Indian Journal of Science and Technology, Vol 8(21), DOI:10.17485/ijst/2015/v8i21/79090 September 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Effects of Security Policies, Security Awareness of Hospital Employee to Patients' Personal Information Protection

Sung-Soo Kim* and Kyu-Ho Jeoung

Department of Healthcare Management, Cheongju University, Cheongju, South Korea; mra7033@naver.com

Abstract

With the development of hospital information systems and digitalization of patient records, the importance of protecting patient information is steadily increasing. In order to develop policies for patient information protection, this study conducted empirical analysis on the effects of security policies, security awareness and employees' individual characteristics on security effectiveness in local public hospitals. The results indicated that security policies have a significant effect on security awareness and individual characteristics, but have no effect on security effectiveness. Therefore, it is important to establish security policies that can positively affect security effectiveness. This study also suggests additional multilateral research on administrative security factors.

Keywords: Hospital Information Systems, Security and Privacy, Security Awareness, Security Effectiveness, Security Policies

1. Introduction

With the development of computer technology, hospital information systems are rapidly changing. Information in hospitals consists mostly of patient information[1]. Patient information is stored in hospital information systems such as Electronic Medical Record (EMR), Order Communication System (OCS) and Picture Archiving and Communication System (PACS). As patient information includes very sensitive information such as diagnosis and treatment of disease, family history and genetic information, outside leakage of this information can cause more severe damage than other kinds[1, 2]. Since a huge amount of patient information is managed in digitalized form, the necessity of information protection is increasing[3, 4].

U.S. legislated and has applied the Health Insurance Portability and Accountability Act (HIPAA) to patient information[5]. Organization for Economic Cooperation and Development (OECD) countries and Japan manage patient information with private information protection rules without specialized laws for patient information protection[6]. Korea is now in the process of legislating the "Protection and Use of Health Information Act" and has permission for information exchange among medical institutions, following patient consent, ahead. However, studies on information protection in medical institutions have left much to be desired. Thus, with the importance of patient information increasing and studies falling short of those in other industries, studies on patient information are highly required.

Medical institutions are workplaces where various tasks are performed for patients. With the development of medical information systems, accessibility to patient information is also increasing. Given this reality, it is very urgent to implement safe management of patient information[7]. Thus far, studies on patient information protection have been mainly conducted on technological aspects. However, with the specificity of the contents of patient information, administrative security is vital. Consequently, it is very meaningful to conduct a study on government operated local public hospitals immediately

* Author for correspondence

prior to the legislation of Protection and Use of Health Information Act. Hence, effective policy studies for patient information protection in public hospitals established in major cities across the country are expected to have an enormous spillover effect. Therefore, this study conducted empirical analysis on the effect of security policies, security awareness and individual characteristics of medical institution employees on security effectiveness. By investigating whether medical institutions' security policies change security awareness and personal characteristics and verifying if security policies and security awareness bring about security effectiveness, this study intends to utilize the results as basic material for the establishment of effective security policies in medical institutions.

2. Theoretical Framework and Study Hypotheses

Information protection refers to protecting existing system information from opening, altering, destructing and delaying, intentionally or by mistake[6]. In this information-oriented society, information security should start from information users' awareness of the importance of information protection in all organizations.

In medical institutions, patient information is mainly generated during the process of diagnosing and treating diseases. Thus, patient information refers to information, generated during treatments, related to patients' health condition that is used to judge the need for health care provision and providing health care[8].

Information related to patients' health is very sensitive compared to that in other fields, and should thus be protected as a human right. Additionally, in medical institutions, written patient records are disappearing as the result of the introduction of various hospital information systems including EMR and the importance of information management is being magnified[9].

This study focused on the protection of patient information generated both on- and off-line. In this light, it discussed the factors below and sets a number of hypotheses. The focus is on managerial protection of the psychological and cognitive elements of patient information users.

2.1 Security Policies

To efficiently protect information, security policies are the most important security requirements for all entities that access information. Security policies do not just refer to one standardized type of policy, but should be optimized in accordance with organizational duties, goals, and features such as type, size, roles and information system management[10]. Because medical institutions put publicity before profit, this feature should be closely related to security policies. Users can easily trust security policies that are well defined and verified for patient information protection. Thus, this study selected security policies as predisposing factors that could influence security awareness, individual characteristics and security effectiveness.

H1: Stronger security policies would have a positive effect on security awareness.

H2: Stronger security policies would have a positive effect on individual characteristics.

H5: Security policies would positively influence security effectiveness.

2.2 Security Awareness

Patient information is computerized as a result of the development of hospital information systems that can quickly deliver a large amount of information to various persons to increase efficiency. However, the possibility of large-scale exposure of patient information continues to increase, creating new problems in patients' privacy protection[11]. Thus, doctors, nurses, medical technicians and administrative staff who deal with patient information need to recognize that patient information is very sensitive and valuable[12]. Therefore, only when information system users are aware of information security can the level of information system security consciousness be improved and information leakage minimized. In relation to this, the following hypothesis was set:

H3: Higher security awareness would more positively influence security effectiveness.

2.3 Individual Characteristics

It is essential to be well informed of security regulations required by an organization in dealing with patient information. Stanton et al.[13] considered acquisition of security knowledge to be an individual characteristic, and emphasized it as a predisposing factor for security effectiveness. This study specified security knowledge as an individual characteristic and performed a survey regarding understanding of security systems, password encouragement for patient information protection and solutions and responding measures for information

leakage. Thus, it was expected that individual characteristics would influence security effectiveness. Therefore, the following hypothesis was set:

H4: Individual characteristics would positively influence security effectiveness.

2.4 Security Effectiveness

After identifying security risk and determining degree of risk, security effectiveness could be realized by examining places where security measures or security controls are needed. In order to maximize security effectiveness, security education programs and security measures should be devised to control information leakage. After consulting Kankanhalli et al.[14], the current study measured security effectiveness by conducting a survey regarding experiences of exposing patient information violation regulations.

The main factors that influence security effectiveness have been based on the literature discussed above. In this study, a research model was developed (Figure 1) and used as the basis for verifying hypotheses.

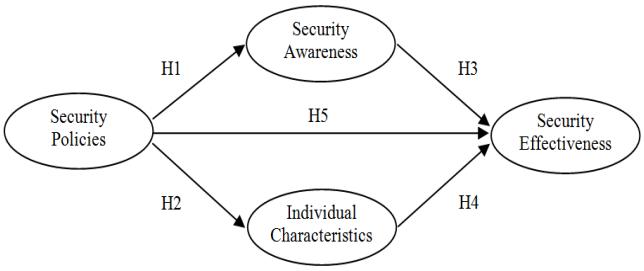

Figure 1. Research model.

3. Methodology

3.1 Sample

This study aims to substantiate the effect of individual characteristics and security awareness based on medical institutions' security policies for security effectiveness. For this purpose, employees of local government operated public hospitals were selected as subjects. The survey was conducted using structured questionnaires completed by administrative staff, medical technicians, nurses and doctors from 7 hospitals across the country. The research duration was 2 months, taking place between June and July 2014. A total of 500 questionnaires were distributed and 263 employees responded (response rate = 52.6%). After exclusion of 7 insincere questionnaires, data from a total of 256 questionnaires were used in the final analysis.

3.2 Construct Measures

Items in the self-administered questionnaire consisted of 4 questions about the medical institutions' security policies, 5 questions about respondents' security awareness, 4 questions about individual characteristics and 4 questions about the respondents' experience of security effectiveness. All questions were rated on a 7-point Likert Scale ranging from 1 point for "not at all" to 7 points for "very much so". Demographic characteristics surveyed included gender, age, career years, position and department.

3.3 Data Analysis

PASW Statistics version 18.0 was used for frequency analysis of respondents' general characteristics and analysis of questionnaire question reliability. Structural Equation Modeling (SEM) was used for the verification of hypotheses. SEM enables the presumption of multiple and mutual subordinate relationships, inclusion of potential variables in the relationships, and presumption of measurement errors[14]. AMOS version 18.0 was used to conduct SEM analysis.

Table 1. Construct measures

Variable	Definition	Items	Reference
Security policies	Degree of hospital's execution of Security Regulations and Procedure	4	Wiant[10] Doherty and Fulford[15] Karyda et al.[16]
Security awareness	Degree of interest in and recognition of importance of patients' Information Security	5	Khan et al.[11] Agrawal and Johnson[12] Drevin et al.[17] Leach[18]
Individual characteristics	Degree of prior knowledge related to protection of patients' information which affects the use and performance of hospital's Information System	4	Stanton et al.[13] Baldwin and Rice[19] King and Xia[20]
Security effectiveness	Degree of exposure experience of patients' information based on real experience	4	KanKanhalli et al.[14] Herath and Rao[21]

4. Result

4.1 Respondent Profile

The results of analysis on the general characteristics of the respondents are shown in Table 1. The ratio of women to men was comparatively higher, with 184 women (71.88%) and 72 men (28.13%) subjects. In order of frequency, age ranges included 94 persons (36.72%) aged 30-39, 78 persons (30.47%) aged 40-49 and 58 persons (22.66%) aged 20-29 and 26 persons (10.16%) over the age of 50. Of all participants, 66 persons (25.78%) had been employed for less than 5 years, and 57 persons (22.27%) for over 20 years, respectively. In terms of position, the highest number of respondents was 208 for general employees (81.25%). Additionally, in order of frequency, representation of work departments included 104 (40.63%) nurses, 93 (36.33%) medical technicians and 59 (23.05%) administrative personnel.

Table 2. Demographic characteristics

	Variable	N	%
Sex	Male	72	28.13
	Female	184	71.88
Age	20~29	58	22.66
	30~39	94	36.72
	40~49	78	30.47
	50+	26	10.16
Career	0~4	66	25.78
(year)	5~9	50	19.53
	10~14	52	20.31
	15~19	31	12.11
	20+	57	22.27
Position	Staff	208	81.25
	Assistant Manager	25	9.77
	Senior Manager	23	8.98
Department	Administration	59	23.05
	Nurses	104	40.63
	Medical technicians	93	36.33
	Total	**256**	**100.00**

4.2 Reliability and Validity

SEM analysis was applied to detect relationships among constructs. Each measurement model was analyzed for respective constructs prior to analyzing the substantive model[22]. Convergent validity was achieved if the standard estimate of the measures to their respective constructs were at least 0.50[23]. Table 2 shows the range of loadings between 0.509 and 0.989, thus establishing convergent validity.

Further supporting convergent validity, the Composite Reliability (CR) of all constructs was above 0.6[23] and the Average Variance Extracted (AVE) was above 0.5[24]. The inter-variable correlations (Table 3.) were examined and the square-root AVEs were higher than correlations, suggesting that the construct was more closely related to its own measures thus supporting discriminated validity (Table 4)[24].

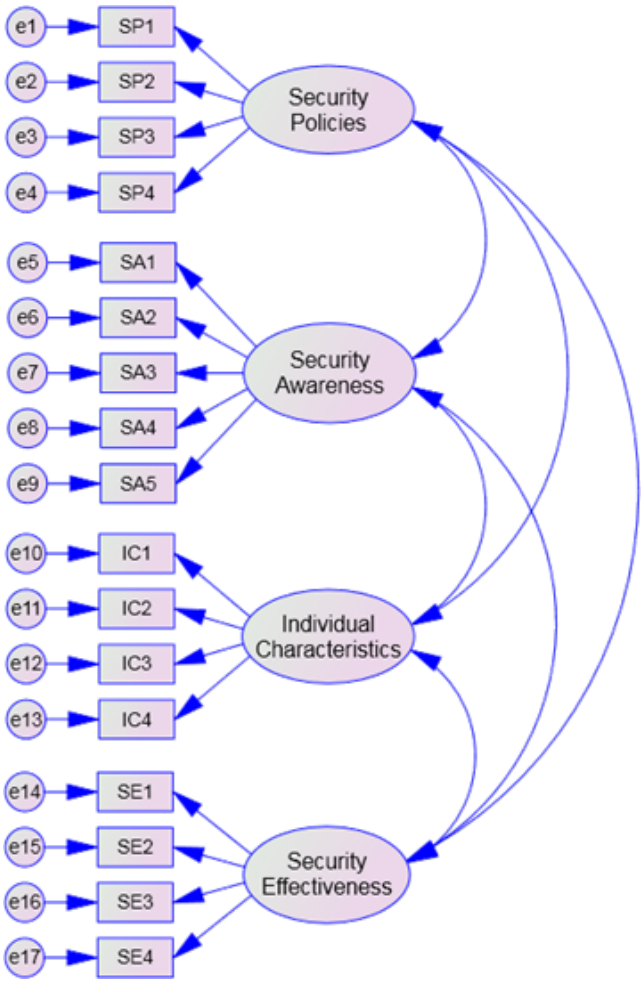

Figure 2. Confirmatory factor analysis.

Table 4. Correlation matrix among factors

Construct	SP	SA	IC	SE
SP	0.667			
SA	0.364	0.792		
IC	0.551	0.255	0.640	
SE	-0.097	-0.111	-0.123	0.857

4.3 Hypotheses Testing

Results of analysis using the SEM for the verification of hypotheses based on the study model are shown in Tables

Table 3. Results of measurement model test

Construct	Item	Estimate	Standard Estimate	S.E.	t-value	p-value	CR	AVE
Security	SP1	1.010	0.842	0.050	20.231	<0.001	0.889	0.667
Policies	SP2	0.986	0.891	0.042	23.405	<0.001		
(Sp)	SP3	1.036	0.926	0.038	26.972	<0.001		
	SP4	1.000	0.926					
Security	SA1	1.131	0.888	0.059	19.032	<0.001	0.950	0.792
Awareness	SA2	1.084	0.934	0.052	20.953	<0.001		
(SA)	SA3	1.024	0.882	0.054	18.814	<0.001		
	SA4	1.040	0.899	0.053	19.500	<0.001		
	SA5	1.000	0.833					
Individual	IC1	0.812	0.816	0.038	21.203	<0.001	0.875	0.640
Characteristics	IC2	0.773	0.733	0.047	16.510	<0.001		
(Ic)	IC3	1.010	0.977	0.022	45.308	<0.001		
	IC4	1.000	0.979					
Security	SE1	0.705	0.509	0.087	8.073	<0.001	0.957	0.857
Effectiveness	SE2	0.386	0.513	0.056	6.867	<0.001		
(SE)	SE3	1.291	0.989	0.056	23.226	<0.001		
	SE4	1.000	0.833					
Model Fit		X^2=288.326(df=109, p<0.001), X^2/DF=2.645 GFI=0.888, AGFI=0.843, NFI=0.936, CFI=0.959, RMSEA=0.080						

4 and 5. Based on the goodness-of-fit standard presented by Bagozzi and Yi[21], goodness-of-fit indexes were generally good with X2 = 283.296 (df = 110, p < 0.001), x2/DF = 2.575, GFI = 0.881, AGFI = 0.845, NFI = 0.937, CFI = 0.961 and RMSEA = 0.079.

The path coefficient estimate in which security policy affects security awareness was 0.357 (t = 5.854, p < 0.001). Thus, hypothesis H1 that "Higher security policy has a positive (+) effect on security awareness" was adopted. In addition, the path coefficient estimate in which security policy affects individual characteristics was 0.553 (t = 9.764, p < 0.001). Thus, hypothesis H2 that "Higher security policy has a positive (+) effect on individual characteristics" was adopted. Since the path coefficient estimate with which security awareness affects security effectiveness was -0.026 (t = -0.636, p = 0.525) hypothesis H3 that "Security awareness has a positive (+) effect on security effectiveness" was rejected. Furthermore, the path coefficient estimate with which individual characteristics affects security effectiveness was -0.045 (t = -0.999, p = 0.318). Thus, hypothesis H4 that "Individual characteristics have a positive (+) effect on security effectiveness" was rejected. Finally, the path coefficient estimate with which security policy affects security effectiveness was -0.009 (t = -0.199, p = 0.842). Therefore, hypothesis H5 that "Security policy has a positive (+) effect on security effectiveness" was rejected.

In summary, results indicated that while security policies have a statistically significant positive effect on security awareness and individual characteristics, they ultimately do not have effect on security effectiveness.

Table 5. Result of SEM

Path	Estimate	Standard Estimate	S.E.	t-value	p-value
SP → SA	0.234	0.357	0.040	5.854	<0.001
SP → IC	0.602	0.553	0.062	9.764	<0.001
SA → SE	-0.009	-0.026	0.014	-0.636	0.525
IC → SE	-0.009	-0.045	0.009	-0.999	0.318
SP → SE	-0.002	-0.009	0.010	-0.199	0.842
Model Fit	X^2=283.296(df=110, p<0.001), X^2/DF=2.575 GFI=0.881, AGFI=0.845, NFI=0.937, CFI=0.961, RMSEA=0.079				

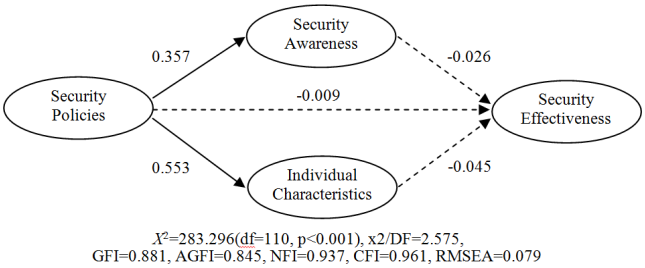

Figure 3. Result of model testing.

Table 6. Summary of support for hypotheses

Hypotheses	Result
H1: Stronger security policies would have a positive (+) effect on security awareness.	Supported
H2: Stronger security policies would have a positive (+) effect on individual characteristics.	Supported
H3: Higher security awareness would influence security effectiveness more positively.	Not supported
H4: Individual characteristics would influence security effectiveness positively.	Not supported
H5: Security policies would influence security effectiveness positively.	Not supported

5. Conclusions

To suggest effective policies for patient information protection, this study was conducted on the employees of local public hospitals established in the major cities around the country. The effect of security policies on security awareness and individual characteristics and their effect on security effectiveness were explored through SEM. Implications of major study results are as follows.

First, security policy proved to have positive effect on security awareness and individual characteristics, showing it is the antecedent to enhancing them. Security policy is the highest requirement necessary for the realization of information protection in an organization[10, 15]. The results of this study correspond with those of preceding studies on information protection in various industries[25].

Second, in general, sharing information about security policy among members of an organization brings security effectiveness, which can minimize the damage from information leakage. Moreover, it enables information system users to recognize the importance of security enhancement awareness level. Preliminary knowledge about information security, which is an individual characteristic, has a positive effect on security effectiveness[26]. In contrast to previous studies, security awareness, individual characteristics and security policy did not have positive effect on security effectiveness[27]. Medical institutions have been slower in developing information technology than other industries. Therefore, it is necessary to consider various influencing factors in and outside of the organization that differ from those of other industries. Moreover, since the study subjects were recruited from local public hospitals, it is necessary consider that they may have difficulty reflecting on the rapidly changing reality of information protection.

In conclusion, although security policy has an effect on security awareness and individual characteristics, it does not necessarily bring about security effectiveness. Therefore, this empirical analysis of the proposed study model can be partially accepted. On the basis of this study, it is supposed that the development of an expanded model is required. Specifically, this model should fit the subjects of this type of study and include research on diverse mediating variables that may influence the relationship between security policy and security effectiveness.

6. References

1. Haux R. Health information systems - past, present, future. Int J Med Informat. 2006; 75(3-4):268–81.
2. Yoon D, et al. Adoption of electronic health records in Korean tertiary teaching and general hospitals. Int J Med Informat. 2012 Mar; 81(3):196–203.
3. Choi Y, et al. Adjusting context-aware RFID in health screening center. Journal of Computer Virology and Hacking Techniques. 2014 May; 10(2):115–8.
4. David B, Larget D, Scherrer T. The security of databases: the Access case. Journal of Computer Virology and Hacking Techniques. 2013 May; 9(2):95–107.
5. Liginlal D, et al. HIPAA Privacy Rule compliance: an interpretive study using Norman's action theory. Comput Secur. 2012 Mar; 31(2):206–20.
6. Wu K-W, et al. The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior. 2012 May; 28(3):889–97.
7. King T, Brankovic L, Gillard P. Perspectives of Australian adults about protecting the privacy of their health information in statistical databases. Int J Med Informat. 2012 Apr; 81(4):279–89.
8. Castle D, DeBusk R. The electronic health record, genetic information, and patient privacy. J Am Diet Assoc. 2008; 108(8):1372–4.
9. Damschroder LJ, et al. Patients, privacy and trust: Patients' willingness to allow researchers to access their medical records. Soc Sci Med. 2007 Jan; 64(1):223–35.

10. Wiant TL. Information security policy's impact on reporting security incidents. Comput Secur. 2005 Sep; 24(6):448–59.
11. Khan FA, et al. A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. Procedia Computer Science. 2014; 34:511–7.
12. Agrawal R, Johnson C. Securing electronic health records without impeding the flow of information. Int J Med Informat. 2007; 76(5-6):471–9.
13. Stanton JM, et al. Analysis of end user security behaviors. Comput Secur. 2005 Mar; 24(2):124–33.
14. Kankanhalli A, et al. An integrative study of information systems security effectiveness. Int J Inform Manag. 2003 Apr; 23(2):139–54.
15. Doherty NF, Anastasakis L, Fulford H. The information security policy unpacked: a critical study of the content of university policies. Int J Inform Manag. 2009 Dec; 29(6):449–57.
16. Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: a contextual perspective. Comput Secur. 2005 May; 24(3):246–60.
17. Drevin L, Kruger HA, Steyn T. Value-focused assessment of ICT security awareness in an academic environment. Comput Secur. 2007 Feb; 26(1):36–43.
18. Leach J. Improving user security behaviour. Comput Secur. 2003 Dec; 22(8):685–92.
19. Baldwin NS, Rice RE. Information-seeking behavior of securities analysts: Individual and institutional influences, information sources and channels, and outcomes. J Am Soc Inform Sci. 1997 Aug; 48(8):674–93.
20. King RC, Xia W. Media appropriateness: Effects of experience on communication media choice. Decis Sci. 1997 Oct; 28(4):877–910.
21. Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis Support Syst. 2009 May; 47(2):154–65.
22. Anderson JC, Gerbing DW. Structural equation modeling in practice: a review and recommended two-step approach. Psychol Bull. 1988; 103(3):411–23.
23. Bagozzi RP, Yi Y. On the evaluation of structural equation models. J Acad Market Sci. 1988; 16(1):74–94.
24. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. J Market Res. 1981 Feb; 18(1):39–50.
25. D'Arcy J, Hovav A. Deterring internal information systems misuse. Commun ACM. 2007 Oct; 50(10):113–7.
26. Kim M, Hong Y. Implementation of a web-based smart electronic needle system. Journal of Computer Virology and Hacking Techniques. 2014 May; 10(2):101–8.
27. Oh S-Y, et al. Recent trends in mobile communication systems. Journal of Computer Virology and Hacking Techniques. 2014 May; 10(2):67–70.