HEALTH INFORMATION SECURITY: A CASE STUDY OF THREE SELECTED MEDICAL CENTERS IN IRAN

Nafiseh Hajrahimi1, Sayed Mehdi Hejazi Dehaghani1, Abbas Sheikhtaheri2
Department of Medical Informatics. Faculty of Health Services Management and Medical Information Sciences, Isfahan University of Medical Sciences (IUMS), Isfahan, Iran1
Department of Health Information Management, School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Iran2

Corresponding author: Sayed Mehdi Hejazi. Department of Medical Informatics, Faculty of Health Services Management and Medical Information Sciences, Isfahan University of Medical Sciences, Isfahan, Iran. E-mail: hejazi@mng.mui.ac.ir

1. INTRODUCTION

Nowadays most of modern health systems are based on the computer networks to transfer data among users inside and outside of the health care center (1-10). Legislation is needed, to manage access to computer networks resources. With this tool access control policies can be managed in the therapeutic organizations. Health care sector has changed a lot in providing health services. The changes made through the Internet and mobile technologies include remote health monitoring, counseling, on-line, e-clinics ports, access to patient’s information and tracking of individuals. Given these changes, it is predicted that by 2014 electronic health records (EHR) will be universal and will fit all health maintenance organizations (8). Based on a recent study the US has been able to save up $1 billion dollar using this electronic approach (11). Information technology has invested in health care, but it made much less than the income earned in other industries. The evidence shows that the reason was insufficient security indicators and breach in data security and unfortunately the results were patients’ dissatisfaction, psychological distress and social stigma (10). Advances in information technology and its compatibility with the healthcare industry have been led to progress in health care, higher quality, health care lower cost and advances in medical science. But they have led to increased potential information security risks (6). Also, the growth of digital medical records has made the medical identity theft as a magnet for hackers. In addition a recent study in America showed that 75% of patients are concerned about unauthorized disclosure of their confidential information and to share them on Web sites (12-24). Conscious disclosed medical information is the second created security gap (9). Considering the results of previous studies, it was found that most researchers are interested in the integration of different disciplines together. For example, the integration of psychology and sociology to explore the role of employees in information security risk management (1, 6, 17-22) or economic integration with the information systems to identify the investment decisions (23-25). Unfortunately, little research sought to examine the risks and security gaps in health information systems while the need here felt more than other industries.

1.1. Literature review

Khin Than Win in his study concluded that information security enhances the patient confidentiality and leads to the public interest for EHR use. He drew the conclusion that Security technology is not fully accountable to achieve these goals.
and a lot of studies are still needed in this area (24). Fernando and Dawson began to study clinical privacy and data security. For this purpose 26 medical centers were studied. They found security vulnerabilities in health information systems and showed that considering them can be effective in security control of health care centers. In this study, researchers examined the techniques involved in the software implementation of health information systems. In this paper, a set of software techniques have been studied for user identification and authentication of access control. Encryption is introduced as a powerful tool to support the storage and transfer of data (15). In a study entitled “the impact of data security and privacy on remote health care applications”, the researcher defines the role of security and privacy in faster and better development of this technology. Telemedicine provides any medical care through an active media such as the Internet, mobile and satellite. Using telemedicine devices largely depends on the system security (25).

As part of the IT industry Cloud Computing is making rapid progress. Along with benefits of this technology credit risks exist. Thus, in this study the security and privacy risks and Cloud Computing have been discussed (19). In the security of health information study some researches were found with a focus on technological solution to protect the privacy of patients in the wired and wireless networks of a medical center (12). Other studies have investigated the impact of HIPAA standards (7, 21). Recently, many studies are oriented on new methods, such as methods based on quantitative research, economic analysis, and statistical models of patient privacy, public policy, risk management and the impact of Health Information Technology on medical errors (2, 14). To check the quality of healthcare provided with the aid of two AHP and TOPSIS approaches, two studies were done entitled “Quality of health care services by using fuzzy AHP approach” and “approach combining the fuzzy AHP and fuzzy TOPSIS based on strategic review of electronic services quality in the health care industry” (3, 4).

2. METHODOLOGY

Based on the objective this research is, research–practical. In this study preliminary data collection is through a questionnaire. The study population included IT management staff in medical centers, IT management experts in Isfahan University of Medical Science and scholars in this field. In this study to assess the safety of patient health information, 3 medical centers (Amin hospital, Chamran Hospital and Al-Zahra Hospital) were chosen (that their HIS is under Windows and some under the Web produced by various companies). The sample is composed of 40 people. Scientific validity of the questionnaire was determined by group of academic experts. The reliability of the questionnaire was calculated around 0.916 using Cronbach’s alpha. The information security evaluation in each medical center was calculated with a hybrid model of fuzzy AHP and TOPSIS.

2.1. Multi Criteria Decision Approaches

Decision-making is a multi-criteria mathematical model and refers to a problem-solving approach which is used to choose one option among a limited number of options (17). MADM methods are known to facilitate the application procedure and compound approaches can preserve this strength and create multiple sources of knowledge (18). To achieve more efficient decisions, this study uses compound AHP and fuzzy TOPSIS approach so that each approach compensates for the weaknesses of the other.

The underlying logic of TOPSIS method was to define the positive ideal solution and negative ideal solution (23) and is based on the fact that the option selected has the shortest distance from the ideal solution. Positive and negative ideal solution is a hypothetical solution in which all index values are similar to the maximum and minimum index values in the database (17). In summary, the positive ideal solutions are the best available measures of values and negative ideal solution are the worst available measures of values (23). Because the measured variables are the language variables, we use the theory of fuzzy AHP. Five-point Likert scale is the range of each question. For each option (very high, high, moderate, low, very low), a triangular membership function is defined in the range of zero to 100, which is shown in Table 1. Then, the procedure is explained step by step.

Health information security evaluation framework is shown in Figure 1.

| Value | Membership function | Five-grade Likert |
|-------|---------------------|------------------|
| 9     | (40,70,100)         | Very High        |
| 7     | (30,60,90)          | High             |
| 5     | (20,50,80)          | Average          |
| 3     | (10,40,70)          | Low              |
| 1     | (0,30,60)           | Very Low         |

Table 1. Membership function of triangular fuzzy numbers

**Step One:** Determine the index of fuzzy numbers based on the principle of expansion. At this stage, the numbers are added together and the average is calculated.

\[ E_{ij} = \frac{(E_{i1} + E_{i2} + \ldots + E_{in})}{m} \]

**Step Two:** Each value can be displayed as a triangular fuzzy number.

\[ E_{ij} = (L_{ij}, M_{ij}, U_{ij}) \]

**Step Three:** Three-point triangular number is calculated as follows:

\[ LE_{ij} = \frac{\sum LE_{k}}{m} \]

\[ ME_{ij} = \frac{\sum ME_{k}}{m} \]

\[ UE_{ij} = \frac{\sum UE_{k}}{m} \]

**Step Four:** Change fuzzy values into defuzzy ones based on the center.

\[ CA_{ij} = \frac{(\sum ME_{ij} - LE_{ij}) + (ME_{ij} - LE_{ij})}{3} + LE_{ij} \]

**Step Five:** Then use the TOPSIS method.

**Step Six:** Determine the positive ideal solution \( V_j^+ \) and negative ideal solution \( V_j^- \):

The best values for each matrix index vector \( v + j = v \)

Worst vector-matrix values for each index \( v + j = v \)

**Sixth step:** Calculate the each variable distance to positive and negative ideals.
Calculating the Euclid distance of each alternative to the positive ideal 
\( (v_j - v_i) + 2\Sigma d + 1 = \sqrt{ } \)
Calculating the Euclid distance of each alternative to the ideal negative 
\( (v_j - v_i) - 2\Sigma d \)

**Step Seven:** Determine the relative proximity (CL *) of an alternative to the ideal solution:

\[
CL^*_i = \frac{d_F - d_i}{d_F + d_i}
\]

**Step Eight:** Rating Options: Any option that has a larger CL* is better.

### Determining the indicators of health information security

Based on studying the literature and interviews with the designers and managers of health information systems, 27 indicators were selected which are shown in Table 2. In the next step, to identify effective criteria, a questionnaire with a range of five-point Likert scale was created and distributed then was analyzed by test. Among the 27 indicators, 7 indexes gained points more than 3 (values less than three are not importance) and were selected as effective indicators which are shown in Table 3.

#### The used model

For each variable, there exist answers based on the number of respondents which has a triangular fuzzy number. Table 4 shows the fuzzy performance criteria. So far the weight of each indicator and security situation of each center based on each index was determined. Because the performances are in a form of fuzzy, these values must be Defuzzy. To turn fuzzy numbers into a certain number, (area center)

### Table 3: Impact indicators

| Impact indicators          | Safety Equipment | Verification and system design | User access management | Network access control | Cryptographic controls |
|---------------------------|------------------|--------------------------------|------------------------|------------------------|-----------------------|
|                          |                  |                                |                        |                        |                       |

#### Table 2: Indicators of health information systems security

Based on studying the literature and interviews with the designers and managers of health information systems, 27 indicators were selected which are shown in Table 2. In the next step, to identify effective criteria, a questionnaire with a range of five-point Likert scale was created and distributed then was analyzed by test. Among the 27 indicators, 7 indexes gained points more than 3 (values less than three are not importance) and were selected as effective indicators which are shown in Table 3.

#### Table 3: Impact indicators

| Impact indicators          | Safety Equipment | Verification and system design | User access management | Network access control | Cryptographic controls |
|---------------------------|------------------|--------------------------------|------------------------|------------------------|-----------------------|
|                          |                  |                                |                        |                        |                       |

#### Table 2: Indicators of health information systems security

| Indicators                                                   | Management commitment to safety information | Independent review of safety information | Safety of third-party access | Independent contractor | Independent contractor | Classified information | Audit                                      |
|--------------------------------------------------------------|---------------------------------------------|-----------------------------------------|-----------------------------|------------------------|------------------------|------------------------|---------------------------------------------|
| Safety in the development and support processes              | Safety Equipment                             | Verification and system design           | Functional immune system    | Access control system   | Access control systems | Control access to applications | Audit logging                              |
| Media handling and safety                                    |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Exchange of information                                      |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Audit                                                        |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Access control policy                                        |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| User access management                                       |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Network access control                                       |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Access control systems                                       |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Control access to applications                               |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Functional immune system                                     |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Immune system files                                           |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Safety in the development and support processes              |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |
| Cryptographic controls                                       |                                             | User access management                   | Access control systems      | Control access systems  | Control access to applications | Functional immune system | Audit logging                              |

#### Table 4: Phase performance criteria of three health centers

| Health Information Security Evaluation Criteria | Amin[C] | Shahid chamran [B] | Azhara [A] |
|------------------------------------------------|---------|--------------------|------------|
| Safety Equipment                                | (26.54,23.52,44) | (23.54,42.34,52) | (26.54,35.23,47) |
| Verification and system design                  | (37.95,43.55,35) | (43.54,42.34,52) | (42.34,42.55,35) |
| User access management                          | (27.54,34.42,55) | (23.54,40.55,32) | (34.32,55,42) |
| Network access control                          | (37.54,43,55)   | (42.54,32,45)     | (43.54,55,32) |
| Cryptographic controls                          | (39.54,43,55)   | (42.54,32,45)     | (43.54,55,32) |
| Safety in the development and support processes | (39.54,43,55)   | (42.54,32,45)     | (43.54,55,32) |
| Access control system                           | (53.21,63.22,71) | (35.64,42,35)     | (42.34,56,73) |

#### Figure 1: Information security framework for the study of selected medical centers.
paired comparisons and also critical indicators in related to information security were used in assessment of medical centers information security. By comparing the current results and ranking provided, the strengths of this model are clear. One of the important results of this study prove of superiority in diagnostic ability of a hybrid approach compared with the non-hybrid approach (TOPSIS) is. The comparisons made, using the conceptual model for medical centers and other research institutions in more right decisions will be very useful. The results of this study, information security situation at these centers was determined and each of these according to the ratings they received should consider appropriate measures to maintain or enhance their status.

4. CONCLUSIONS

In the proposed approach, the fuzzy theory was used to determine the security measures. Compound decision model was used in the ranking of selected medical centers (Al-Zahra, Chamran, Amin) and according to that Chamran Hospital was ranked first, Al-Zahra was ranked second and Al-Zahra was ranked third. Medical centers with higher grade should have a convenient way to maintain the security of health information and weaker institutions should try to have more powerful centers. The decision making of the current study in ranking of health care centers was used regarding health safety information. This model can be used in all decisions to rank health care centers.

REFERENCES

1. Baker WH, Rees LP, Tippett PS. Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision Making. Communications of the ACM. 2007; 50(10): 88-97.
2. Basu G, Zahedi FM, Gelen D. The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online. Information Systems proceedings of the conference in America, 2007.
3. Büyüközkan G, Çiçği G. A combined fuzzy-AHP and fuzzyTOPSIS based strategic analysis of electronic service quality in healthcare Industry: expert system with application. 2011; 39(3): 2341-2354.
4. Büyüközkan G, Çiçği G, Güleyis A. Stratification of healthcare cybersecurity using fuzzy-AHP methodology: expert system with application. 2011; 39(8): 9407-9424.
5. Cavusoglu H, Mishra B, Raghunathan S. A Model for Evaluating IT Security Investments. Communications of the ACM. 2004; 47(7): 87-92.
6. Dhillon G, Buckhoust J. Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. Information Systems Journal. 2000; 14(1): 127-143.
7. Ferreira A, Correia R, Antunes L, Palhais E et al. How to Break Access Control in a Controlled Manner. IEEE Symposium on Computer-Based Medical Systems. 2006.
8. Goldschildt PG. HIT and MIS: Implications of Health Information Technology and Medical Information Systems. Communications of the ACM. 2005; 48(10): 69-74.
9. Hasan R, Yurick W. A Statistical Analysis of Closed Storage Security Breaches on a Hospital Information System in Canada. Proceedings of the 11th World Congress on Health Medical Informatics – MedInfo, Brisbane, Australia, 2007.
10. Malin B. A Computational Model to Protect Patient Data from Location-Based Identification. Artificial Intelligence in Medicine. 2007; 40: 223-239.
11. Malin B, Arilds E. Confidentiality Preserving Decision Theory. Communications of the ACM. 2007; 16(1): 130-152.
12. Miller AR, Tucker CE. Privacy, Network Effects and Electronic Medical Record Adoption. Proceedings of the Sixth Workshop on the Economics of Information Security, Carnegie Melon, 2007.
13. Odabi I, Olawasegun S. Data Security in Health Information Systems by Applying Software Techniques. Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS). 2011; 2(5): 775-781.
14. Richter P. Enforcing Privacy through Security in Remote Patient Monitoring Ecosystems. 4th International NSC on Information Technology Applications in Biomedicine, 2007.
15. Rao RV, Davin JP. Decision-Making Framework Models for Material Selection Using a Combined Multiple Attribute Decision Making Method. Journal of Adv Manufacturing Technology. 2008; 35: 751-760.
16. Shih H, Shyu HJ, Le ES. An Extension of TOPSIS for Group Decision Making. Mathematical and Computer Modelling. 2007; 45: 801–813.
17. Sotto Lisa, Treacy Bridge C, McClean Melins D, L. Privacy and Data Security Risks in Cloud Computing, Electronic Commerce & Law Report. 2010; 15: 186.
18. Straub D, Collins RW. Key Information Liabilities: Issues Facing Managers of Software Piracy, Proprietary Databases, and Individual Rights to Privacy. MIS Quarterly. 1990; 14(2): 143-156.
19. Terry NP, Francis LP. Ensuring the Privacy and Confidentiality of Electronic Health Records. Dissertation. University of Illinois, Law Review. 2007; 68375.
20. Vaae E. Danger is in the Eye of the Beholders: Social Representations of Information Systems Security in Healthcare. Journal of Strategic Information Systems. 2007; 16: 130-152.
21. Wang YJ. Applying FMCDM to Evaluate Financial Security Evaluation. Systems proceedings of the conference in America, 2007.
22. Won K. A review of security of electronic health records, Health Information Management. 2005; 340(1): 13.
23. Zaidan BB, Zaidan AA. Impact of data privacy and confidentiality in developing telemedicine applications. International Journal of Pharmacology. 2011: doi:10.3923/ijp.