (encryption and authentication) – security is provided at the highest level, and integrity, authentication, verification and etc. measures are carried out. Levels are chosen based on requirements of the field of implementation [34].

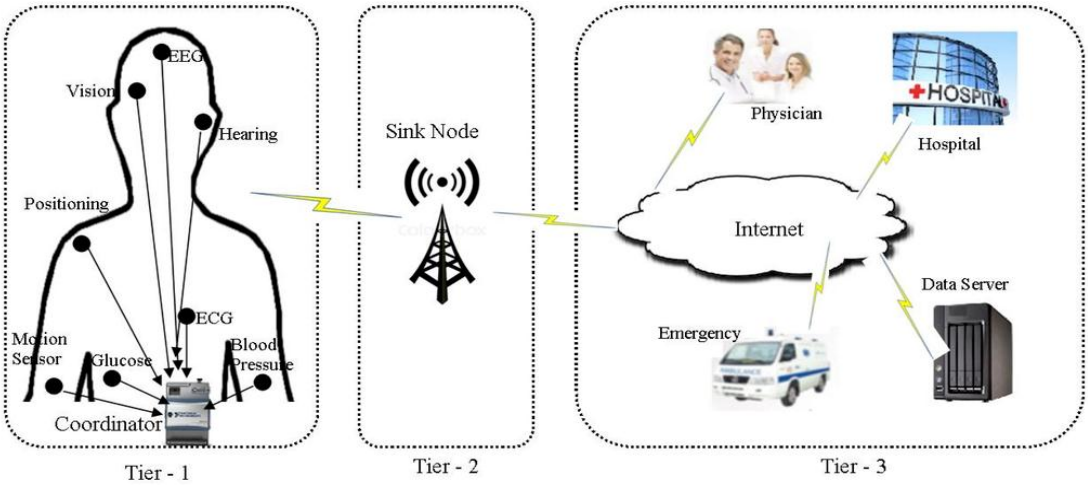

Figure 1. WBSN architecture [31]

Information security management standard in e-health

ISO 27799 [35] is a standard specifically adapted for healthcare and defines the guiding principles for supporting the interpretation and implementation of ISO/IEC 27002 standard in healthcare sector. This standard is directed towards requirements of information security management. The implementation of these guiding principles enables health organizations to

reduce the number and mitigate the impact of dangerous incidents and provide the base level of confidentiality, integrity and availability of personal medical data.

The standard provides clear, accurate and healthcare-specific recommendations on choosing and implementing the security measures for the protection of healthcare information and can be adapted to wide-range scales, locations and models of provision of services largely encountered in healthcare. ISO 27799 standard considers 11 security fields which cover 39 main security categories overall. Each category presents the description of one of several security measures.

ISO 27799 standard reviews various security sectors such as: 1) information security policy, 2) information security organization, 3) asset management, 4) human resources security, 5) physical and environmental security, 6) communications and operations management, 7) access control, 8) purchase, development and exploitation of information systems, 9) management of information security incidents, 10) information security aspects in management of uninterruptedness of activities and 11) compliance with requirements.

Problems of information security in e-health

ICT-based technologies help to reduce the burden of healthcare systems and improve the quality of healthcare services. These technologies include biosensors, computer-based diagnosis, wireless body sensor network, mobile medicine, radiofrequency identification (RFID), cloud computing, communication protocols, electronic medical information, Big data, Internet of Things, etc. As a result, the complexity of healthcare systems has dramatically increased in recent years. However, it is unacceptable to allow for mistakes in the integration of these technologies into healthcare systems, since it may cost a human life. Moreover, as errors occur in such systems, the update and restoration of systems takes substantial efforts and time. As a result, e-healthcare systems must be rigorously tested before implementation.

Although several approaches have been developed for testing and verification of healthcare systems, medical incidents related to ICT occur frequently, which lead to several losses. Hence, it is important to carry out scientific-empirical research in below-mentioned directions for adequate testing and verification of medical information systems and medical devices:

- methods of testing and verification of e-healthcare systems;
- methods of verification of e-healthcare software and equipment;
- methods of evaluation of the reliability of medical sensors, m-medicine and WBSN;
- evaluation of robustness of e-healthcare systems against denials;
- methods of evaluation of reliability of HER systems and personal medical data.

Several problems are present regarding the implementation of m-medicine: communication security in wireless communication network between a patient and medical service provider, provision of sufficient reliability of distant medical control functions, accuracy provision of medical data received with wireless network devices, etc.

In order to provide the data security in e-healthcare systems, information security can be appropriately provided in a whole communication infrastructure. Therefore, it is important to conduct scientific-empirical research in the following directions:

- evaluation of information security loopholes in e-health systems;
- methods of evaluation of information security risks in e-health systems and medical devices;
- methods of access control in e-health systems;
- secure network architecture in e-health systems;
- methods of secure transmission of personal medical information, e-mail and storage;
- methods of detection of interventions and fraud in e-health systems;
- methods of forensic investigation on security of e-health systems.

Development of Privacy Preserving Data Mining methods. Data anonymization for analytics in e-health sector is not sufficient for protecting the user privacy. Hence, it is important to develop

appropriate approaches, methods and technologies in order to prevent the cases of privacy violation during personal data mining. Unlike widely used data mining and machine learning methods, PPDM requires the modification of entry data. The modification of input data aims to prevent the disclosure of sensitive information in personal data and violation of individual privacy. PPDM methods encountered in literature can be grouped in two directions: randomization methods and cryptographic methods [36].

The majority of PPDM algorithms are suggested only at theoretical level, and only a small share of those are implemented for real practical situations or tested by employing real data. This makes the unambiguous evaluation of security level to be provided to their users more complicated.

Conclusion

Electronic health promises various perspectives in the field of availability of high-quality medical services and medical information to the whole society. Moreover, the wide application of information and communication technologies in compilation, storage, processing and exchange of medical data generates several threats in terms of immunity of personal life and information security. The adoption of adequate measures against these threats and development of necessary mechanisms must become an important component of any incentive in the electronic health.

References

1. Della Mea V. What is e-Health (2): The death of telemedicine? // Journal of Medical Internet Research, vol. 3, no.2, 2001 :e22. doi:10.2196/jmir.3.2.e22.
2. Building Foundations for eHealth - Progress of Member States. World Health Organization, 2006. 339 p.
3. George C., Whitehouse D., Duquenoy P. (eds.) eHealth: Legal, Ethical and Governance Challenges. Springer, 2013. 396 p.
4. Mamedova M.G. Information security of personal medical data in electronic envrionment // Information technologies problems, 2015, №2, pp.16–30.
5. Sabnis S. , Charles D. Opportunities and challenges: Security in eHealth // Bell Labs Technical Journal, 2012, vol. 17, no. 3, pp. 105–111.
6. Agbele K.K., Nyongesa H.O, & Adesina A.O. ICT and information security perspectives in e-health systems // Journal of Mobile Communication, 2010, vol. 4, no. 1, pp. 17–22.
7. Mohammad Y.M. Information security strategy in telemedicine and e-health systems: A case study of England's shared electronic health record system. PhD. Brunel University, 2010, http://www.bura.brunel.ac.uk/handle/2438/4669
8. Atlas of eHealth country profiles. WHO Global Observatory for eHealth. World Health Organization 2016, 392 p.
9. Fridsma D. Electronic Health Records: The HHS Perspective // IEEE Computer, 2012, vol. 45, no.11, pp.24–26.
10. Fernández-Alemán J.L., Secor I.C., Lozoya P.Á.O., Toval A. Security and privacy in electronic health records: A systematic literature review // Journal of Biomedical Informatics, 2013, vol. 46, pp. 541–562.
11. Zingerman B.V. Shklovsky-Kordi N.E. Electronic medical record and principles of its organization // Physicin and information technologies, 2013, №2, pp.37-58
12. Atchinson B.K., Fox D.M. The politics of the Health Insurance Portability And Accountability Act // Health Affairs, 1997, vol. 16, no. 3, pp. 46–150.
13. Azarm-Daigle M., Kuziemsky C., Peyton L. A review of cross organizational healthcare data sharing // Procedia Computer Science, 2015, vol. 63, pp. 425-432.
14. Lin S.-P. Determinants of adoption of mobile healthcare service // International Journal of Mobile Communications, 2011, vol. 9, no. 3, pp. 298–315.

15. mHealth: New horizons for health through mobile technologies. Global Observatory for eHealth series - Volume 3. World Health Organization. 2011. 112 p.
16. ITU-T Technology Watch Report: Standards and eHealth. January 2011, 20 p. http://itu.int/en/ITU-T/techwatch/Pages/ehealth-standards.aspx.
17. ITU-T Technology Watch Report: E-health Standards and Interoperability. April 2012, 24 p. http://www.itu.int/oth/T0B15000013/
18. Basu S., Karp A., Li J., Pruyne J., Rolia J., Singhal S., Suermondt J., Swaminathan R. Fusion: Managing healthcare records at cloud scale // IEEE Computer Society, 2012, vol. 45, no. 11, pp. 42–49.
19. Alguliyev R., Imamverdiyev Y. Big Data: Big Promises for Information Security // 8th IEEE International Conference on Application of Information and Communication Technologies (AICT), 2014, pp. 1–4.
20. C. Weaver "Patients put at risk by computer viruses," Wall Street Journal, 13 June, 2013, http://www.wsj.com/articles/SB10001424127887324188604578543162744943762
21. The 2014 Bitglass Healthcare Breach Report. http://www.bitglass.com/company/news/press_releases/healthcare-data-breach-report
22. Munro D. Data breaches in healthcare totaled over 112 millionr in 2015. 31 December, 2015.
23. Camp L.J., Johnson M.E., The Economics of Financial and Medical Identity Theft. 2012. Springer. – 180 p.
24. Fifth Annual Study on Medical Identity Theft. Ponemon Institute, February 2015, 38 p.
25. TrapX Security: Anatomy of an attack MEDJACK (Medical Device Hijack). May 2015.
26. Storm D. MEDJACK: hackers hijacking medical devices-to create backdoors in hospital networks // Computerworld, June 8, 2015, http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html
27. National Cybersecurity and Communications Integration Center. Attack Surface: Healthcare and Public Health Sector. 2012, 10 p.
28. ISO/TS 22600-1 Health informatics – Privilege management and access control – Part 1: Overview and policy management. ISO 2006. 27 p.
29. ISO/TS 22600-2 Health informatics – Privilege management and access control – Part 2: Formal models. ISO 2006. 26 p.
30. Eze B., Peyton L. Systematic literature review on the anonymization of high dimensional streaming datasets for health data sharing // Procedia Computer Science, vol. 63, pp. 348–355, 2015.
31. Bangash J.I., Abdullah A.H., Anisi M.H., Khan A.W. A survey of routing protocols in wireless body sensor networks // Sensors, 2014, vol. 14, no. 1, pp. 1322–1357.
32. Ameen M., Liu J., Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications // Journal of Medical Systems, 2012, vol. 36, no. 1, pp. 93–101.
33. Rushanan M., Kune D.F., Swanson C.M., Rubin A.D. Sok: Security and privacy in implantable medical devices and body area networks / Proc. 35th Annual IEEE Symp. on Security and Privacy, 2014, pp. 524–539.
34. Kwak K.S., Ullah S., Ullah N. An overview of IEEE 802.15.6 standard / Proc. of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010, pp. 1–6.
35. International Organization for Standardization (ISO). ISO 27799-2008 Health informatics – Information security management in health using ISO/IEC 27002, 2008.
36. Aggarwal C.C., Yu P.S. Privacy-preserving data mining: models and algorithms. New York: Springer, 2008, 514 p.