Patient's Electronic Environment Information Rights

Mahtab Karami (PhD) 1
1Health Information Management Research Center (HIMRC), Department of Health Information Technology and Management, School of Allied-Medical sciences, Kashan University of Medical Sciences, Kashan, Iran.

ABSTRACT

Background and Aim: Electronic health record is one of the most important achievements of the eHealth to achieve a patient-centered care. The aim of the patient-centered care is 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, it is necessary to healthcare organizations to create the security solution in order to protect the rights of their patients.

Materials and Methods: This review is based on the 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 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" in order to develop their own security and development of programs.

Introduction

Electronic Health Records (EHR) has become a powerful tool for patient and clinicians. In the field of EHR having comprehensive information system is considerably helpful to provide patient-centered care.1 The purpose of EHR is providing 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 was 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 face the security and privacy threats.1 According to reviewed studies, the 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. 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 with regard to these three axes are discussed in detail.
Materials and Methods
This review study was conducted based on a library research and web-based electronic. The aim of study was to identify the common security actions which can be applied to reduce the potential risks for healthcare information. In order to literature review the 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.

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

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 in order 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 that means the right of individuals to criticize or accept about 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, it is the claim of individuals, groups or institutions 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 exactly same the data which is received. This has a significant impact on patient safety.
- **Availability** refers to 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 that means the sender and receiver agree on the exchange.1–7

Security Strategies
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 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 environment and nature, and threats caused by the bad performance of 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 is 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 particular threat to develop 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 a 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 to 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 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, 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 gather 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 lock and key. In this way, in addition to providing access to patient information for clinicians, they may be limited. Alternatively, 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.3,8,10,11  
**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 health information system is a combination of user name and password. In this case, the password is more secure than 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 callback, when modem is connected to the system, this program checks the phone number at first and then approves the accessibility.13,11,8,4  
- **Tokens** 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 token is that they may be lost or misplaced or stolen. When tokens are used with passwords, it is essential that the password be written on the token or somewhere near it.3,9,14,15  
**C-3) Audit trails** is 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 insure the security of data transfer from a place to another in the network against the eavesdropping or 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 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.3,4,10,11,16,17  
**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, but they cannot protect a system against all types of the attacks, for example, firewall cannot stop the viruses which can be hidden within the documents.  
**C-6) Viruses checking:** virus control is an important part of 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 computer and then replicated. Worms typically transfer from one computer to another via e-mail.3,9,12,14,15  
**Conclusions**  
Security plan for a health care organization includes identifying potential threats and implementing
processes to eliminate or reduce these threats in order 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 these equipment are very expensive.

Often, health care organizations are faced with two main challenges to plan an effective security program. The first challenge is how to make balance between the need for security and the security-related costs, and the second challenge is how to make 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 to 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.

In order to develop 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 electronic environment should involve 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