J Med Syst (2010) 34:629–642
DOI 10.1007/s10916-009-9276-7

ORIGINAL PAPER

Security Requirements and Solutions in Electronic Health Records: Lessons Learned from a Comparative Study

Mehrdad Farzandipour · Farahnaz Sadoughi · Maryam Ahmadi · Iraj Karimi

Received: 6 January 2009 / Accepted: 8 March 2009 / Published online: 1 April 2009

Abstract A growing capacity of information technologies in collection, storage and transmission of information in unprecedented amounts has produced significant problems about the availability of wide limit of the consumers of Electronic Health Records of Patients. With regard to the existence of many approaches to developing Electronic Health Records, the basic question is what kind of Model is suitable for the guarantee of the security of Electronic Health Records? The present study is a descriptive–comparative investigation conducted in Iran in 2007, along with comparisons made Electronic health records information security requirements of Australia, Canada, England and U.S.A with. The research was based on the study of texts such as articles, library's books and journals and reliable websites from 1992 to 2006. Based on the collected data, a primary Model was designed. The Delphi Technique was offered to evaluate the questionnaire and final Model was designed and proposed. Australia, Canada, England and U.S.A have requirements related to organizing information security, classifying and controlling information asset, security of human resources, environmental and physical security, Operational and communication management security, information access control security and development and Maintenance security of Electronic Health Records information systems. In the U.S.A, the above security requirements are presented in administrative, Physical and Technical safeguards. Based on the research findings, a comprehensive model of electronic health record security requirements in seven pivots is presented for Iran. This model is a collection of EHR security requirements from studied countries. The studied countries are solely subject to part of elements of this model. The suggested model is different from the ones used in other countries in some respects and is recommended for application in Iran.

Keywords Security model · Security requirements · Information security · Electronic health records

M. Farzandipour (✉)
Kashan University of Medical Sciences,
3rd km. of Ravand-Kashan Highway,
Kashan, Iran
e-mail: farzandipour_m@kaums.ac.ir

F. Sadoughi · M. Ahmadi · I. Karimi
Iran University of Medical Sciences,
Tehran, Iran

F. Sadoughi
e-mail: f_sadoughi@yahoo.com

M. Ahmadi
e-mail: m_ahmadi24@yahoo.com

I. Karimi
e-mail: irajk100@yahoo.com

Introduction

Today, one of the most important applications of information technology (IT) in the field of health is making Electronic health Records (EHR). Enhancing capacity of information technologies and communications due to collecting, storing and transferring information in considerable levels, have produced significant difficulties for patients [1]. The patients have concerns about individuals accessibility to their own EHR [2, 3]. Computer records of various places are accessible and security defect in its system can disclose hundreds or thousands records [4].

Security and protection of patient's health data are not only demanded by the patient himself, but in most developed countries they are also required by law. Health data need to be protected against manipulation, unauthorized access and abuse. Therefore, aspects of data security and data protection, including: confidentiality, Integrity, authentication, accountability and availability need to be considered carefully for every activity which deals with storing and exchanging information, especially when developing and implementing HER [5].

Previous research on medical records manual system of Iran in Isfahan healthcare centers in 2002 revealed that, in 82% of units, there where not suitable protective mechanisms for the security of patients records [6]. The security system of the present hospital medical records meets only 62.3% of the international standards showing deficiencies in this field [7]. Another piece of research in 2004 in the U.S.A, revealed that concerns of security problems and information confidentiality are a considerable obstacle to wide performance of computer records systems and data distribution [8]. The 2003 investigation of Canada revealed that presence and implementation of policies and security infrastructure are widely different across organizations, and almost 75% of them do not contain the key policies for accessibility to information in place [9].

Electronic health discussion started with the approval of TAKFAB project in Iran, Ministry of Health and Medical Education in 2001. Further related studies reveal that TAKFAB measures have not been truly national or have remained unfinished. Electronic health development requires a supreme public institute to take the necessary steps for electronic health development in the country. Fortunately, in 2008, information technology high council was established in the presidency institute [10].

Dispersed activities are presently done in relation to hospital information systems in Iran. The potentials and needs for sharing information hardly taken into account in these systems and all of them supplied in non-shareable formats [11]. Based on previous studies, each Iranian citizen are suffers from disease in the last 12.5 years of his/her life. This indicates that there is more need for healthcare data systems in this life period of Iranians and implementing the electronic health record is essential with respect to its noticeable capabilities in society health promotion. Furthermore, one of the basic issues of EHR is that patients can see their electronic records. Thus, in the future, each citizen will be able to observe his/her EHR with proper security precautions [10]. The establishment of private limits and security for information causes people to be able to control their personal information and to guarantee its confidentiality and security [12]. Protecting health information is as important as locking your doors at home every night [13].

As the country Iran starts designing and moving toward electronic health record, information security becomes an inseparable part of electronic health record architecture and its technical and executive requirements must be thought of. Issues of electronic health information security are new in Iran. Therefore general standards of information security management as well as specific standards in health domain are utilized. In addition more guidelines and rules for this specific context need to be compiled and developed and the study of EHR security policies is a crucial step to take in Iran [14], and seems is need focus on human and technical factors for success of security policies in Iran.

Objective

With regard to the recent attention of the Ministry of Health and Medical Education, to establishing EHR for each Iranian and to the concerns about information security, it is necessary to provide and compile EHR security requirements and use other countries, experiences. Thus, the basic question of this study is, "what kind of Model is suitable for guaranteeing the security of EHR information in Iran?

Method

This research was carried out in a descriptive–comparative method in Iran in 2007 in Three Phases as follows:

Phase one: Comparative study

In this research, security requirements of Electronic health records information in Australia, Canada, England and U.S.A were studied in the following seven pivots:

1- Organizing security of information refers to management liability to information security, independent review of information security, third-party access security and independent contractor.
2- Classifying security and asset control refers to assets accountability, information classification and audit.
3- Security of human resources refers to security requirements in job responsibilities, training users, responding to security incidents and employment termination.
4- Physical and environmental security refers to secure areas, equipment security and general controls.
5- Security of operations and communications management refers to operational procedures and responsibilities, system planning and acceptance, housekeeping, network management, media handling and security, information exchange and audit logging.
6- Access control security refers to access control policy, user access management, user responsibilities, network

access control, operating system access control, application access control, monitoring system access and mobile computing.

7- Development and maintenance security of electronic health records information systems refers to systems security conditions, security in application systems, security of system files, Security in development and support processes and cryptographic controls.

In the U.S.A, these seven pivots were classified in three pivot classes including, Administrative safeguards, Physical safeguards and Technical safeguards. The countries studied in this research were selected by using library's resources, the internet and consultation with professionals based on the following features:

Developing integrated records of patients electronically is one of the preferences of many countries [12]. But from among Countries that are planning for developing Electronic health records and have advanced in this field such as Brazil, Malaysia, Canada, Hong Kong, Denmark, England, U.S.A, Southern Africa, Australia, Germany and France, our Subject countries include Australia, Canada, England and U.S.A were selected base on following aspects [15–20]:

1- National effort to developing Electronic health records and its Infrastructure
2- Expansion of designing and trail accomplishment scope of Electronic Health Records
3- Cooperation of private section along with governmental section in designing and;
4- Suitable investment in designing and developing of Electronic Health Records

After selecting the subject countries, information on seven pivots of Electronic Health Records security requirements were derived from these countries and was studied in comparative tables. Data collection was done through the study of documents, records, articles, books and journals available in libraries or on websites published by health information organizations in those subjected countries. Unreliable websites were excluded from the study, and only reliable websites such as National Health Services (NHS), Health Connect, Health Online, Advisory Council of Health Infostructure (ACHI), Health Infoway and Health Insurance portability and Accountability Act (HIPAA) were included. These articles were all in English, published from 1992 to 2006. For Iran, we referred to the directives issued by the Ministry of Health and the investigations made in this country to obtain information on security requirements for EHRs [11].

Phase two: Designing the preliminary model

To design the primary Model, security requirements of Electronic Health Records of the studied countries were compared to each other. Similar items were eliminated and different items in each mentioned pivot were included in our suggested Model.

Phase three: Determining the reliability of the proposed model

To determine the validity of the Proposed Model Delphi Technique was used. For this purpose, questionnaire items were constructed based on the contents of the primary model including the three choices of "agree", "disagree", and "neutral". For each subsection of the questionnaire, there was also one open ended question. The data for the questionnaire were collected from Valid and formal websites in the subject countries and are considered as formal documents.

The validity of the proposed model questionnaire was also assessed using the viewpoints of academic the professionals, medical records specialists and Health Information Management specialists in Iran. Some items were added to it based on the professionals' opinions and some items were eliminated. To determine the reliability of the questionnaire, Brown Pearson method was used. The questionnaire was administered to a number of specialists. After 10 days again. The two administrations of the tool helped researchers to better determine its reliability. The reliability coefficient of the questionnaire was estimated 95%.

After determining the reliability and validity of the questionnaire based on the proposed model including seven aforementioned parts, the questionnaire was sent to 35 specialists including, Health ministry information Technology management professionals, experts of information Technology Management in medical sciences universities and faculty members of universities in the country. The questionnaire was sent by post and/or forwarded through email. Thirty-two participants completed and returned the questionnaire.

In order to analyze the collected data, descriptive statistics was used. Items of the model which had been approved by less than 50% of the participating experts were eliminated from the model, and the items that had been confirmed by 75% or more of the professionals were accepted. If an item confirmed by 50% to 74% of the participants, it was put to votes again.

Results

Results of the comparative study

All subject countries emphasize the definition of information security responsibilities, clearly by security official (Table 1).

The majority of subject countries place emphasis on the calculation of all assets of organization information technology and on information classification and users awareness of confidential health information (Table 2).

All of subject countries place emphasis on including security requirements in job duties and training for security methods to all third parties and users of organization information (Table 3).

All subject countries emphasize creating secure levels for environmental and physical protection of information and equipments security for preventing possible damages (Table 4).

The majority of subject countries emphasize the development of operational procedures and responsibilities for the performance of computers, regular back up of information, computing media handling and security and existence of formal agreements between organizations for exchange of electronic information (Table 5).

The majority of subject countries place emphasis on developing access control policy to information and user access management (Table 6).

The majority of subject countries place emphasis on security in application systems and files (Table 7).

Results related to reliability of the model

Thirty-two specialists participated in the study. Based on the findings 66% of specialists were 25–34 years old and 34% were 35–54 years old. Work experience for 69% of them was 3–9 years and for 16% 10 years or more. Fifty-three percent of the participants were male and 47% of them were female. Eighty-five percent of the participants held B.A, 9% M.A., and 6% Ph.D degrees. Educational course of them was computer engineering.

According to the majority of the specialists, information security in organization is a tool for the success of the IT

Table 1 Comparison of the organization requirements of information security of EHR in subject countries

Health information security organization requirements		Countries			
		Australia	Canada	England	U.S.A.
Management liability to information security and allocation of responsibilities	Establishing Information security management team in organization	√	√	√	–
	Giving responsibility of all subjects related with organization information technology security to security management team	√	–	–	–
	Giving responsibility of all subjects related with information technology security to Board of directors from organization of care custodian	–	–	√	–
	Clear explanation of information Security responsibilities by security responsible official	√	√	√	√
	Confirming new facilities of processing information by information technology manager	√	–	–	–
	Presence of inter organizational information Security advisor for giving professional advises in organization	√	–	–	–
	Establishment suitable relationship between related external organizations for quick response to security events	√	–	–	√
Independent review of information security	independent review of policy implementation of information security	√	√	–	√
	written Confirm of implementation the information security policy by organization executive manager or board of directors	–	√	–	√
Third-party access security	Evaluation and access control of third parties to information technology facilities	√	√	–	√
	Access of third-parties to information technology facilities base on valid contraction with mentioning all of the conditions that are adopt with policies and organization standards	√	√	–	√
Security in external organizations contracts	Mentioning security conditions in contractions in case of delivering management or process control of information facilities to an external organization	√	–	–	√
	Harmony of information security activates by different parties representatives of agency	–	√	–	–
	Formal allocation of information recipient organizations duties for information confidentiality maintenance	–	√	–	√

Table 2 Comparison of the control and classification security requirements of EHR assets in subject countries

Security requirements of information assets classification and control		Countries			
		Australia	Canada	England	U.S.A
Assets accountability	All assets accounted and have a nominated owner	√	√	√	–
Information classification	Information security classification into four levels, public, internal, confidential and secret information	√	–	–	–
	Being rules of determination, documentation and practicable of acceptable use of information assets in organization	–	√	√	–
	Confidential classification of all health data in organizations as private health information	–	√	–	–
	Information classification by owner of information assets	–	–	√	–
Systematic auditing of assets	Awareness of users in all organizations from being confidential of information by labeling on information	√	√	√	–
	Systematic Auditing of assets inventories, regular labeling design, information classification and handling guidelines	–	–	√	√

project (that in subjected countries has not point to it). They also confirmed information classification to three classes. (Table 8).

Most specialists agreed with items on human resources security, physical and environmental security and communications and operations management security (Table 9).

The necessity of developing very highly secure layers of medical sciences databases and information storage encoding formats in database were emphasized by the participants. This was not observed in the primary models used for the study (Table 10).

Discussion

The findings of this comparative study showed that the subject countries emphasized the clear explanation of information security responsibilities and third party access security [21–23]. Experts participating in the study emphasized all items of the above-mentioned pivot. In addition, information security as a tool for the success of information technology project was stressed. The experts did not agree to give the responsibility of information security to the manager of organization, neither did they agree with the

Table 3 Comparison of the human resources security requirements of EHR in subject countries

Human resources security requirements		Countries			
		Australia	Canada	England	U.S.A
Including security requirements in job responsibilities	Including the roles and security duties of organization security policy in job description of organization information security staff	√	√	√	√
	Checks on permanent and temporary staff and contractors from the viewpoint of making security risk in job process	√	–	√	√
	Signing contraction for keeping information confidentiality by personnel as a part of primary conditions of employment	√	√	√	√
	Determining responsibilities and duties of personnel concerning information security in employment conditions	√	√	√	√
	Investigation of identification and address accuracy of permanent or temporary users and contractor in all of the organizations	–	√	–	–
Information security training	Training security procedures to staff and all third-party users of organization information	√	√	√	√
Responding to security incidents	Quick report to all of the events that effect on security of organization information by management channels	√	–	√	√
	Record and reporting any security malfunctions that observed by all of the users	√	–	√	√
	Establishing and following information security procedures for reporting software malfunctions	√	–	–	√
	Establishing formal disciplinary process for any users violation of organization information security policies	√	–	√	√
Terminating user access in employment termination	End of users access to information at their employment termination in organization	–	√	–	√

Table 4 Comparison of the environmental and physical security requirements of Information of EHR in subject countries

Physical and environmental security requirements		Countries			
		Australia	Canada	England	U.S.A
Secure areas	Protecting information technology facilities with developing buffers around them	√	–	√	–
	Access control of individuals to information technology facilities by appropriate entry controls	√	√	√	√
	Creating secure areas with special security requirements in order to protect offices, rooms and facilities	√	√	√	√
	Guidelines control of secure work environments in order to enhance the environments security	√	–	–	√
Protecting equipment security	Sitting and protecting of security equipment to reduce the risks, environmental threats and opportunities for unauthorized access	√	√	√	√
	Protection of computing and communications equipment against temporary power failures and other electrical anomalies with use of uninterruptible power supply	√	√	√	–
	Protection of power and telecommunications cabling carrying data from damage or interception	√	–	√	–
	Properly maintain of computing and communications equipment in accordance with manufacturer's instructions	√	–	√	√
	applying supervisions and security procedures for equipment used outside of organization premises	√	√	√	–
	Taking legal ground from responsible person of information technology services help desk and erasing information of all equipment before destruction of information technology equipment	√	–	–	–
General controls of equipment	Turning out personal computer equipment in un-use state	√	–	√	–
	Non-keeping sensitive information by user on their desk	√	–	√	–
	Non-removing equipment, facilities or software belonging to organization from premises without authorization	√	√	√	–
	Destruction of medias that contain information or overwriting them, in case of un-need to long-term use them	–	√	√	–
	Permitting hardware and software repairs just by maintenance authorize personnel	–	–	√	–
	Not placing any foods and drinks near the computer equipments by employees	–	–	√	–
	Removing confidential or sensitive information on printers, photocopy machine and fax as soon as possible	–	–	√	–

Table 5 Comparison of the security requirements of communications and operations management of EHR in subject countries

Security requirements of communications and operations management of health information		Countries			
		Australia	Canada	England	U.S.A
Secure operational procedures and responsibilities	Record and maintain of performance procedures in organization computers performance	√	–	√	–
	Changes control in information processing facilities and systems	√	√	√	√
	Establishing and following of incident management responsibilities and procedures	√	–	√	√
	Segregation of duties and areas of responsibility of employees and contractors as possible	√	√	√	√
	Separating development and testing facilities of software from operational facilities	√	√	–	√
	Including appropriate control and measurement of risks in contractions of information processing facilities office with a foreign contractor	–	–	√	√
System planning and acceptance	Monitoring and projections of future capacity requirements to ensuring information processing power and storage	√	√	√	–
	Definition of acceptance criteria for new information systems and testing them before acceptance	√	√	√	–
	Following suit procedure to prevent and detect the introduction of malicious software and remind users to use licensed software on organization systems	√	√	√	√

Table 5 (continued)

Security requirements of communications and operations management of health information		Countries			
		Australia	Canada	England	U.S.A
	Presence of comprehensive design of network and its Components into information technology section	–	–	√	–
House keeping	Secure and regular back-up copies of business information and software	√	√	√	√
	Reporting of information Processing and communications systems faults by users and performing Essential actions	√	–	√	√
Network security management	Performing necessary control by network managers to Achieve and maintain security in organization LAN and WAN	√	–	√	–
	Encoding health information while transferring them and use of public key infrastructure	–	√	–	√
	Maintain accuracy of resource and destination data while transferring information	–	√	–	√
Media handling and security	Following operating procedures to protect documents, computer media, data and system documentation from damage, theft and unauthorized access	√	√	√	√
	Maintaining health information on portable media	–	√	–	–
	Disposal of computer media when no longer required	√	√	√	–
	Taking adequate procedures for handling and storage of information in order to protect information from unauthorized disclosure or misuse	√	√	√	√
	Protection of system documentation (data memory) from unauthorized access	√	√	√	√
Information exchange	present formal agreement between organization and other ones for electronic information and software exchange	√	√	√	–
	Protecting media tools in transport from unauthorized access, misuse or corruption	√	–	–	√
	Protecting electronic commerce against fraud, contract disputes, disclosure or modification of information	√	–	–	–
	Using organization policy by users in internet applying and instructions of e-mail for e-mail security	√	–	√	–
	Implementing policy and guidelines to control the business and security risks in electronic office systems	√	–	√	–
	Creating procedures and essential control at using other traditional forms to exchanging information	√	–	√	–
	Maintaining backed-up information in secure physically environment outside of main place	–	√	–	–
	Following official process of information confirm before information is made publicly available in internet and protect of integrity of such information.	√	–	√	–
Audit logging	Create a secure audit record in Organization electronic systems	–	√	–	√
	Capability of organization electronic systems to displaying the former content of a record at any point in the past, as well the associated details of who entered, accessed or modified the data and at what time	–	√	–	√
	Retain and protect of secure audit log of all Organizations for the entire retention period of the records audited	–	√	–	–
	Being operational audit logging of information systems at all times	–	√	–	–
	Providing automated analysis tools in electronic systems to detection and prevention of system misuse	–	√	–	–
	Electronic systems capability to analyzing and identifying of all information users and related persons to information	–	√	–	√
	Providing appropriate security measures in electronic systems to protect audit logs from tampering	–	√	–	–
	Performing logs and audit logs in all of the organizations on a regular and ongoing basis	–	√	–	–

item on the costs that should be paid for the security project. Based on the recommendations of one of the experts, determining security level and the cost of information security should be relative to sensitivity of the project and its contents. In the studied countries requirements no mention have been made of these points.

With regard to importance and sensitivity of electronic information in treatment environments, Joint commission of

Table 6 Comparison of access control security requirements to information of EHR in subject countries

Access control security requirements to health information		Country			
		Australia	Canada	England	U.S.A
Access control policy	Definition and documentation of business requirements for access control and restricting to what is defined in access policy	√	√	√	√
User access management	Using a formal user registration and de-registration procedure for information access to all computing systems	√	√	√	√
	Developing limitation and allocation control and use of system or application privileges	√	√	√	–
	Control of passwords allocation through a formal management process	√	–	√	√
	Regularly reviewing user access rights	√	–	√	√
	Developing time limitation of user entrance to organization	–	√	√	√
	Periodically review of user registration details to information system	–	√	–	√
	Granting access to users by role-based in organization	–	√	√	√
	Each user access to information in a single role in each working period	–	√	–	–
	Capability of granting access to users in working groups	–	√	–	–
	Timely revocation of user access privileges to information	–	√	–	–
	Optional access control to information	–	√	–	–
User security responsibilities	Following users from good security practices in the selection and use of password	√	–	√	–
	Defining user responsibilities in organization and user agree to them	–	√	–	√
	All users and contractors awareness of security requirements and procedures for protecting unattended equipment	√	–	√	–
Network access control	Users direct access just to allowable services	√	–	–	–
	Controlling the path from user terminal to the computer service	√	√	–	–
	Taking authorization by remote users access	√	√	√	–
	Secure access control to diagnostic ports	√	√	–	–
	Performing controls to segregate groups of information services, users and information systems in networks	√	√	–	–
	Restricting capability of users connection in shared networks in accordance with to network services use policy	√	–	√	√
Operating system access control	Using secure log-on process for access to organization information systems	√	–	–	–
	Allocation unique user to all uses for their personal and sole use	√	√	–	√
	Using password management system to ensuring password quality	√	–	–	–
	Restricting and tightly control of using system utility programs	√	√	–	–
	Access control to operating systems	√	√	–	–
Application access control	Restricting access to information and commercial system functions in according with the defined business access control policy	√	–	–	√
Monitoring system access	Monitoring and reviewing regularly use of information systems	√	–	√	√
	Computer clocks synchronization for accurate recording of incidents	√	–	–	–
Mobile computing	Performing appropriate controls to protect against risks of working with mobile computing facilities	√	√	√	–
	Developing policies and procedures to authorize and control telecommuting activities	√	√	–	–
	Ensuring protect of mobile computer facilities by organization	–	–	√	–

accreditation in U.S.A has emphasized the medical records department manager responsibility in keeping information [24]. AHIMA (American Health Information Management Association) research in 2006 indicated that 100% of organizations have a security officer [25]. The security official is responsible for all policy developments, training and security compliance activities [13]. Schaectel has stated that every organization must have the activity listed as 'security management' [26].

The boost information security in computer systems, an information security manager should be appointed in healthcare centers, to determine users' information security responsibilities. It seems that this can be achieved by developing related organizational positions in the organizational

Table 7 Comparison of information systems development and maintenance security requirements of EHR in subject countries

information systems development and maintenance security requirements		Countries			
		Australia	Canada	England	U.S.A
Systems security conditions	Determining security control to new systems or improving present systems base on job conditions	√	–	√	–
Security in application systems	Validating data input to application systems	√	√	√	–
	Incorporating validation checks into systems to detect corruption of the data processed	√	–	√	√
	Validating data output from application system	√	√	√	–
	Possibility of identifying unique patients or persons by information system	–	√	–	√
Security of system files	Implementation control of software on operational systems	√	√	√	–
	Access control to programs structural files	√	√	√	–
	Maintaining used software of information systems in supportive level by provider	–	–	√	–
Security in development and support processes	Implementation of changes in information systems under strict change control Procedures	√	–	√	√
	Review and test of application systems whenever changes occur	√	–	√	–
	un-using real data to testing	–	–	√	–
	Taking actions by organizations to preventing damages of software systems	–	–	√	–
	Controlling purchase, use and modification of software to protect against covert channel and Trojan code	√	√	–	–
	Performing essential controls to security of software development of independent contractor	√	–	–	√
Cryptographic control	Providing digital signature for users by information system	–	√	√	–
	Validating and preserving digital signatures by information system	–	√	√	–

chart of healthcare centers and definition of the related duties.

The findings of this comparative study showed that the majority of subject countries in the pivot of control and classification security, emphasized assets accountability, information classification and awareness of users [21–23]. The difference was that Australia emphasized four sensitive classes [22], Canada stressed classification of information to the general and confidential manner [21], and England emphasized information classification by the information assets owner [23]. Specialists evaluating the proposed model emphasized all of above pivot subjects. The only difference was that the confidentiality of information was classified into three classes instead of four.

Zahedifars' research revealed that financial sheets related to treatment of the patients were part of confidential sheets in 90.9% of the studied manual systems. Also in 18.2% of the units, there were appropriate protective mechanisms for security of the records related to AIDS patients, psychotic patients and other sensitive diseases [6].

It seems that healthcare centers of Iran disregard asset control and classification security and they never follow a standard method. Thus, the classification of Electronic Health Records information in three classes including, administrative, financial and diagnostic as well as treatment information is essential. In addition, information must be classified into the three security classes of internal, confidential and secret classes respectively and mechanisms for information protection and access level for the each class must be defined.

The findings of this comparative study showed that all subject countries in pivot of human resources security emphasized including security requirements in job responsibilities and training all of the organization employees and third party users [21–23]. Specialists confirmed all of items of this pivot.

It is critical that every computer user be aware of his/her information security [13]. Results from the study in 2003 of Canada indicated that 90% of employees were required to sign confidentiality agreements [8]. Yung and Cookie stated that management should help to decrease risk potential and damage to the organization's assets such as information by investment on training the workforce [24]. AHIMA research indicated that 64% of the organization's new employees were trained for security rules in-house [25].

With attention to designing Electronic Health Records in the many countries, determining responsibilities and security duties in job activities is necessary. Also, training is provided in protecting electronic health records information security in the beginning of employment and during the job in training programs.

Table 8 Information security organization and classification security requirements and assets control of EHR from the professionals' point of view

Health information security organization requirements
Items agreed on by 75% or more
Management liability to information and allocation responsibilities:
(1) Considering information security for IT project success in organization as a tool
Independent review of information security policy
Access Control third-party to information Technology facilities
Containing security requirements in external organizations contracts
Items agreed on by less than 50%
Management liability to information and allocation responsibilities
(1) Giving responsibility of organization information technology security subject to: Organization manager or information Technology manager or network manager or security manager or board of directors
(2) Considering information security for IT project success in organization as a goal
(3) Spending cost for IT project information security to rate: 10–40%
Security requirements of assets classification and control
Items agreed on by 75% or more
Accounting all information technology assets of organization and determining an owner for them
Information classification
(1) Information classification to three classes:
(a)First class, optional determine of internal access levels to information and preventing from external access to them
(b)Second class, confidentiality of inter-organization information and protecting them from external access
(c)Third class, secret information and protecting them from unauthorized access externally or internally
(2) Confidential classification of all health data in organization as private health information
Systematic auditing of assets
Items agreed on by less than 50%
Information classification
(1) Security classification of information to unclassified and common information
(2) Information classification by owner of information assets

The findings of this comparative study revealed that all subject countries emphasized developing security areas and protecting security equipment from unauthorized access in the pivot of physical and environmental security [21–23]. Specialists evaluating the proposed model emphasized this pivot. Equipment security includes keeping computers out of the patients or high-traffic areas, locking rooms containing sensitive assets, destroying electronic information when no longer needed and only allowing the certain individuals to access sensitive areas or data applications [13]. Therefore, with regard to the importance of the subject, it is essential that hardware equipments, software, and the electronic health records networks be maintained. Placing network cables in suitable ducts and servers of the systems in a locked room is vital. In servers sites and other installed equipments, hindering-detector systems and tools should be installed and to prevent damages resulting from power failures UPS (uninterruptible power supply) should used to keep the EHR databases server, powered for few minutes or hours [27].

The findings of this comparative study showed that all subject countries emphasized the secure operational procedures and responsibilities, system planning and acceptance, housekeeping and media handling and security [21–23]. Specialists evaluating the proposed model emphasized these items as well. The difference was on items related to recording telephonic conversations of the people who contact and the disposal of computing media in the long-term, which were not confirmed in this study.

Research in Canada in 2003 has shown that all organizations use firewall software to protect computer systems from damage in development and support processes [21]. Another investigation in 2003 indicated that, about 66% of subject organizations have plans for the regular audit and report of unusual access [9]. In Iran, because of the developing nature of hospital information systems, in some healthcare centers, some simple procedures are used for the security of information. For example, the research done by Zahedifar [6] showed that in all of the studied units, diskettes contain patients' information were kept in a secure place [6].

Salahi explained in a similar study that the present security systems of hospital medical records storage and retrieval is equal to 62.3% of that of the international standard which shows deficiencies in instruction and standards in this field in Iran [7]. Gupta has stated that

Table 9 Security requirements of human resources, information physical and environmental and communications and operations management of EHR from the professionals' point of view

Human resources security requirements
Items agreed on by 75% or more
Including security requirements in job responsibilities
Information security awareness, education and training
Reporting security incidents and malfunctions
Terminating user access upon termination of their employment with the organization
Physical and environmental security requirements of health information
Items agreed on by 75% or more
Using security perimeters to protect areas that contain information systems
Protecting equipment security
General controls of equipment and information from security hazards
Security requirements of Communications and operations management of Health information
Items agreed on by 75% or more
Secure operational procedures and responsibilities
System planning and acceptance procedures
Housekeeping procedures
Network Security management
Media handling and security procedures
Information and software exchange procedures
Audit logging procedures
Items agreed on by less than 50%
Secure operational procedures and responsibilities:
Recording content telephone conversations with persons who contacted with them
Media handling and security procedures:
Disposal of computer media when no longer required

network-based firewall is the best option for operating systems security. It is a lock for computer against outside intruders [13]. Also; Van der Haak has stated that secure socket layers (SSLs) can be used for establishing a secure connection. This method guaranties secure low-cost end-to-end transmission of information over the potentially insecure internet. In addition, for immediate access to health information, back-up procedures are often used to prevent accidental destruction or loss of data. Also accountability can be ensured by means of audit trail logs or file logs [5].

Therefore, recording all communications with the electronic health record system is necessary. For preventing damage to system, use of anti-harmful codes and firewall, doing regular back-ups of current information on systems, protecting information security by encoding information, use of public key infrastructure (PKI) and continuous performing of system logging is required.

The findings of this comparative study showed that all of subject countries emphasized developing user access control policies for health information and for the management of user access [21–23]. Specialists evaluating the proposed model emphasized all of access control policy requirements of the subject countries.

Based on the study in U.S.A in 2004, almost 88% of the individuals prefer password use for access secure to information [8]. According to an investigation in Canada in 2003, more than 80% of the subject organizations have set policies for staffs and physicians access to clinical records. All of them had access control to clinical systems with user ID and password and 90% of them had unique user ID and password [9]. Another study done in Isfahan about healthcare center's use of mechanized hospital information systems showed that in 81.8% of the studied units, information was uploaded to computers by authorized personnel who had passwords. In all of the units, users had access only to a part of computer programs related to their duties [8] which is similar to the present research findings.

Findings from research in 2004 in U.S.A indicated that lack of policy related to access to patients' information is the most important obstacle to developing a national infrastructure of health information. Only 5% of the individuals have electronic access to information and about 37% of them felt no need for electronic access to the patient's confidential information [8]. Based on the research in Canada in 2003, information access policy is widely different in organizations. About 25% of organizations have

Table 10 Security requirements of access control and information systems development and maintenance of EHR from the professionals' point of view

Access control security requirements of health information
Items agreed on by 75% or more
Access control policy
User access management
User security responsibilities
Network access control
Operating system access control
Application access control
Monitoring system access and use
Mobile computing and telecommuting
Development and maintenance security requirements of health information systems
Items agreed on by 75% or more
Systems security conditions
Security in application systems
Security of system files:
(1) Necessity of developing secure layer to medical sciences database is very high (75–100)
(2) Information storage to encoding format in database
Security in development and support processes
Cryptographic control
Items agreed on by less than 50%
Security of system files:
(1) Necessity of developing secure layer to medical sciences database:
(a) is low (1–25 score)
(b) is middle (25–50 score)
(c) is high (50–75 score)
(2) Information storage to decoding format in database

privacy policies and access to the information in place. More than 50% of organizations have policies related to remote access to the clinical information. Less than 50% have security aspects for remote access. about 33% have access controls for electronic information that has limited specialists access for clinical services, and about 40% provide unlimited access for clinical specialists [9], that is against the present research findings.

It seems, in spite of the lack of comprehensive requirements about access control security in Iran, some healthcare centers understand the need and practically apply provisions for health record information security. Therefore, unique electronic identifiers for patients, institutions, and service providers need to be developed based on accurate national electronic health records to make user identification and data tracing possible.

The findings of this comparative study indicated that the majority of subject countries emphasized the security of application systems and files in the pivot of information systems development and maintenance security [21–23]. Specialists participating in the study emphasized this pivot as well. In addition, the necessity of developing highly secure layers for the medical sciences databases and storing information in databases as encoded was confirmed, which was not included in the security standards of the countries studied in the present work.

In spite of importance of designing and launching comprehensive electronic health records, information security maintenance is even more important in the continuous use of the electronic system in health care. Thus, software databases for electronic health records must have high security layers. Encoded information placed in databases, with decoding keys for system managers and possibly use of electronic signature is recommended.

Conclusion

Based on the research findings, a comprehensive model of the electronic health record security requirements is presented for Iran in seven pivots. This model is a collection of EHR security requirements from studied countries. Each of the subject countries uses only part of this new model.

Its differences with studied countries model is that, in the classification and assets control axis, classification of health

information as public and un-classified have not been confirmed. In the procedures and operational responsibilities axis, 'recording telephonic conversations' and in handling and media security axis, 'disposal of computing media when no longer required' have not accepted.

Information security as a tool for the success of information technology project in organization, the necessity of the developing highly secure layers for medical sciences databases and storing information in databases as encoded information have been confirmed as new dimensions added based on this study.

Because the EHR issue and its security is novel in Iran, more research in this field must be carried out. Based on the results of the current study and researchers' experiences, the weakness of the electronic health systems in Iran consists of:

1- Lack of sufficient qualified manpower in the health informatics and its security.
2- Lack of appropriate health information classification.
3- Undetermined responsibilities of the health staff and insufficient training information security.
4- Non-use of communications and operations security systems.
5- Lack of security procedures for health electronic systems development and maintenance.

On the other hand, it seems that attention to physical and environmental security of current electronic information systems in the health centers of Iran and use of access control methods to health electronic information are the sole strengths of current systems. However, the system must be supported with determining IDs for all patients, service providers and institutions. Thus there are many gaps between current situation and the desired EHR security requirements in Iran. The following areas need to be taken into account:

(A) in pivot of health information security organization:
    1- Management liability to information security and allocation responsibilities.
    2- Access control of third-party when implementing IT projects.
(B) in pivot of assets classification and control security:
    1- Accounting all of information technology assets of organization and determining an owner for them.
    2- Information classification as private health information in three classes as follows:
        – First class; internal access level including administrative information.
        – Second class; confidentiality of inter-organization information, including financial information.
        – Third class; secret information including diagnostic and treatment information.
(C) in pivot of human resources security:
    1- Including security requirements in job responsibilities and training of staffs.
    2- Reporting all of security incidents.
(D) in pivot of communications and operations management security:
    1- Use of firewall to protecting network systems.
    2- Use of anti-harmful codes to protecting information files.
    3- Doing regular back-up of information.
    4- Use of public key infrastructure.
    5- Performing Audit logging.
(E) in pivot of development and maintenance security:
    1- security of system files and cryptographic controls by:
        – developing secure layer to medical sciences database and;
        – Information storage to encoding format in database and providing decoding key for security manager.

With regard to stated issues, the healthcare industry in Iran has much to learn from the studied countries as it has began to move toward electronic health records and a nationwide health information network. There are many concerns on how information networks will protect data. Consumers will be watching the healthcare industry to see how well it implements EHR security requirements, before they put their trust in a national information network.

The EHR security requirements should ensure that technical and administrative measurers have to be taken in order to achieve the objectives of data protection and security. Using proposed comprehensive model and enacting, auditing and modifying security standards by the officials of the Ministry of Health in general and, the 'Statistic and Information Technology Management Sector' of Iran Health Ministry in particular is recommended.

Acknowledgement The authors would like to thank Abbas Zare-ee from the English Department, University of Kashan for editing the manuscript.

Conflict of interests No conflicts of interest have been declared.

References

1. National Electronic Health Records taskforce [Internet]. A health information Network for Australia. 2000 July-[cited 2006]. Available from: http://www.health.gov.au/internet/hconnect/publishing.nsf/content/7746B10691FA666CCA257128007-B7EAF/$File/ehrrept.pdf.

2. Lyons, R., Payne, C., McCabe, M., and Fielder, C., Legibility of doctor's hand writing: quantitative comparative study. *BMJ*. 317:863–864, 1998.
3. Woodward, B., The computer-based patient record and confidentiality. *N. Engl. J. Med.* 333:1419–1422, 1995. doi:10.1056/NEJM199511233332112.
4. Aspen Reference Group, *Health information management manual*, 1st ed. Aspen: Maryland, 1999, p. 5:1.
5. Van der Haak, M., et al., Data security and protection in cross institutional electronic patient records. *Int. J. Med. Inform.* 70:117–130, 2003. doi:10.1016/S1386-5056(03)00033-9.
6. Zahedifar, R., Study rate of respect for patients Rights in Medical Records Units of Isfahan University of Medical Sciences [Thesis]. Medical Information Management Faculty, Tehran: Iran University of Medical Sciences, 2002.
7. Salahi, M., An Investigation on Conditions of Storage and Retrieval of Patients' Medical Records in Teaching Hospitals of Iran University of Medical Sciences and Their Comparison with National Standards and Standards in the US. [Thesis]. Medical Information Management Faculty, Tehran: Iran University of Medical Sciences, 1998.
8. HIMSS [Internet], 2004 HIMSS National health information infrastructure survey; 2004 July-[cited 2006]. Available from http://www.himss.org/content/files/2004.
9. Canada Health infoway [Internet], Infoway pan-Canadian EHR survey phase. I. Results and Analysis; 2003 January-[cited 2006]. Available from: http://www.canadahealthinfoway.ca/pdf/EHR-survey-phaseI.pdf.
10. Bitaraf, E., Riazi, H., and Fathi Roodsari, B., *Comparative study of Electronic Health in the word*, 2/2 ed. Ministry of Health and Medical Education: Tehran, 2007, p. 398.
11. Riazi, H., Fathi Roodsari, B., and Bitaraf, E., *Electronic health record, concepts, standards and development approaches*, 1st ed. Ministry of Health, and Medical education: Tehran, 2007, p. 125.
12. Cornwall, A. [internet]. Electronic health Records: An international perspective; 2002-[cited 2006]. Available from: http://www.home.vicnet.net.au.
13. Gupta, A. K. [Internet]. How to protect Your Data when you are on the web. 2008 Apr-[cited 2009]. Available from: http://www.aafp.org/fpm/20080400/29howt.html-.
14. Itiran [Internet], Looking to progress path of electronic health records. 2008 Oct-[cited 2009]. Available from: http://itiran.com/?type=article&id=9999.
15. Commonwealth Department of Health and Aged Care [Internet], The benefits and difficulties of introducing a national approach to electronic health records in Australia; 2002 April-[cited 2006]. Available from: http://www.health.gov.au.
16. Commonwealth of Australia [Internet], International approaches to the electronic health record; 2003 January-[cited 2006]. Available from: http://www.healthconnect.gov.au/internet/hconnect/publishing.nsf/Content/43598FE37A3E7270CA257128007B7EB7/$File/v3-1.pdf.
17. National committee on vital and Health statistics [Internet]. Information for health; 2001 November-[cited 2006]. Available from http://www.ncvhs.hhs.gov/nhiilayo.pdf.
18. Behnam, S., A Comparative Study of Accessibility levels and confidentiality of Medical Records in Selected Countries [Thesis]. Medical Information Management Faculty, Tehran: Iran University of Medical Sciences; 2005.
19. CIHI [Internet]. Privacy and Confidentiality of health information at Canadian institute for health information; 2002-[cited 2006]. Available from: http://www.secure.cihi.ca/cihiweb/en/downloads/privacy_policy_priv2002_e.pdf.
20. Department of Health and Human Services [Internet]. 45CFRparts 160,162 and 164 Health Insurance Reform: security standard; Final Rule; 2003 February-[cited 2009]. Available from: http://www.hipaa.org.
21. Canada Health infoway [Internet]. Electronic Health Record privacy and security Requirements; 2005-[cited 2006]. Available from: http://www.canadahealthinfoway.ca.com.
22. ABC pty Ltd IT Services [Internet]. Information Security Controls and procedures manual; 2006-[cited 2006].Available from: http://www.maralan.com.au.
23. NHS [internet]. IM &T security policy; 2004 Nov-[cited 2006]. Version 1.1. Available from: http://www.northumberlandcaretrust.nhs.uk.
24. Mohammad pour A. A Comparative Study on the Hospital Standards of Ministry of Health and International Standards of Joint Commission on Accreditation of Hospital [Thesis]. Medical Information Management Faculty, Tehran: Iran University of Medical Sciences; 2006.
25. AHIMA [Internet]. The state of HIPAA privacy and security compliance. 2006 April-[cited 2009]. Available from: http://www.ahima.org/emerging_issues/2006statefHIPAAcompliance.pdf.
26. Schaectel, D., *How to build safety management system*, 1st ed. Professional Safety: USA, 1997.
27. Schackow, E., Palmer, T., Epperly, T. [Internet]. How to protect your patient Data. 2008 Jun-[cited 2009]. Available from: http://www.aafp.org/fpm/20080600/a3ehrm.html-.

Record: 1

Title: Providers rate what's hot and what's not.

Source: Modern Healthcare; 3/1/2010, Vol. 40 Issue 9, p32-32, 1/2p

Document Type: Article

Subject Terms: *INFORMATION technology
*MEDICAL informatics
*DATA security
*DATA warehousing
*INDUSTRIAL surveys
UNITED States. American Recovery & Reinvestment Act of 2009

Geographic Terms: UNITED States

Abstract: The article reveals the findings of "Modern Healthcare's" annual health information technology (IT) survey on the popular things in healthcare information technology. Fifty-eight percent of survey respondents stated that they want to see that the meaningful-use criteria of the American Recovery and Reinvestment Act of 2009 be met. Among the top IT priorities survey participants have in mind include electronic health records, data privacy and security and data warehouses.

Full Text Word Count: 448

ISSN: 01607480

Accession Number: 48445798

Database: Academic Search Complete

Section: Special Feature

Providers rate what's hot and what's not

What's the hottest thing in healthcare information technology? That s just what we wanted to know.

Modern Healthcare asked respondents to its annual health IT survey to select their top three "hot button" priorities from a list of 21 technologies.

OK, no shocker here: Meeting the meaningful-use criteria of the American Recovery and Reinvestment Act of 2009 was the people's choice by a landslide, chosen as one of their three picks by 58% of survey respondents.

But what about the other IT priorities respondents selected? As it turns out, seven others out of the top 10 will help providers clear meaningful-use hurdles: electronic health records (50%); clinical communications infrastructure and ambulatory clinical IT systems (both at 26%); inpatient systems (22%); data privacy and security, (16%); information exchange (14%); and data warehouses (12%)

(View chart at ModernHealthcare.com).

The two outliers in the bunch:

* Consolidating all IT functions using common applications, chosen by 19% of respondents and ranked No. 6 on the hot-button list.

* Physician practice management systems, selected by 15% of participants and ranked No. 8.

Thus, eight of the top 10 "have something do with: 'You've got to put EMRs in; you've got to get meaningful use out of them; you've got to get the data out of them,'" says Dave Garets, president and CEO at HIMSS Analytics, the IT market research subsidiary of the Healthcare Information and Management System Society. "I'm not even remotely surprised by this."

The relatively low ranking in the survey of some IT projects--particularly others also required to meet meaningful-use targets--was a bit disconcerting, however, given all that's on the federal IT agenda, according to Garets.