Information Security Requirements for Implementing Electronic Health Records in Iran

Amir Ashkan Nasiripour
Associate Professor, Department of Information Technology Management, Electronic Branch, Islamic Azad University, Tehran, Iran
drnasiripour@iauec.com

Somayeh Hamzeh
Master of Art, Department of Executive Management, Science and Research Branch, Islamic Azad University, Tehran, Iran

Sina Golesorkhi
Master of Science, Department of Information Technology Management, Electronic Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

Background and Goal: ICT development in recent years has created excellent developments in human social and economic life. One of the most important opportunities to use information technology is in the medical field, that the result would be electronic health record (EHR).The purpose of this research is to investigate the effects of information security requirements in electronic health records and importance and priority of each of them in this project deals with Iran.

Methodology: this research is a descriptive-survey in nature and was conducted on December 2009 to December 2010. Its statistical population was comprised of experts and professionals of health industry of the country who had work record in Health Electronic. 83 people were selected to answer the questionnaires. One-way test was used to analyze data. After their effect was proven using variance analysis and Shefe test, their priority was evaluated through SPSS16.

Findings: Information safety criteria in Health Electronic Records fell into four categories. Security variables with average of 4.10 and access control 3.26 have highest and lowest importance, respectively, from experts' point of view. Personnel security 3.96, management of activity continuation when facing loss 3.99 and physical and environmental security (4.52) stand in third and fourth ranks. Communication management and exploitation (3.71) takes jointly second and third ranks. System support and development (3.58) took the second rank.

Conclusion: All criteria of organizational security that include , personnel security, physical security, communication and exploitation management, access control, support and expansion system; and compliance with law are effective on implementation of EHR (Electronic Health Care) in the country. Public trust toward the privacy of their medical records in EHR can be increased through observing privacy of people's information, ability to monitor and prosecute any offense, observance of moral and legal standards and providing a system that can identify attack on EHR.

Keywords

Electronic health record, information security, heath card.

1. INTRODUCTION

Advancement of communication & information technology brought about remarkable development in a great variety of sciences, industries and services and caused emergence of new areas such as e-government, e-learning and e-health. Vast information is produced in businesses area, and doing many affairs to process overwhelming bulk of information. Management of this information has come to be increasingly a difficult task necessitating the utilization of information technology in information management [12]. Health care scope in an area which deals with a vast bulk of information because it renders services to every single member of the community has no choice but processing a vast amount of information. While many

detailed cases are opened only to maintain and supervise certain places and facilities, little attention is paid to maintaining and improving the health care records of the community members. Almost all physicians are of the opinion that considerable part of the medical/care records of the patients is not available to them [9]. Information technology is considered as a decisive solution in implementation of the main strategies of this domain into. Therefore, e-health, as a great foundation of e-government, can pave the way for solving many dilemmas which health care currently faces [11].

From ISO perspective, an EHR must essentially be updated, reliable, complete, precise, safe and available and also must be designated in such a manner that is of sufficient capacity to provide complete set of health care services, regardless of the type of model they may use. Designing such records can be traced back to traditions, language and culture of a particular region. E-health records must not be created only for patients, but they must be created and used for investigation on social diagnosis for all members of community as well. Such EHR must focus mainly on people health. They must be able to cover all people, whether they are patient or in healthy condition [5].

EHR knows how to distribute people's health care information, and is in need of ratification and compatibility in a region to a common information model by compatible systems, and ratification of relevant international standards [3]. There must be constrains on granting EHR Meaningful Standards Development permissions in order to determine what things must/must not be taken into account when carrying out standardization process. Structure of EHR must be designed in a way that can support the entire applications common in health care domain [15]. Electronic Health Records is composed of EHR system, E-Prescription, Telemedicine, Telehealth, and E-booking [14]. In Iran, the concept of EHR is:"a set of information relating to individuals' health condition, from before birth (including information of embryo period and its prior time-such as information of laboratory fertilization) to after death (such as information of place of burial and etc.). such information are saved electronically with time, and when they are required, whole of part of them can be available to relevant individuals, regardless of time and place" [2].

EHR is an important discussion in e-health, since there are many other innovations and works which deal with such a system, such as health card, tele-medicine, geographical information systems for health care system as well as decision-maker systems. Furthermore, this is a specialized system which is essential for health care management in various layers and levels. In fact, EHR is a fundamental infrastructure to fulfill the above-said matters and maintaining their integration [4].

In study on a rural area in Southern Georgia, a team comprising of several specialties and 27 medical teams and 75,000 active patients evaluated the economic impacts of utilization of EHR. According to the study, net profit which is gained from EHR amounts to $2.5m per annum and $12.7m during give years. Prior to implement this project, average income of the physician was $382; while, it rose to $ 444 and number of employees needed to register details in the cases increased nearly 60% after implementation of such project [13].

In spite of the mentioned advantages, this project has also certain disadvantages including privacy and reliability [10]. When a technology develops and its applications start to increase in various areas, some misuses may happen and it may also be utilized in negative, demagogues and immoral purposes. EHR is not an exemption [7]. The biggest danger which encounters EHR system, in terms of privacy and security, is lack of sufficient knowledge and instructions. Clear instructions and operational rules and regulations constitute the base of security in an information system [8]. This study aims at testing and evaluating the impact of current requirements of information security in EHR system of Iran. In addition, the existing international standards in medical information security are posed in order to make attempt to localize them and provide sufficient solutions and security alternatives to ensure the managers and users of health care services that EHR could be an effective system in Iran.

2. MATERIALS & METHODS

This is a descriptive-survey study in applied objective. Its statistical population contains professional experts and academic professors of Ministry of Health and Treatment as well as Basijian Health Care Institute and Social Security of Tehran province. It is entirely composed of 83 individuals. For gathering data, two methods were used, library method and field method in December 2009 to December 2010. Library method was used in writing style of the study and field method was used to gathering data and achieving results. Questionnaires containing 28 questions and the measurement scale instrument was Likert 5-choice scale (1= very low, 5= very high) that were used as means for gathering data. The interviews were conducted in person. The validity of the questionnaire was measured through content validity. The internal consistency was measured through Cronbach's alpha which was equal to 0.74 . Due to lack of sufficient flexibility of library sources and the long distance between Iran and progressive countries in terms of information security infrastructures, experiences and knowledge of experts and managers were additionally used.

To analyzing data, was used SPSS 16 software. this research deals with information security requirements for EHR based on variables of organizational security, personnel security, physical security, communication and exploitation

management, access control, system support and expansion, compliance of law and reliability. At first, the impact of such variables were evaluated separately: organizational security, personnel security, physical security, communication and exploitation management, access control, system support and expansion, compliance of law constituted the first hypothesis and reliability constituted the second hypothesis of the research. Meaningfulness Disparity Test was carried out between variables forming the hypotheses of the research in order to discover the influence of each one of the said variables on the hypotheses based on variance analysis, which eventually was discovered using multiple regression model. T- Test was used as meaningfulness test of the effect of variables on information security requirements in EHR. Tests were carried out in meaningfulness level of 0.05 , and acceptation or rejection of such an effect was done based on p-value. "Normality of data" was one of the assumptions of the one-way T-Test. Therefore, such normality was determined before acceptation or rejection. Whether there is any meaningful difference between the criteria which were posed about information security requirements in EHR, based on experts' opinions and which difference, in any, takes priority to be studied was evaluated using Scheffe test.

3. RESULTS

Findings of this research indicated that in reliability level of 95%, the effect of implementation of information security requirements in development and improvement of EHR can be accepted. That is, implementation of such requirements exerts influence on putting EHR system into operation. On the other hand, the variables such as personnel security, physical security, communication and exploitation management, access control, system support and expansion and compliance of law are effective on information requirements for EHR because meaningfulness level of each one of them is less than 0.05. furthermore, when reliability level is 95% the effect of design and implementation of a proper security solution for preserving medical records of individuals on increased reliability of the medical network can be accepted. It means that implementation of such requirements increases the reliability of medical network resulting in support of this project inside the country. Further, average value of each one of the said variables has a meaningful difference with "3" and is more than 3. Therefore, the effect of the variables on determination of the information security requirements for EHR is high (Table 1).

Table 1. The average and sig of variables

Variables	Mean	Sig
organizational security	4.11	0/000
personnel security	3.96	0/000
physical security	4.02	0/000
communication and exploitation management	3.72	0/000
access control	3.27	0/000
system support and expansion	3.58	0/000
compliance of law	4.00	0/000

The effectiveness level of Shefeh test was found to be less than 0.05 indicating that average of these groups are not equal and they have meaningful difference. Also the results of variance analysis indicated that information security criteria of EHR fall into four categories: organizational security with average of 4.10 and access control 3.26 have highest and lowest importance, respectively, from experts' point of view. Personnel security 3.96, management of activity continuation when facing losses 3.99 and physical and environmental security (4.02) stand in third and fourth ranks. Communication management and exploitation (3.71) takes jointly second and third ranks. System support and development (3.58) took the second rank (Table 2).

4. DISCUSSION & CONCLUSION

According to the research, variables of organizational security, personnel security, physical security, communication and exploitation management, access control, system support and expansion, compliance of law and reliability have influenced information security requirements of EHR. Studies have been carried out in Britain which indicates that Health Services System has prepared a ten-years program aiming at modernizing the health care system. In September 1998, "Information for Health of Information Strategy for Modernizing (NHS) 1998-2005" document was published. In this document "Information Strategy" means to ensure utilization of the information for the purpose of providing best health care services. The Strategy intends to have sufficient amount of information to make relevant decisions in health care domain. In designing and implementing systems which are needed certain principles must be taken into account which are information have individual – based nature, systems shall be integrated, information shall be safe and reliable, and information shall be shared throughout NHS. In this country, to set up a HER, six stages have been designated for ERPs which include: Stage one: management of the patients' affairs and independent systems. Stage two: stage one plus integration through patient comprehensive imaging. Stage three: stage two plus digitalization of the clinical instructions, results report, prescription and integrated care by physicians. Stage four: stage three plus access to information

banks, including the instructions, warnings, electronic regulations, supporting specialized systems. Stage five: stage four plus clinical special modules, imaging the documents. Stage six: stage five plus tele-medicine and other multimedia applications (such as PACS). Access to these stages has been planed through a seven – year schedule in three stages (1998-2005). In Sept. 18, 2002 final document of evaluation of the technical structure of the pilot project was published in which both advantages and disadvantages had been assessed and relevant recommendations had been given. In the meantime, an information bank was created from the experiences gained from each project in order to pave the way for the future activities[1].

Table 2. Grouping variables

	Subset for alpha = 0.05			
Variable	**1**	**2**	**3**	**4**
Access control	3.2685			
System support and development		3.5839		
Communication management and exploitation		3.7156	3.7156	
Personnel security			3.9600	3.9600
lowest importance			3.9977	3.9977
Physical security			4.0222	4.0222
Security variables				4.1091
Sig	1.000	.890	.056	0815

Another research which was carried out in Canada indicates that Canada has a good record of innovations in rendering health care services. From beginning of 90s, health care officials have been searching for ways to make best use of information technology in modernizing public health care services network. In 1994, Canadian Institute for Health Information was founded. The Institute provided its strategy on Feb., 1999 which is based on empowerment of people to make conscious decisions about their health conditions, rendering integrated services, observance of privacy and emphasizes on fundamental role of information, relevant and timely information for decision-making, service superiority, responsibility and understanding the health indices. In Dec. 2000, five components of EHR which were organizations and people, processes, information and standards were identified and the scope of work which was compiling standards of National EHR, policies and regulations on privacy, c coordination operation in all regions were determined [1].

Findings of this research indicate that organizational security takes higher priority, much more focus must be made on EHR. For this purpose, it is recommended to set up a body under the name of information security management committee to coordinate information security and define the responsibilities and powers of each person. As to the physical security, safe places must be designated for maintenance of the information. Offices, medical offices, rooms etc need to be equipped with efficient security instruments. Places where information are loaded and discharged must essentially be separated from medical centers. Different facilities such as information maintenance sites, feed sources and cables must be entirely safe.

Compatibility with legal requirements is possible through knowing the laws in effect, follow-up to ratify new regulations, assessment of coding laws, registry of impermissible accesses to prove offences of offenders. The systems must also be controlled and equipped with discrimination means. On personnel security, it is recommended to determine the security considerations in job responsibilities of each employee. Personnel must receive training before starting their jobs. Incidents and malfunctions should be reported. Disciplinary procedures must be laid down to prevent disciplinary offenses, and the logical punishments must be defined for the offensive physicians.

It is necessary to document all activities, to separate the functions and duties of each employee and to separate the pilot facilities and developing facilities from each other. Security can be achieve through managing portable media, removing useless media, preserving security of the system documentary and e-mails in supporting media. In order to control access, equipments which are not possible to monitor through special software. Real access of users must be reviewed and users' options must be managed in regular intervals. Proper security models must be used in passwords. Network accesses including users' identity, user terminal up to server, all hardware connected to network and connection routs must be controlled. Safe entries to operating system, authentication of the users, creating system alarm when facing dangers and time limit for busy and unsafe departments, access control to operating system must be carried out appropriately.

It is recommended that managerial processes such as user registry, accesses level management, user password management, etc. must be done in users access (personnel and physicians). All security events must be registered and processes in system carefully. Internal processes, requests authentications etc. About the patients' cases must be carried out in order to develop and support the system. Study on possibility to change the operating system and control of hidden channels through experts during development and security support processes must be conducted by providing relevant instructions to control any changes. Coding con-

trols including coding policies, codes credits and utilization of digital signatures in prescriptions and the measures which must be taken in urgency situations should be done properly. On solutions to fight against test crisis, maintenance and reevaluation must be carried out in order to exert activity continuation management when facing losses.

All things considered and paying special attention to information security requirements in implementation of EHR, we recommend: To implement a system which can identify any attack on EHR aiming at improving the public trusts to the system. To avoid overall changes in system, security Archetypes must be designated in EHR. It is noteworthy that in an era which puts high value on scientific studies and researches, need to set up and operate strong, comprehensive information networks and implement an EHR library project is an inevitable necessity.

REFERENCES

[1] Bitaraf, E., and H Riazi. 1998. Comparative Study of Electronic Health in the world, 1: 129-31.

[2] Raimund, V.,and W Florian. 2009. Architecture for a Distributed National Electronic Health Record System in Austria, 45-6.

[3] Torabi, M.,and R Safdari. 2010. Electronic Health Record, Tehran, Iran. 21-2.

[4] Stophen, N., 2004. Record, Document, Massaging & Data Standard/Architecture – Comparative Study – Report to the Information Standards Advisory Board, 46-8.

[5] Bill, T., 2009. Appearance health information standards, 77-9.

[6] www.gehr.org

[7] ADEN, T., and J RIESMEIER. 2009, A survey and Analysis of Electronic Healthcare Record Standards, 88-9.

[8] Heard,S., .2003. Template and Archetypes: how do we know what are talking about? Version 1.2.

[9] Kia, U., and M.D Heitmann. 2010, HL7 Clinical Document Architecture (CDA) – Introduction of the Clinical Document Architecture Release in Germany – The Sciphox experience, 86-7.

[10] Bird, L.2003, ISO TC 215 – 13308 – Health informatics – Requirements for an Electronic Health Record Architecture, 76-7.

[11] http:// www.cchit.org/

[12] Heard, S., 2009. E-Health in Europe, 65-7.

[13] Warren, J., and A Barretto. 2007, Linking Guideline to Electronic Health Record Design for Improved Chronic Disease Management, 88-9.

[14] Eichelberg, M., and J Riesmeier. 2009, A Survey and Analysis of Electronic Healthcare Record Standards; ACM Computing Surveys, 90-1.

[15] Laleci, B., 2006. a Survey on the Analysis of Electronic Healthcare Standards; eHealth StakeHolders meeting Brussels. http://www.srdc.metu.edu.tr/stakeholder_group/public-docs/ride-analysis-her-standards.pdf