BHL
Bioethics and Health Law Journal
journal homepage: www.journals.sbmu.ac.ir/bhl

Review Article

Patient's Electronic Environment Information Rights

Mahtab Karami (PhD)[1*]

[1] Department of Health Technology Assessment, School of Public Health, Shahid Sadoughi University of Medical Sciences, Yazd, Iran.

ARTICLE INFORMATION

Article history:
Received: 19 November 2020
Revised: 06 January 2021
Accepted: 22 March 2021
Available online: 04 May 2021

Keywords:
Security
Patient's Information Rights
Electronic Environment

*** Correspondence**
Mahtab Karami (PhD)
Tel: *+98 31 55548883*
Fax: *+98 31 55548883*
E-mail: *m.karami@ssu.ac.ir*
ORCID ID: 0000-0003-2335-6627

ABSTRACT

Background and Aim: Electronic health record is one of the most important achievements of the eHealth to achieve patient-centered care. The aim of patient-centered care is the accessibility of all patient information to clinicians to have the best decisions for the patients. Creating an environment for sharing information and developing e-health information caused the security and privacy of health information of patients to become an important and challenging issue. In this regard, healthcare organizations must create a security solution to protect the rights of their patients.

Materials and Methods: This review is based on library research and Internet searches in the major databases such as Web of science, Emerald, Proquest, EBSCO host research, PubMed, and search engines like Google and Google Scholar. In this review, essays, books in the field of medical informatics, and the security of information systems in the health system have been studied.

Ethical Considerations: Publication of the results is carried out without bias, honestly, and by citing the original reliable resources and references.

Findings In this review, how to maintain information security programs and health information systems in addition to improving quality of care to achieve three main objectives related to security, including confidentiality, accuracy, and the availability around three core axes of administrative safeguards, physical safeguards, and technical safeguards are discussed.

Conclusion: The health centers should be consistent in four main areas standards, rules and policies related to the contribution and access to information, communications and operations management, access control and security of human resources including awareness and education of the users about security issues should involve a range of users ranging from therapists to legal and technical experts and always consider the principle of "protecting the rights of patients with convenient access to patient information" to develop their security and development of programs.

Cite this article as: Karami M. Patient's Electronic Environment Information Rights. *Bioeth Health Law J.* 2021; 1: 1-5 (e9). http://doi.org/10.22037/bhl.v1i1.38151

Introduction

ELectronic Health Records (EHR) has become a powerful tool for patient and clinicians. In the field of EHR having comprehensive information, the system is considerably helpful to provide patient-centered care (1). The purpose of EHR is to provide evidence-based information about patient care in the past, present, and future. This documentation provides a communication tool between different clinicians (2). Once medical records were developed electronically, the capacity to be accessible everywhere was developed. For this purpose, it is essential to collect medical information from different sources. This feature of the ability to access and progress in information and communication technologies has led to a situation in which patient information faces security and privacy threats (1). According to reviewed studies, security is an essential functional requirement for developing EHR, in this regard, it is necessary to plan a security program including the identification of potential threats and administrative processes to remove threats or to reduce their impacts on developing the damage for healthcare organizations. The security program of healthcare organizations should be developed around three axes including the administrative, physical and technical safeguards that each can be divided into subgroups. In this article, first, the concepts of this field are defined and then the strategies of protecting the patients' rights concerning these three axes are discussed in detail.

Ethical Considerations

Publication of the results is carried out without bias, honestly, and by citing the original reliable resources and references.

Materials and Methods

This review study was conducted based on library research and web-based electronic. The study aimed to identify the common security actions which can be applied to reduce the potential risks for healthcare information. To literature review, scientific databases such as Web of science, Emerald, Proquest, EBSCO host research, PubMed, and books in the field of medical informatics and security of information systems in the healthcare system were used as primary sources.

Findings

Development of a security plan to protect the information and information systems in addition to the improvement of the quality of healthcare, it is necessary to be around three core of administrative, physical, and technical safeguards to achieve the three main objectives related to information rights of patients, including confidentiality, integrity, and availability.

In terms of patients' rights, we are faced with the following concepts:

- **Security** includes measures, techniques, and technologies used to safeguard data and also accountability which means the right of individuals to criticize or accept why certain things have happened.
- **Privacy** means the rights of individuals to protect the healthcare information aimed to not to be shared with other people and also to control the information that should be revealed. In other words, individuals, groups, or institutions claim to determine when, how and how much information should be shared with others.
- **Confidentiality** defines as a process that ensures information is accessible only to authorized persons. Confidentiality is achieved through access control and encryption techniques.
- **Integrity** ensures that the information is accurate and does not change in unauthorized ways which means when data are the same as the data which is received. This has a significant impact on patient safety.
- **Availability** refers to the usability and accessibility of information is authorized on demand of an organization or individual. This has a significant impact on the effectiveness of care.
- **Authentication** means a process that confirms the user's identity.
- **Authorization** is the process of creating access right for the user.
- **Non-repudiation** ensuring that every transaction that happens is approvable which means the sender and receiver agree on the exchange (1-7).

Security Strategies

The security program of healthcare organizations can be developed around three axes including the administrative, physical and technical safeguards. These safeguards are explained in detail as follow:

A) Administrative safeguards: These safeguards include risk analysis and management, chief security officer, and security system evaluation:

A-1) the risk analysis: It is a security program including identifying potential threats for security and administrative processes to remove the threats or reduce their impacts on developing the damage as follows:

- *Boundary Definition*: This step should be determined in detail through the determination of the health information for patients, health information systems, and users of information and systems.
- *Threats identification*: is implemented through making a list of potential threats to health systems, including human threats, threats to the environment and nature, and threats caused by the bad performance of the technology.
- *Vulnerability identification:* It is determined using software packages, interviews, audits, and external consultants, flaws or weaknesses in system procedures or design.
- *Analysis of security controls* Analysis includes preventive controls and controls designed to detect actual or potential breaches.
- *Risk likelihood determination*: It includes the degree of risk for each part of the health information system.

- *Impact analysis*: At this stage, the effects of security breaches on confidentiality, integrity, and availability are determined.
- *Risk Determination*: At this point, all the information gathered up to determine the actual level of risk based on factors such as the likelihood of a particular threat to developing particular damage, the extent to which threats are successfully exploited, and the adequacy of planed or existing security controls.
- *Security Control Recommendations*: this final step is to compile summary reports on the findings of the analysis and recommendations for improving the security controls.

A-2) Chief Security Officer: any healthcare organization should consider a person to be responsible for monitoring information security programs. This person as a chief security officer should report to the chief information officer (CIO) or another administrator in the health care organization.

A-3) System security evaluation: increasing effort has been applied to create a global standard for IT security. For example, one source of these standards include computer system evaluation criteria, published by the U.S. military and the other standard is ISO15408 that according to them the organization's security systems can be assessed (8-9).

B) Physical safeguards: These safeguards are listed in the following:

B-1) Assigned security responsibility: each employee should be responsible for one part of the security system. For example, in the nursing unit, the director is responsible for the fact that all employees should be trained on the importance and application of security measures. Another important point is that a network administrator should consider as the person responsible for assigning initial passwords and removing access from terminated employees or employees who transfer to other departments.

B-2) Media control: This control includes the policies and procedures that control receiving and removing the hardware, software, and computer media in and out of the organization, their movements inside the organization, and also the approach for data storage. Methods of disposal or final state of electronic media is also another aspect of the media control so that when an organization gathers its old computers or equipment, some policies should be considered for destroying patients' information.

B-3) Physical access control: This control is performed through the use of physical tools such as a lock and key. In this way, in addition to providing access to patient information for clinicians, they may be limited. Alternatively, the inventory control system can be used that involving marking or tagging each piece of equipment with a unique number and assigning each piece to a location and a responsible person. When the equipment is moved, retired, or destroyed, it should be documented in the inventory control system. Another form of physical control is to install antitheft devices, such as chains that attach computers to desks, alarms, and other tools that deter thieves.

B-4) Workstation Security: Because the workstations allow access to patient information, they must be placed in areas that are secure or monitored at all times. The screen is placed in such a way that information is not visible to everyone. Another important aspect is developing clear policies for the use of shared workstations (4, 8, 10, 11).

C) Technical safeguards: These safeguards are as follows**:**

C-1) Access control: This means that only people, who need to be aware, should have access to health information and patient's identity. Health data access control methods may be through an available user-based, role-based, and context-based access (1, 3, 4, 9, 12).

C-2) Entity authentication methods: one or more of the following methods are used to confirm the qualification procedures for inspection.

- *Password System:* The most common method for access control in the health information system is a combination of user name and password. In this case, the password is more secure than the username.
- *Biometric Identification Systems:* Biometric identification methods are in the form of a voiceprint, fingerprint, handprint, retinal scan, face print, or full body scan.
- *Telephone callback procedures:* This method is used when the employees want to have access to the information from home. In the callback, when the modem is connected to the system, this program checks the phone number at first and then approves the accessibility (13, 11, 8, 4).
- *Token*s are tools such as key card which inserted to the door or PC. In this system, identification is based on the user's possession of the token. The disadvantage of a token is that it may be lost or misplaced or stolen. When tokens are used with

passwords, the password must be written on the token or somewhere near it (4, 9, 14-15).

C-3) Audit trails are a procedure that shows who has access to the system and what has been done in the available time. It also creates the potential for network administrators to observe the use of network resource (14, 16).

C-4) Data encryption is used to ensure the security of data transfer from a place to another in the network against $^{\text{eavesdropping}}$ or $^{\text{seeking to intercept}}$. Forms of encryption that are used in the health sector include:

- *Public Key Infrastructure:* In this system, there are two public and private keys. Usually, data are encrypted using the public key and with the particular private key.
- *Pretty Good Privacy (PGP):* The public key and the digital signature are used and the sender and receiver must both have the same P.J.P on their workstation (4, 10, 11, 16, 17).

C-5) Firewall safeguard: firewall was defined as "a system or combination of systems that support an access control policy between two networks" (4). This term can be used to describe software that protects computing resources or a combination of software, hardware, and policies that protect these resources. The most common location for a firewall is between the internal network and the Internet. Although firewalls are present overall the healthcare security systems, they cannot protect a system against all types of attacks, for example, the firewall cannot stop the viruses which can be hidden within the documents.

C-6) Viruses checking: Viruses control is an important part of a health information security program. Common types of viruses are in the form of file infectors, system or boot-record infectors, and macro viruses. Worms are also certain types of viruses that are stored on a computer and then replicated. Worms typically transfer from one computer to another via e-mail (4, 9, 12, 14, 15).

Conclusions

Security plan for a health care organization includes identifying potential threats and implementing processes to eliminate or reduce these threats to achieve goals such as confidentiality, accuracy, and availability. In this regard, it is necessary to protect both information and IT-related equipment such as networks; hardware, software, and applications since this equipment is very expensive.

Often, health care organizations are faced with two main challenges to planning an effective security program. The first challenge is how to make a balance between the need for security and the security-related costs, and the second challenge is how to make a balance between security and the availability and accessibility of health data anywhere and anytime if needed.

Thus, the main purpose of maintaining health information or medical records is to improve the quality of patient care. On one hand, if the security measures are so strict, then, proper access to patient information will be difficult.

On the other hand, if the organization allows the staff unlimited access to patient information, then, the patient's rights in terms of privacy and confidentiality will be undermined and also IT-related equipment will be at significant risk.

To develop a security program, health care organizations must do three main activities to overcome these challenges. These activities include compliance with standards, rules, and policies on information sharing and accessibility; communications and operations management; and access and security control on human resources. This control is just awareness and educates users about security issues.

Therefore, health care organizations to achieve a good security program in an electronic environment should involve a spectrum of users from clinicians to lawyers and always pay attention to the principle of "protecting the rights of patients with proper access to patient information".

Acknowledgements

None.

Conflict of Interest Statement

The author declares that they have no conflicts of interest.

References

1. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal. 2021 Jul 1;22(2):177-83.
2. Xie W, Mehta N, Palvia P. Value co-creation dimensions and challenges in EHR systems. Journal of Information Technology Case and Application Research. 2020 Jul 2;22(3):188-215.
3. Fernández-Alemán JL, Señor IC, Lozoya PÁ, Toval A. Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics. 2013 Jun 30;46(3):541-62.

4. Petoft A, Abbasi M. Citizenship Rights: from Good Governance to Administrative Procedures. Tehran: Justice Publication. 2017:205-6.
5. Chen YY, Lu JC, Jan JK. A secure EHR system based on hybrid clouds. J Med Syst. 2012; 1;36(5):3375-84.
6. Abbasi M, Azizi F, SHAMSI GE, Naserirad M, AKBARI LM. Conceptual definition and operationalization of spiritual health: A methodological study.
7. Yoo S, Kim S, Lee S, Lee KH, Baek RM, Hwang H. A study of user requests regarding the fully electronic health record system at Seoul National University Bundang Hospital: challenges for future electronic health record systems. International journal of medical informatics. 2013; 31;82(5):387-97.
8. Moghaddam, Mahmoud Nekoei, et al. "Awareness of Patients' rights charter and respecting it from the perspective of patients and nurses: A study of limited surgical centers in Kerman city, 2013." Bioethics Journal (Quarterly) 4.11 (2016): 31-56.
9. Abasi M, Petoft A. Citizenship Rights: from the Government Protection to Monitoring on it. Tehran: Justice Publication. 2017:59-65.
10. Abbasi M, Petoft A. Citizenship Rights: from the Foundations to the Social Basis. Tehran: Justice Publication. 2017:58-63.
11. Singh AK, Anand A, Lv Z, Ko H, Mohan A. A Survey on Healthcare Data: A Security Perspective. ACM Transactions on Multimidia Computing Communications and Applications. 2021 May 17;17(2s):1-26.
12. Abbasi M, Majdzadeh R, Zali A, Karimi A, Akrami F. The evolution of public health ethics frameworks: systematic review of moral values and norms in public health policy. Medicine, Health Care and Philosophy. 2018 Sep;21(3):387-402.
13. Rodrigues JJ, editor. Health Information Systems: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications. IGI Global; 2009.
14. Petoft A, Abassi M. Fundamentals of Neurolaw. Tehran: Medical Ethics and Law Research Center, Shahid Beheshti University of Medical Sciences. 2019.
15. McWay DC. Today's health information management: An integrated approach. Cengage Learning; 2013.
16. Hristidis V, Varadarajan RR, Biondich P, Weiner M. Information discovery on electronic health records using authority flow techniques. BMC medical informatics and decision making. 2010; 22;10(1):64.
17. Jamshidi A, Petoft A. citizens'rights in the light of modern administrative procedures. journal of bioethics, 2012; 6 (21):23-50