Global Spectrum of Research and Humanities
ISSN: 3007-9136
Vol. 2 No. 1 (2025): Spring

Information Security Management: The Effect of Organizational Commitment and Perceived Consequences of Disclosure of Confidential Information on Patient Information Breach Intention

[1]Mohammad Ekram Yawa, [2]Mohammad Qurban Hakimi
https://doi.org/10.69760/gsrh.01012025008

Keywords:

Security policy
Intent to Violate Information Security
Commitment

Abstract:

Background and Objective: Information security is a vital issue in the field of health and medicine. In most of the research conducted in this field, the human factor has been ignored and a kind of technical view and approach has been adopted. The present article was conducted with the aim of determining the relationship between personnel's perception of the consequences of information disclosure and employees' commitment to their intention to violate information security.

Materials and Methods: The sample of this study consisted of 181 specialists from specialized teaching hospitals in Kabul city who were sampled using a locally developed questionnaire using a convenient method. To measure the perceived consequences of information disclosure, D'Arcy et al.'s questionnaire with 7 questions and two dimensions of perception of the certainty and severity of punishments was used, and to measure organizational commitment, Allen and Meyer's 24-question questionnaire with three dimensions of affective, normative, and continuum commitment was used. After confirming the face validity, content and construct reliability using Cronbach's alpha and composite reliability, the hypotheses were tested using the partial least squares method and Smart PLS software.

Findings: The findings of this study showed that the perception of medical specialists of organizational policies that indicate the certainty and severity of penalties for information disclosure had a significant negative relationship with their intention to breach the security of patient information ($P<0.001$). The results also showed

[1] Asst. Prof. Dr. Mohammad Ekram Yawar, Dean of the Faculty of Law, International Science and Technology University, Warsaw, Poland, ekram.yawar@istu.edu.pl, https://orcid.org/0000-0003-3198-5212

[2] Mohammad Qurban Hakımı ,Master's degree student in health management, İSTANBUL KENT University, İstanbul, Türkiye, Mail: masihyk2018@gmail.com, https://orcid.org/0009-0005-6121-5069.

that the physicians' perception of commitment, which included affective, normative, and ongoing commitment, was not significantly related to their intention to breach patient information security.
Ethical considerations: Participation in data collection was voluntary, verbal consent was obtained from participants, and they were assured of the confidentiality of their identities.
Conclusion: Organizational policies regarding the severity and severity of punishments for doctors who violate information security should be tightened at the hospital level and even at the ministry level, and should be communicated to healthcare professionals, including doctors, through various tools.

1. Introduction

The use of information technology capabilities in the health industry,[3] in the form of various e-health applications, is becoming more widespread.[4]

Since the security and control of patient-related health information is a fundamental[5] component of all health care information systems,[6]

this relationship has raised significant concerns about privacy and information security, as patient medical records contain some of the most private and confidential information about the patient and, given that computerized information is readily accessible from multiple locations, it can be easily compromised.[7] Defects in these systems will lead to the risk of information disclosure.[8]

This is while the human factor is often considered as one[9] of the most important factors in information systems security programs.

In the event of creating all technical provisions and security policies, the lack of awareness and carelessness of users can render all technical protections ineffective.[10] For this reason, two factors, deterrence and employee commitment,[11] are proposed as potential factors effective in reducing information security breaches.[12]

According to deterrence theory, technical measures have deterrent power when they provide knowledge of unacceptable behavior and then create fear or a desire to prevent negative consequences.[13] According to this theory, since security policies are equivalent to organizational rules, it is expected that understanding the consequences of violating organizational rules will reduce information disclosure behaviors, because

[3] Peikari,et, al.2013.
[4] Hussain and Peikari,2016.
[5] Kuo A,2016.
[6] Fakhrzad,et,al.2012.
[7] Huffman.2006.
[8] Ghazi-Asgar, et al.2018.
[9] Fernández-Alemán,,et,al.2018.
[10] Fernández-Alemán,,et,al.2018.
[11] Khosravani,et,al.2017.
[12] Siponen and, Vance,10.
[1313] Luxton,et,al.2012.

the implementation of these measures will increase employees' awareness of the consequences of information disclosure. Deterrence theory states that when individuals are about to commit a violation, they weigh the severity and likelihood of its benefits and harms and then take action accordingly.[14]

Deterrence theory includes formal sanctions such as punitive laws and policies established by organizations and informal sanctions such as disapproval from colleagues, feelings of guilt, and anxiety from others, so personnel's awareness of the existence and severity of sanctions and the intention to misuse confidential information can increase their security behaviors.[15]

Employee compliance with information security policies has been reported as one of the major problems in organizations in the field of security principles.[16] It is estimated that more than half of all information security system breaches are directly or indirectly caused by inappropriate employees.[17] Violations of security policies by employees are often due to negligence and ignorance or to intentional behavior that violates organizational regulations.[18] Based on deterrence theory, organizational policies regarding the consequences of information disclosure include 2 dimensions: the certainty of punishment[19] and the severity of punishment.[20] On the other hand, commitment can be a major factor in maintaining confidentiality among individuals.[21] Individuals who are more committed to the values and goals of the organization are more likely to be active and contribute more to the organization, and are less likely to leave the organization and find new job opportunities. In fact, the concept of organizational commitment implies a positive attitude that results from employees' feelings of loyalty to the organization and is manifested by the participation of individuals in organizational decisions that consider the organization's members and their success and well-being. Studies conducted in this field show that employee commitment to the organization will have very valuable results for the organization.

Salehifard and Khalaj Asadi[22] and Allen and Meyer consider the dimensions of organizational commitment to include affective commitment, continuance commitment, and normative commitment. In a study, it was shown that more committed technical staff have a greater tendency to maintain ethical principles in the hospital environment.

However, most research related to organizational commitment has been directed towards[23] discovering the predictors and outcomes of organizational commitment.[24] (Considering that the effect of the variables of information disclosure consequences and organizational commitment on the disclosure of confidential information has not been examined simultaneously in research, the present study can be considered a breakthrough in this area. On the other hand, considering the important and determining role of information security in patient health cases in hospitals and its role as one of the most important pillars of treatment, it is worth studying the above-mentioned variables in terms of human factors (employees).[25] Therefore, this article was conducted with the aim of determining the relationship between personnel's perception of the

[14] Albert,et.al.2015.
[15] Ibid.
[16] Peikari,et,ak.2018.
[17] Stanton,et,al.2005.
[18] Lusignan,et,al.2007.
[19] Siponen and, Vance,10.
[20] Peikari,et,ak.2018.
[21] Khosravani,et,al.2017.
[22] Sedaghatifard and Khalaj,2011.
[23] İbid.
[24] Zahed,et,al.2017.
[25] Kluge.2007.

consequences of information disclosure and employees' commitment to their intention to violate information security. To this end, the following hypotheses were examined in this study:[26]

- Personnel's perception of organizational policies that indicate the certainty and severity of penalties for information disclosure has a significant negative relationship with their intention to breach patient information security.[27]

- Personnel's perception of affective, normative, and ongoing commitment does not have a significant negative relationship with their intention to breach patient information security.[28]

2. Ethical considerations

In order to comply with ethical considerations, the following steps were taken:

1- Obtaining a letter of introduction to attend the research environment from the university of the place of study.

2- Obtaining permission from the hospital director and department officials to attend the researcher and carry out the necessary steps.

3- Introducing yourself to the participants and briefly explaining the purpose of the study, the method of cooperation, the benefits and disadvantages of participating in the study, and the purpose of completing the questionnaire.

4- Obtaining written informed consent from participants to participate in the study.

5- Obtaining permission from participants to complete the questionnaire.

6- Assure participants of maintaining privacy, confidentiality, and privacy of information.

7- Assure participants that they can withdraw from the study at any time if they wish, and that they are even free to withdraw from the study at any stage.

8- Collect data in terms of time and place with the consent of the participants.

9- Ensure that the participants are fully informed about the analysis and interpretation of the data and adhere to the principles of anonymity in the implementation, analysis, reporting and dissemination of information.[29]

3. Materials and Methods

The research method in this study is descriptive, correlational, and falls into the category of field studies. The study population consisted of all kidney specialists in specialized teaching hospitals in Kabul city. Based on the Morgan table, a sample size of 220 of them was selected using convenience sampling. After the questionnaires were distributed, 181 of them completed the research questionnaires. The first part of the collected questionnaires dealt with individual characteristics, and the second part included three questionnaires: organizational commitment, perception of the severity and certainty of punishments, and

[26] Kruger and Kearney,2006.
[27] Farzandipour,et.al.2010.
[28] Ghayour,et,al.2016.
[29] Elahi,et,al.2009.

an information security breach intent questionnaire, which were adapted and standardized from articles published in reputable scientific journals.[30]

To measure individuals' perceptions of the consequences of information disclosure, the questionnaire by D'Arcy et al.[31] was adapted, standardized, and standardized. The questionnaire consists of 7 items and has two dimensions: perception of the certainty of punishments and perception of the severity of punishments. To measure organizational commitment, the 24-item organizational commitment questionnaire by Allen and Meyer[32] was used. The present questionnaire has a total score as organizational commitment and three subscales of affective commitment, normative commitment, and continuance commitment. The scoring method for non-demographic questions is based on a 5-point Likert scale from 5 (completely agree) to 1 (completely disagree).

To validate the questionnaire, three methods were used: content validation (by reviewing the questionnaire by professors and experts in the field), face validation (by distributing the questionnaire among a limited number of the target population), and after data collection, construct validation using a confirmatory factor analysis approach.[33]

After confirming the validity and reliability, the proposed model was analyzed by SmartPLS software using the partial least squares approach.

4 Findings

The findings are reported in three sections: Demographic data, construct validity and reliability, and hypothesis testing.

4.1 Demographic Results

As shown in Table 1, most of the respondents were male (62.98%) while the largest group of respondents were between 31-40 years old (46.41%) with 11-15 years of work experience (23.2%).

The findings related to demographic data are shown in Table 1.

[30] Sohrabi and Von,2016.
[31] D'Arcy,et.al.2009.
[32] Allen and Meyer,1990.
[33] Waldo,et,al,2014.

Table 1: Demographic data

Characteristics		Abundance	Percentage
Gender	Male	114	62/98
	Female	67	02/37
Age	30 and under 30	48	26/52
	31-40	84	46/41
	41-50	42	20/23
	Over 50	7	3/87
Service Experience	Less than 6 years	65	35/91
	6-10	35	19/34
	11-15	42	20/23
	16-20	15	8/29
	21-25	10	5/52
	Over 25 years	14	7/73

4 .2 Construct Validity and Reliability

Since the sample size was smaller than 200 people and the model was complex (two-dimensional structure), the partial least squares method (PLS: Partial Least Square) was used for confirmatory factor analysis and hypothesis testing.

After assessing the validity of this method, items 26, 35, 6, 7, 4432, and 46 were removed from the model due to the lower than standard factor loadings in the variables.

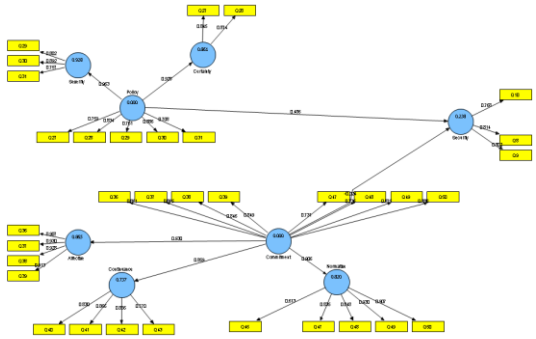

Figure 1: Results of confirmatory factor analysis

As shown in Figure 1, all variables had factor loadings greater than 0.5 on their respective variables. In addition, as shown in Table 2, the average variance extracted (AVE) was greater than 0.5.

Table 2: Reliability and validity results

Variables	Cronbach's Alpha	CR	AVE
Emotional commitment	0.94	0.96	0.85
Severity of punishment	0.75	0.85	0.74
Commitment	0.94	0.95	0.69
Continuous commitment	0.85	0.90	0.69
Normative commitment	0.89	0.92	0.70
Policy	0.85	0.89	0.63
Security	0.71	0.84	0.63
Severity of punishment	0.75	0.86	0.67

In addition, as shown in Table 3, it was found that the rule of Lerker and Forner was observed. For reliability testing, the Reliability Composite (CR) scale and Cronbach's alpha were used, and as shown in Table 2, the composite reliability and Cronbach's alpha value greater than 0.7 indicate high reliability for the scale. Therefore, the results indicate that the scale has acceptable validity and reliability.

Table 3: Al-Rak and Furn's rule

Variables	Average	1	2	3	4	5	6	6
Emotional	0.85							
Commitment	0.74	0.63						
Punishment	0.69	0.67	0.52					
Firmness	0.69	0.68	0.55	0.51				
Commitment	0.70	0.48	0.60	0.62	0.53			
Continuous	0.63	0.62	0.56	0.35	0.59	0/42		
Commitment	0.63	0.63	19/0	0.52	0.56	0/51	0.51	
Normative	0.67	0.67	0.63	0.53	0.26	0/48	0.61	0/60

4.3 Hypothesis Testing

SmartPLS software was used to test the hypotheses and as shown in Table 4, no significant relationship was observed between the intensity of employee commitment and security compliance, while it was found that perceived organizational policies can be significantly related to security compliance in the organization ($P<0.001$).

The details of this hypothesis test are shown in Figure 2.

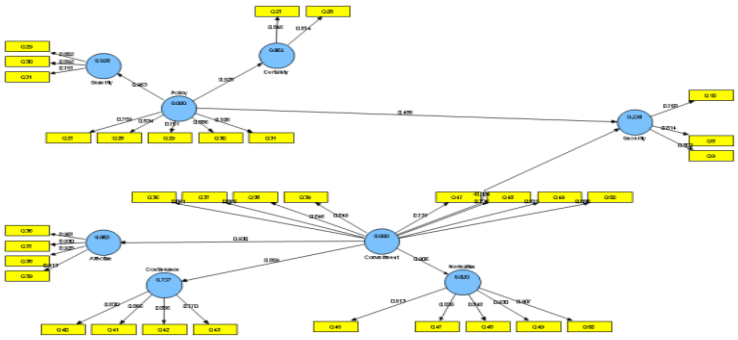

Figure 2: Hypothesis results

Table 4: Hypothesis results

Hypothesis	t-value	Hypothesis result
The Relationship Between Commitment and Intention to Breach Information Security	0/39	Rejected
The Relationship Between Perceived Consequences of Disclosure and Intention to Breach Information Security	69/33	Accepted

5. Discussion

The present article aimed to determine the relationship between staff perception of the consequences of information disclosure and staff commitment with their intention to breach information security.

In the first hypothesis of the study, staff perception of organizational policies that indicate the certainty and severity of punishment for information disclosure was examined, considering its negative relationship with their intention to breach patient information security. The results obtained indicated that at a significant level ($P<0.001$), the present hypothesis is confirmed.

The results of the present study are consistent with the results obtained from previous studies.[34] In explaining the present findings, it can be stated that when employees examine their behavioral outcomes and are faced with the issue that they will face penalties for not complying with security principles, they have a lower desire to engage in risky behaviors in the field of information security. In other words, when individuals evaluate the outcomes of their behaviors through the consequences (punishment and certain punishment), they have a lower desire to violate the organization's information security. It can also be stated that the greater the level of certainty of receiving punishments, the lower the likelihood of information abuse behaviors. [35]

Karimi and Peekari[36] (29) showed that when the consequences of information disclosure are clearly stated in the organization's security policies and employees know what punishments they will face if they engage in information security-violating behaviors, they react positively and take action to avoid punishment. They

[34] D'Arcy,et,al.2009.
[35] Karimi and Peikari,2018.
[36] Ibid.

will adhere to the organization's security policies, so they will have less intention to violate security principles.

In the second hypothesis of the study, based on the perception of staff from emotional, normative[37] and continuous commitment, there is a significant negative effect on the intention to violate the security of patient information by staff, the research hypothesis was not confirmed and rejected.[38] The results of the present study are contradictory to the results of previous studies.[39] In explaining the above findings, it can be stated that since an organization's human resources are considered its greatest wealth and asset, and the success of organizations depends on the presence of efficient and capable individuals who follow and are influenced by the organization's policies and programs and consider themselves committed to their implementation, because the efficiency and type of values and policies governing the organization are what drive individuals in the organization and have a pervasive effect on the organization's components. [40]

Therefore, if members of an organization have common goals, values, and policies, they will ultimately develop an emotional attachment to them and will remain committed and loyal to the organization[41] and, as a result, follow security policies and orders and programs that are consistent with them. However, since such results were not found, it can be stated that the severity and certainty of the policies and penalties determined for information security breaches in the relevant organization have sufficient deterrent power to prevent behaviors that are inconsistent with the organization's policies, and that technical solutions Preventing information misuse is effective enough. The intention to misuse an organization's information is influenced by various factors, the most important of which are motivational factors.[42]

As a result, it can be said that just as there is a need for sufficient motivation to form and carry out information abuse behaviors, an individual must also have sufficient motivation to prevent it. Therefore, in the present context, it can be stated that if the intensity of inhibitory behaviors and their perception are greater than the motivational factors effective in launching it, it can be effective in preventing the occurrence of information abuse behavior in the organization. Barton et al.[43] state that users of a system can be inspected and reprimanded for violating the organization's security policies when they have sufficient self-awareness about the behavioral consequences.

For this reason, they believe that the first step to prevent the misuse of an organization's information is to provide awareness of the severity of the penalties determined for privacy-violating behaviors and information disclosure through organizational culture.

Chong and Eggleton[44] propose a threat model to prevent behaviors related to information security violations. In the threat model, individuals' evaluation of the severity of the penalties proposed for information security violations reduces risky and violating behaviors.

The attention of managers and officials of the Ministry of Health to the issue of information security is among the issues that are regulated and determined based on the theory of deterrent behavior. Therefore, if individuals' assessment of the certainty and severity of penalties related to non-compliance with security principles is incorrect or if they do not have a perception about the severity of penalties related to non-

[37] Stanton,et,al.2005.
[38] Barton,el,al.2016.
[39] Koskosas,et,al.2011.
[40] Ibid,
[41] Ziaee,et,al.2011.
[42] Hasanzadeh,et,al.2011.
[43] Barton,el,al.2016.
[44] Chong and Eggleton,2007.

compliance with information security principles, they will follow the organization's policies less and their risky behaviors regarding compliance with information security principles will increase.[45]

Therefore, in this context, it is suggested that in defining organizational policies, they specify the behaviors that cause information security violations so that users know what behaviors are considered information misuse from the organization's perspective, and identify the motivating factors effective in the formation of intentional information misuse behaviors so that they can regulate the severity of penalties in a way that has a deterrent effect.

It is also suggested that dos and don'ts be stated explicitly and clearly in order to prevent misunderstandings about organizational policies. . Also, given that the results of the present study did not show a significant relationship between organizational commitment and security components, it can be concluded that the power of organizational policies plays a greater role in preventing information misuse than in maintaining organizational information security. Therefore, it is suggested that similar studies be conducted to confirm or refute these results. Also, given that the method of the present study is correlational, cause and effect cannot be inferred from it, and also because the present study was conducted in a service institution, caution should be exercised in generalizing its results to other institutions.[46]

6. Conclusion

The findings of this study indicate that if staff are aware of the consequences of breaching and disclosing confidential and sensitive patient information, they will refrain from disclosing this information. The consequences of disclosing information for staff can include organizational consequences such as reprimand, suspension, dismissal, or legal consequences such as referral to judicial authorities for investigation and punishment of cases of illegal disclosure of confidential and sensitive information.

Obviously, hospital management can play a significant role in increasing staff awareness in this regard by implementing appropriate tools to inform their staff in this regard, such as holding training courses and classes, sending periodic SMS to staff, and including relevant materials in internal bulletins and publications.

References

Albert L, Michelle M, Yair L.(2015) Examining users'personal information sharing awareness, habits, and practices in social networking sites and e-learningsystems. Online Journal of Applied KnowledgeManagement 2015; 3(1): 180-207.

Allen N, Meyer J.(1990) The measurement and antecedents of affective, continuance and normative commitment. Journal of Occupational Psychology1990; 63(1): 1-18.

Barton KA, Tejay G, Lane M, Terrell S.(2016) Information system security commitment: A study ofexternal influences on senior management. Computers& Security 2016; 59: 9-25.

Chong VK, Eggleton IRC.(2007) The impact of reliance on incentive-based compensation schemes, information asymmetry and organisational commitment onmanagerial performance. Management AccountingResearch 2007; 18(3): 312-342.

[45] Karami,et,al.2013.
[46] Luxton,et,al.2012.

D'Arcy J, Hovav A, Galletta D.(2009) User awareness ofsecurity countermeasures and its impact on information systems misuse: A deterrence approach. InformationSystems Research 2009; 20(1): 79-98.

Elahi S, Taheri M, Hassanzadeh A. (2009)A framework for the role of human factors in information systems'security. Management Research in Iran (Modares Human Sciences) 2009; 13(2): 1-22.

Fakhrzad M, Fakhrzad N, Dehghani M.(2012) The Role of Electronic Health Records in Presenting Health Information. Media 2012; 2(4): 31-40.

Farzandipour M, Sadoughi F, Ahmadi M, Karimi I.(2010)Security requirements and solutions in electronic health records: lessons learned from a comparative study. J Med Syst 2010; 34(4): 629-642.

Fernández-Alemán JL, Sánchez-Henarejos A,Toval A, Sánchez-García AB, Hernández-Hernández I,Fernandez-Luque L.(2015) Analysis of health professional security behaviors in a real clinical setting: an empirical study. Int J Med Inform 2015; 84(6): 454-467.

Fernández-Alemán JL, Señor IC, Lozoya PÁO,Toval A.(2013) Security and privacy in electronic health records: A systematic literature review. J Biomed Inform 2013; 46(3): 541-562.

Ghayour Baghbani SM, Shojaei Kalate Bali N,Chenarani H, Ashoori J.(2016) The Relationship between Organizational Commitment, Job Satisfaction andSocial Orientation, and the Nurses' Moral Behavior.Med Ethics J 2016; 10(37): 27-36.

Ghazi-Asgar M, Peikari HR, Ehteshami A.(2018) HealthInformation Management: Psychological factorsinfluencing information privacy concerns in psychiatric hospitals. Bali Medical Journal 2018; 7(1): 1 7.

Hasanzadeh M, Karimzadegan Moghadam D,Jahangiri N.(2011) Provide a conceptual framework forevaluating the enrichment and education of informationsecurity awareness of users. J of Syst Inf Serv 2011;1(2): 1-16.

Huffman E.(2006) Electronic Medical Record. Translated by Langarizadeh M. Tehran: Dibagaran; 2006.

Hussain Shah M, Peikari HR.(2016) Usability and reduction of workload and medical errors; a survey amongst community physicians. Telemedicine and e-Health 2016; 2(1): 36-44.

Karami M, Safdari R, Soltani A.(2013) Patient'sInformation Rights: Strategies for Information Securityin the Electronic Environment. Medical ethics 2013;7(25): 83-96.

Karimi Z, Peikari HR.(2018) The Impact of Nurses'Perceived Information Security Training and Information Security Policy Awareness on their Perceived Severity and Certainty of InformationSecurity Breach Penalties (Case: the EducationalSpecialized Hospitals of Isfahan City). JNE 2018; 7(2):17-24.

Khosravani M, Khosravani M, Rafiei F,Mohsenpour M.(2017) Organizational commitment and itsdimensions in nurses working in Arak's hospitals. MedEthics J 2017; 11(39): 37-44.

Kluge EHW. (2007) Secure e-health: managing risks topatient health data. Int J Med Inform 2007; 76(5): 402-406.

Koskosas I, Kakoulidis K, Siomos CH.(2011) InformationSecurity: Corporate Culture and OrganizationalCommitment. International Journal of Humanities andSocial Science 2011; 1(3): 1-12.

Kruger HA, Kearney WD. A(2006) prototype for assessing information security awareness. Computer &Security 2006; 25(4): 289-296.

Kuo A, Dang S.(2016) Secure Messaging in Electronic Health Records and Its Impact on Diabetes Clinical Outcomes: A Systematic Review. Telemedicine and eHealth 2016; 22(9): 125-132.

Lusignan SD, Chan T, Theadom A, Dhoul N.(2007) Theroles of policy and professionalism in the protection ofprocessed clinical data: a literature review. Int J Med Inform 2007; 76(4): 261-268.

Luxton DD, Kayl RA, Mishkind MC.(2012) Health Data Security: The Need for HIPAA-CompliantStandardization. Telemedicine and e-Health 2012;18(4): 124-131.

Mahdad A.(2016) Industrial and Organizational Psychology. Tehran: Jangal Publisher; 2016.

Peikari HR, Ramayah T, Shah MH, Lo MC.Patients(2018)' perception of the information security management in health centers: The role of organizational and human factors. BMC Med Inform Decis Mak 2018; 18(1):102-122.

Peikari HR, Zakaria MS, Norjaya MN, Hussain ShahM, Elhissi A.(2014) Role of CPOE usability in the reduction of prescribing errors. Healthc Inform Res 2013; 19(2):93-101.

Sedaghatifard M, Khalaj Asadi SH.(2011) Relation with job satisfaction Index to organizational commitment infaculty members of Islamic Azad University-GarmsarBranch. Journal of Modern Industrial/ OrganizationPsychology 2011; 2(6): 39-51.

Siponen M, Vance A.(2010) Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly 2010; 34(3):487-502.

Sohrabi Safa N, Von Solms R,(2016) Furnell S.Information security policy compliance model in organizations. Computers & Security 2016; 56: 70-82.

Stanton JM, Stam KR, Mastrangelo P, Jolton J.(2005) Analysis of end user security behaviours. Computer &Security 2005; 24(2): 124-133.

Waldo RF, Antonsen E, Ekstedt M.(2014) Information security knowledge sharing in organizations:Investigating the effect of behavioral information security governance and national culture. Computers &Security 2014; 43: 90-110.

Zahed Babelan A, Khaleg Khah A, Kazemi S,Gharibzadeh R.(2017) The Role of Spiritual Leadership and Professional Ethics in Organizational Commitment ofHealth Care Workers. Bioethics Journal 2017; 7(26):23-30.

Ziaee MS, Roshandel Arbatani T, Nargesian A.(2011) Examine the relationship between organizationalculture and organizational commitment among the staffof the library of Tehran University: Based on theDenison organizational culture model. Journal of Academic Library and Information Science (LIS) 2011;45(1): 42-79.

Received: 10.02.2025
Revised: 15.02.2025
Accepted: 18.02.2025
Published: 21.02.2025